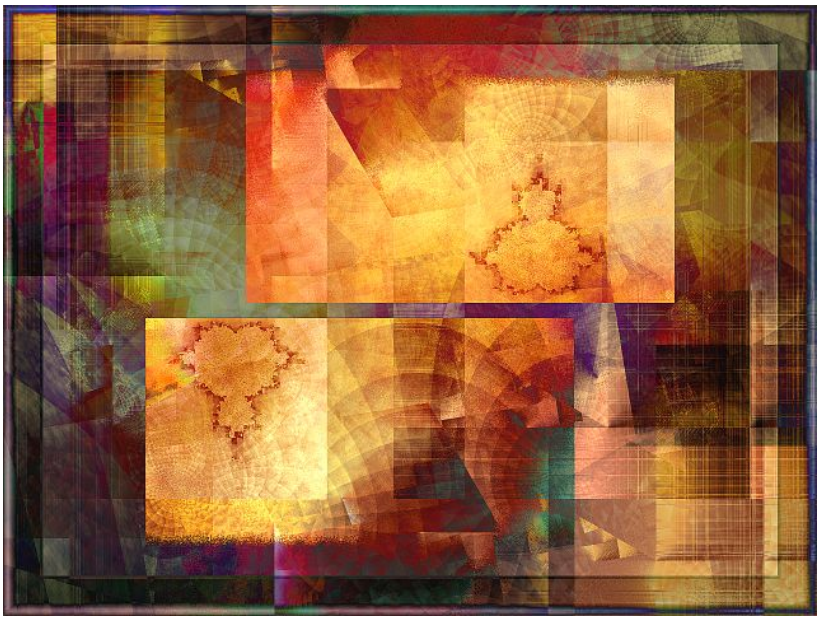
Electronic Colloquium on Computational Complexity, Report No. 62 (2009)

ECCC

Lecture Notes on Algorithmic Number Theory

D. Venturi



Inspired by a series of lectures of

Renè Schoof

Università di Roma "Tor Vergata"

ISSN 1433-8092

LECTURE NOTES ON ALGORITHMIC NUMBER THEORY

Daniele Venturi

Dipartimento INFOCOM, Università di Roma "La Sapienza".

✉ Author's e-mail:
venturi@infocom.uniroma1.it

Author's website:
http://net.infocom.uniroma1.it/homepages/venturi.htm

Version 1.0, June 2009.

PREFACE

The main fount of inspiration for these notes was the class *Crittografia*, taught by Prof. Renè Schoof at the university of Rome *TorVergata* (Italy), faculty of *Mathematics*, I followed during the first semester of the academic year 2008-2009[1].

I was really impressed by Renè's lectures, so that I started going into more depth: this is the result. The material covered in these notes is not new; the only reason for reading them is if an individual reader finds the explanations here easier to understand than those elsewhere. Some examples in the text are taken from [**51**], whereas the part on bilinear pairings follows the exposition of [**33**]. The principal aim is to give a survey on the state of the art of *algorithmic number theory*, with particular focus on the theory of elliptic curves. This is not (surely) the unique survey on this field, but it has one merit: the treatment is almost elementary, and the pre-requisite for reading these notes is just elementary algebra (rings, groups and fields theory). However this text tries to be (as far as possible) self-contained: all the basic results we need will be stated and (when not proved) the reader will be referred to the literature.

Computational security is the aim of most modern cryptographic constructions. The security of modern criptographic schemes stems from the assumption that an adversary is not able to *efficiently* solve certain mathematical problems. That is to say, those schemes *can* be broken given enough time and computational power, but they can be considered *practically* unbreakable. Here we review the most common mathematical problems underlying modern cryptosystems and study the computational complexity related to the best known algorithms known to break them. The structure of the document is as follows.

In the first part (chapters 1-4) we study the basic mathematical tools needed to deal with the above problems. The second part shows how to use what we have learned in the first part to solve three foundamental tasks, namely primality proving, integer factoring and discrete logarithms evaluation. The last chapter deals with two explicit constructions of pairings using elliptic curves. The detailed content of each chapter follows below.

Chapter 1 is dedicated to introductory facts about elliptic curve over a generic field $\varkappa$; in particular we discuss projective coordinates and the group law.

In chapter 2 we shift our attention on elliptic curves over a finite field; after extending the basic results of chapter 1 to elliptic curves of the form $E(\mathbb{Z}_p)$ we deal with computational complexity considerations and morphisms. These ingredients will be central to prove Hasse's bound on $\#E(\mathbb{Z}_p)$; lastly we deal with isomorphisms and the j-invariant.

Chapter 3 is about elliptic curves over the field of complex numbers $\mathbb{C}$. Here we study the structure of lattices, orders and double-periodic

[1] See `http://www.mat.uniroma2.it/~eal/cr2008.html`.

functions like Weierstrass' $\wp(z)$; then we define elliptic curves with complex multiplication and examine their properties.

In chapter 4 we deal with the problem of evaluating $\#E(\mathbb{Z}_p)$; we present (in detail) three algorithms, namely Shanks' baby-steps and giant-steps, Schoof's algorithm and Atkin's algorithm and give an estimate of their computational cost.

Chapter 5 deals with the task of primality proving. First of all we introduce the Miller-Rabin test, then we deal with primality proving for numbers of special form, like Fermat's and Mersenne's numbers. Finally we give the details of the Pocklington's test (and its extension on elliptic curves by Goldwasser-Kilian and Atkin) and the AKS primality proving test, that are the most efficient algorithms known.

Chapter 6 is about integer factoring; we review the Pollard ρ algorithm, Pollard's $p-1$ method and its extension to elliptic curves by Lenstra (ECM), the quadratic sieve (QS) and the number field sieve (NFS).

In chapter 7 we discuss the discrete logarithm problem; after a brief introduction we explain the baby-steps and giant-steps algorithm and the index calculus method.

Finally chapter 8 is about pairings and its implementation via elliptic curves (Weil and Tate pairings in particular).

The appendices contain some general fact we use in the notes and some in-depths examinations, namely (a weak form of) the prime number theorem, the basic steps of euclidean algorithm (and its extended version) with a focus on estimating its computational complexity, some properties of Euler's φ-function and the link between Hasse's theorem and the Riemann hypothesis.

No book is ever free from error or incapable of being improved. I would be delighted to receive comments, good or bad, and corrections. Just send mail to me at:

`venturi@infocom.uniroma1.it`

Acknowledgements: I would like to thank Renè for the time he spent reading these notes and for his suggestions, corrections and (above all) teachings, and Filippo Nuccio for his explanations and patience. More people like them would make the university a wonderful place to work in.

Rome, June 2009 D. Venturi

Contents

CHAPTER 1

Elliptic Curves: Basic Facts

Contents

1.1. Elliptic Curves in the Projective Space

DEFINITION 1.1 (Elliptic curve over a field $\varkappa$). Let $\varkappa$ be a field with characteristic[1] $char(\varkappa) \neq 2, 3$. An elliptic curve over $\varkappa$, denoted $E(\varkappa)$, is defined by an equation of the form:

$$E : Y^2 = X^3 + AX + B \qquad A, B \in \varkappa. \tag{1.1}$$

The curve E is said to be *non-singular* if it has no double-zeroes, i. e. if the discriminant $\Delta_E = 4A^3 + 27B^2 \neq 0$ in $\varkappa$. □

If we take $\varkappa = \mathbb{R}$ we can trace the curve, as it is shown in figure 1.1; the curve E is symmetric and it has either one or three real zeroes.

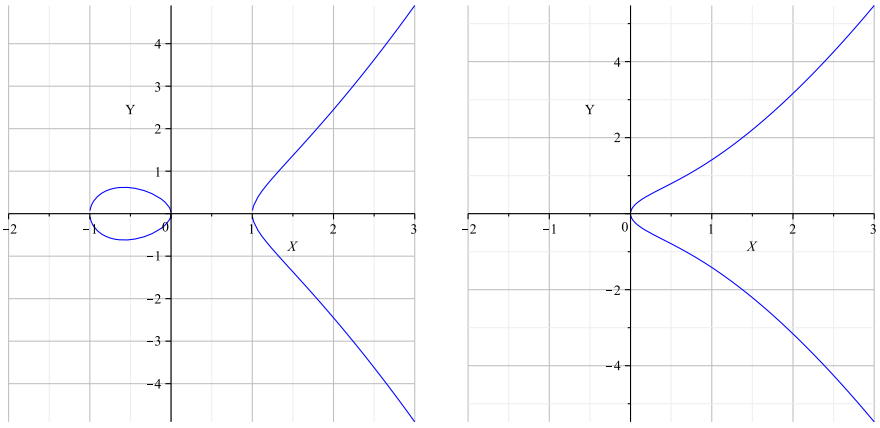
Now we embed the curve E into the *projective plane*; as it will be clear later this step is crucial for the group law to hold, because the point at infinity will play the role of the identity element. The concept of projective plane was introduced during the XVI century as a mean to model the space saw by the human's eye; from the geometric point of view it has some interesting properties, because, for example, there are less special cases (e. g. two lines will always intersect) and it is possible to explain a lot of deep concepts in a more summary and elegant way.

We start with the definition:

[1] For a field $\varkappa$ with multiplicative identity 1, consider the numbers $2 = 1+1$, $3 = 1+1+1$, $4 = 1+1+1+1$, etc. Either these numbers are all different, in which case we say that $\varkappa$ has characteristic $char(\varkappa) = 0$, or two of them will be equal. In the latter case, it is straightforward to show that, for some number p, we have

$$\underbrace{1 + 1 + 1 + \cdots + 1}_{p \text{ times}} = 0.$$

If p is chosen to be as small as possible, then p will be a prime, and we say that $\varkappa$ has characteristic $char(\varkappa) = p$.



(A) $Y^2 = X^3 - X$. (B) $Y^2 = X^3 + X$.

FIGURE 1.1. Two elliptic curves over $\varkappa = \mathbb{R}$.

DEFINITION 1.2 (Projective space). The n-dimensional projective space on an arbitrary field $\varkappa$ is defined as the set of straight lines passing for the origin in $\varkappa^{n+1}$, i. e.

$$\mathbb{P}^n(\varkappa) = (\varkappa^{n+1} \setminus \{0\})/\varrho,$$

where ϱ is the equivalence relation that identifies two points if and only if they belong to the same line passing through the origin, i. e. if and only if they are multiple one of the other:

$$P \,\varrho\, Q \quad \Leftrightarrow \quad P = \lambda Q \qquad \text{with } \lambda \in \varkappa.$$

□

EXAMPLE 1.1. The points of $\mathbb{R}^3$, $P = (1, 2, -3)$ and $Q = (2, 4, -6)$ are multiples, with $\lambda = 2$ and then they locate the same projective point. □

Hence every point in the n-dimensional projective space is an equivalence class of points in $\varkappa^{n+1}$, denoted $[x_0 : x_1 : \cdots : x_n]$; this expression defines the *homogeneous coordinates* of the point. Two vectors locate the same point (i. e. the same class) when $[x_0 : \cdots : x_n] = [y_0 : \cdots : y_n]$, if and only if $\exists\, \lambda \in \varkappa$ such that $y_i = \lambda x_i$, $\forall\, i = 0, \ldots, n$. By the use of homogeneous coordinates we can explain the original definition of projective space, as the affine plane plus the points at infinity. Let $\mathcal{S}$ be the set of points $[x_0 : \cdots : x_n]$ such that $x_0 \neq 0$; we can write every point in $\mathcal{S}$ as $[1 : x_1 : \cdots : x_n]$ in a unique way; hence by the function $\Phi : [1 : x_1 : \cdots : x_n] \mapsto (x_1 \ldots, x_n)$ we define a bijection between $\mathcal{S}$ and the affine space $\varkappa^n$. The points at infinity are the points of $\mathbb{P}^n(\varkappa)$ that do not belong to $\mathcal{S}$, i. e. all the points of the form $[0 : x_1 : \cdots : x_n]$ and the function $\Phi' : [0 : x_1 : \cdots : x_n] \mapsto [x_1 : \cdots : x_n]$ defines a bijection between the points at infinity and the projective space $\mathbb{P}^{n-1}(\varkappa)$. Therefore, for example, the points at infinity in the *projective plane* form a

projective line said *line at infinity*; in the multi-dimensional case we speak of *improper hyperplane*.

Example 1.2. Every point of the projective line $\mathbb{P}^1(\varkappa)$ is of the form $[x_0 : x_1] \neq [0 : 0]$. If $x_1 \neq 0$, we can express the same point as $\left[\frac{x_0}{x_1} : 1\right]$; if $x_1 = 0$ the other value x_0 must be non-zero and we can write the same point as $\left[\frac{x_0}{x_0} : \frac{0}{x_0}\right] = [1 : 0]$. Hence:

$$\mathbb{P}^1(\varkappa) = \{[a : 1] : \ a \in \varkappa\} \cup \{[1 : 0]\} = \mathbb{A}^1 \cup \infty,$$

i. e. $\mathbb{P}^1(\varkappa)$ is the direct sum of the affine space and ∞ (the *point at infinity*). In the same way, every point of the projective plane $\mathbb{P}^2(\varkappa)$ is described by a triple $[x_0 : x_1 : x_2]$ not identically null. Then:

$$\begin{aligned}\mathbb{P}^2(\varkappa) &= \left\{[x : y : 1] : (x, y) \in \varkappa^2\right\} \cup \left\{[x : y : 0] : \ (x, y) \in \mathbb{P}^1(\varkappa)\right\} \\ &= \mathbb{A}^2 \cup r_\infty,\end{aligned}$$

where r_∞ is the *line at infinity*. □

Therefore, to embed the curve E into the projective plane, means to compute:

$$E(\varkappa) \cap \mathbb{P}^2(\varkappa) = \left(E(\varkappa) \cap \mathbb{A}^2\right) \cup \left(E(\varkappa) \cap r_\infty\right). \tag{1.2}$$

The homogeneous equation corresponding to (1.1) is $Y^2Z = X^3 + AXZ^2 + BZ^3$ and if $Z \neq 0$ we have:

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^2 + A\left(\frac{X}{Z}\right) + B,$$

so that the points of the form $\left(\frac{x}{z} : \frac{y}{z} : 1\right)$ represent the first term of equation (1.2). Instead when $Z = 0$, it must be $X = 0$ and $Y \neq 0$ and we can normalize to obtain the point at infinity $\infty = (\infty, \infty) = (0 : 1 : 0)$ that represents the second term of equation (1.2).

1.2. The Group Law

Now we want to define an operation on E such that, given two points of $E(\varkappa)$, it returns another point of $E(\varkappa)$. Let us start with two points on $E(\varkappa)$, $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, and take the line r passing through these points; as it is shown in figure 1.2 the line r intersect the curve in a further point $S = (x_S, y_S)$; let $R = (x_R, y_R) = (x_S, -y_S)$ the symmetric of the point S with respect to the x-axis. We define the sum of the points P and Q as,

$$P + Q \triangleq R.$$

More formally let $r : Y = \lambda\ X + \mu$ be the equation of the line r, if we compute the intersection with the curve we obtain:

$$\begin{aligned}&(\lambda X + \mu)^2 = X^3 + A\ X + B \quad \Rightarrow \quad X^3 - \lambda^2 X^2 + (A - 2\mu\lambda)X + B - \mu^2 = 0 \\ &\Rightarrow \quad X^3 - \lambda^2 X^2 + (A - 2\mu\lambda)X + B - \mu^2 = (X - x_P)(X - x_Q)(X - x_S) = 0.\end{aligned}$$

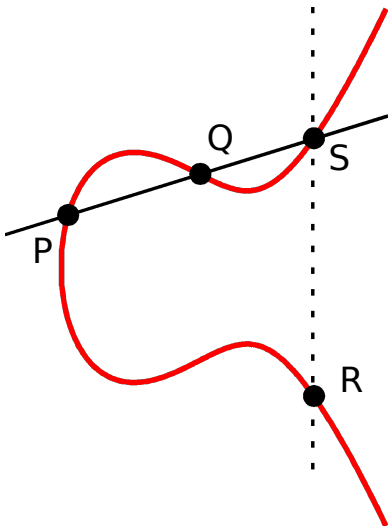


FIGURE 1.2. The sum of two points P and Q on an elliptic curve.

Evaluating the second member we see that the coefficient of X^2 is $-(x_P + x_Q + x_S)$, so that it must be $\lambda^2 = x_P + x_Q + x_S$, i. e.

$$x_S = -x_P - x_Q + \lambda^2 = x_R.$$

Further we can always express y_R as:

$$\lambda = \frac{y_S - y_P}{x_S - x_P} = \frac{-y_R - y_P}{x_R - x_P} \quad \Rightarrow \quad y_R = -y_P - (x_R - x_P)\lambda.$$

Now we have to discern three cases:

(1) $P \neq Q$. Hence simply:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}.$$

(2) $P = Q$. Now λ is the slope of the line tangent at the curve E in $P = Q = (x_P, y_P)$. Then:

$$Y = \sqrt{X^3 + Ax + B} \quad \Rightarrow \quad \frac{dY}{dX} = \frac{3X^2 + A}{2\sqrt{X^3 + AX + B}} = \frac{3X^2 + A}{2Y}$$

$$\Rightarrow \quad \lambda = \frac{3x_P^2 + A}{2y_P}.$$

(3) $P = -Q$. We ask that $P + Q = P - P \triangleq \infty$.

To sum up, we have introduced an operation that given two points on the curve E returns another point of E; the definition is as follow:

DEFINITION 1.3 (The Group Law). Let $E(\varkappa)$ be an elliptic curve $E : Y^2 = X^3 + AX + B$ over the field $\varkappa$, and $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ two points

of E different from the point at infinity. We define $P + Q = R = (x_R, y_R)$ as follows:

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & \text{if } P \neq Q \\ \dfrac{3x_P^2 + A}{2y_P} & \text{if } P = Q \end{cases}$$
$$x_R = -x_P - x_Q + \lambda^2$$
$$y_R = -y_P - (x_R - x_P)\lambda.$$

In the special case $P = -Q$ we take $P + Q = \infty$. □

Let us apply definition 1.3 in a couple of examples.

Example 1.3. Let $E : Y^2 = X^3 + X + 1$, $\varkappa = \mathbb{R}$ and $P = (0, 1)$. First of all $\Delta = 4A^3 + 27B^2 = 31 \neq 0$ so that E is non-singular and it is easy to check that P is indeed a point of E. We evaluate $R = P + P$:

$$\begin{aligned} \lambda &= \frac{3x_P^2 + A}{2y_P} = \frac{0+1}{2} = \frac{1}{2} \\ x_R &= -x_P - x_P + \lambda^2 = \frac{1}{4} \\ y_R &= -y_P - (x_R - x_P)\lambda = -1 - \left(-\frac{1}{4} - 0\right)\frac{1}{2} = -\frac{9}{8} \\ \Rightarrow \quad P + P &= R = \left(\frac{1}{4}, -\frac{9}{8}\right), \end{aligned}$$

and it is straightforward to check that $R \in E(\mathbb{R})$. □

Example 1.4. Let $E : Y^2 = X^3 - X + 1$, $\varkappa = \mathbb{R}$, $P = (1, 1)$ and $Q = (0, 1)$. We compute $R = P + P$:

$$\begin{aligned} \lambda &= \frac{y_Q - y_P}{x_Q - x_P} = 0 \\ x_R &= -1 \\ y_R &= -1 \\ \Rightarrow \quad P + Q &= R = (-1, -1), \end{aligned}$$

and it is straightforward to check that $R \in E(\mathbb{R})$. □

Example 1.5. Let $E : Y^2 = X^3 - X + 1$ be a non-singular elliptic curve over a field $\varkappa$, $P = (x_P, 0) \in E(\varkappa)$ and $Q = P$. As $y_P = 0$ and $Q = P$ we have also $P = Q = -P$ and then $P + Q = \infty$. □

Example 1.6. Let $E : Y^2 = X^3 + 1$, $\varkappa = \mathbb{R}$ and $P = (0,1) \in E(\mathbb{R})$. We compute $3P = P + P + P$ as follows:

$$\begin{aligned} \lambda &= \frac{0+0}{2} = 0 \\ x_{2P} &= -0 - 0 + \lambda^2 = 0 \\ y_{2P} &= -1 - (0-0) = -1 \\ \Rightarrow \quad 2P &= R = (0,-1) = -P. \end{aligned}$$

Hence $3P = 2P + P = P - P = \infty$. So we have shown that P has order 3. □

The surprising fact we are going to discuss now is that the set:

$$E(\varkappa) = \left\{(x,y) \in \varkappa \times \varkappa : \ y^2 = x^3 + A\,x + B\right\} \cup \{\infty\},$$

of the points of $E(\varkappa)$ with the point at infinity is an algebraic[2] *group*, $(E(\varkappa), +)$ with the sum operation of definition 1.3.

The *commutativity* is obvious, either taking a look at the formulas or observing that the line through P and Q is the same through Q and P. The existence of an identity element (i. e. the point ∞) is assured by definition; also the inverse of a point P, namely $-P$, there exists: it suffices to take the reflection of P across the x-axis. Finally we need to prove associativity, and this is the hardest task. One could check the validity of associativity simply proceeding case by case[**51**] and using definition 1.3, even if it is quite tedious. Here we prefer to use a little bit of *algebraic geometry*, but we postpone the proof to section 8.3.

[2]In algebraic geometry, an *algebraic group* (or group variety) is a group that is an algebraic variety, such that the multiplication and inverse are given by regular functions on the variety. Recall that an *algebraic variety* is typically defined as a (finite or infinite) set of points where a polynomial or set of polynomials attain a value of zero. By the way, since our principal purpose is to deal with algebraic varieties defined over finite fields, it is better to identify them with the equations, if we don't want to loose too much information. Algebraic varieties are one of the central objects of study in classical (and to some extent, modern) algebraic geometry.

CHAPTER 2

Elliptic Curves over $\mathbb{Z}_p$

Contents

2.1. Introduction

The major applications of elliptic curves theory in cryptography deal with elliptic curves defined over a finite field like $\varkappa = \mathbb{Z}_p$, where p is a prime. We can adapt the definition given in the previous chapter and state:

Definition 2.1 (Elliptic curve over $\mathbb{Z}_p$). Let[1] $p \neq 2, 3$. An elliptic curve over $\mathbb{Z}_p$, $E(\mathbb{Z}_p)$, is defined by an equation of the form:

$$E : Y^2 \equiv X^3 + AX + B \pmod{p} \qquad A, B \in \mathbb{Z}_p.$$

The curve E is said to be *non-singular* if it has no double zeroes, i. e. if the discriminant $\Delta_E = 4A^3 + 27B^2 \not\equiv 0 \pmod{p}$. □

We can also adapt definition 1.3 of sum, for $\varkappa = \mathbb{Z}_p$:

Definition 2.2 (Group Law for $E(\mathbb{Z}_p)$). Let $E(\mathbb{Z}_p)$ be an elliptic curve $E : Y^2 \equiv X^3 + AX + B \pmod{p}$ over the field $\mathbb{Z}_p$, and $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ two points of E different from the point at infinity. We define $P + Q = R = (x_R, y_R)$ as follows:

$$\lambda \equiv \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} \pmod{p} & \text{if } P \neq Q \\ \dfrac{3x_P^2 + A}{2y_P} \pmod{p} & \text{if } P = Q \end{cases} \tag{2.1}$$

$$x_R \equiv -x_P - x_Q + \lambda^2 \pmod{p}$$
$$y_R \equiv -y_P - (x_R - x_P)\lambda \pmod{p}.$$

In the special case $P = -Q$ we take $P + Q = \infty$. □

[1] We will always consider the case $p \neq 2, 3$ in this note.

As we have seen in the previous chapter, the set:

$$E(\mathbb{Z}_p) = \left\{(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p : y^2 \equiv x^3 + A\,x + B \pmod{p}\right\} \cup \{\infty\},$$

has the structure of an abelian group with the sum operation of definition 2.2; furthermore now the group is finite.

EXAMPLE 2.1. Let $E: Y^2 \equiv X^3 + X + 2 \pmod{p}$ and $p = 5$, we determine $E(\mathbb{Z}_5)$. If p is small it is possible to build-up a table with all the values of $\mathbb{Z}_p$ (see table 2.1). Once you have computed $x^3 + x + 2$, you have to take the

x	x^3	$x^3 + x + 2$	y
0	0	2	no
1	1	4	± 2
2	3	2	no
3	2	2	no
4	4	0	0

TABLE 2.1. Points of $E(\mathbb{Z}_5)$.

square root of the result, i. e. we have to decide if the result is a quadratic residue modulo p or not. Since the only quadratic residues of $\mathbb{Z}_5$ are $0, 1$ and 4 we have determined:

$$E(\mathbb{Z}_5) = \{\infty, (4, 0), (1, 2), (1, -2)\},$$

and $\#E(\mathbb{Z}_5) = 4$. Now there are only two possible structures[**10**] for a group of order 4: it could be a cyclic group or the Klein group (i. e. $E(\mathbb{Z}_5) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$); the Klein group is the smallest non-cyclic group and all of its elements have order 2. Thus it suffices to take a point $P \in E(\mathbb{Z}_5)$ and check if it has order 2 to determine the structure of the group $E(\mathbb{Z}_5)$; let $P = (1, 2)$, we compute $P + P = 2P$:

$$\begin{aligned} \lambda &\equiv \frac{3 \cdot 1^2 + 1}{2 \cdot 2} \equiv 1 \pmod{5} \\ x_{2P} &\equiv -1 \equiv 4 \pmod{5} \\ y_{2P} &\equiv 0 \pmod{5} \\ \Rightarrow \quad 2P &= (4, 0) \neq \infty. \end{aligned}$$

Then $E(\mathbb{Z}_5)$ is not the Klein group, but it is cyclic and P is a generator, because, as it is easy to check, we have: $(4, 0) = 2P$, $(1, -2) = 3P$, $4P = \infty$. □

On the basis of the previous example, we define *torsion points*[2].

[2]We give the definition for $\varkappa = \mathbb{Z}_p$, but it also holds for a generic field $\varkappa$ with algebraic closure $\overline{\varkappa}$. We recall that the algebraic closure of a field $\varkappa$, is the minimal algebraically closed field $\overline{\varkappa}$ that contains $\varkappa$. An algebraically closed field is such that each polynomial with coefficients on it has all zeroes that are elements of the field itself.

Definition 2.3 (Torsion points). Let E be an elliptic curve over $\mathbb{Z}_p$ and n a positive integer. The n-torsion of E is the set:

$$E[n] \triangleq \left\{P \in E(\overline{\mathbb{Z}}_p) : \ nP = \infty\right\},$$

where $\overline{\mathbb{Z}}_p$ is the algebraic closure[3] of $\mathbb{Z}_p$. □

Let us start with $n = 2$, i. e. with the points of order two. Let $E : \ Y^2 = X^3 + AX + B$ an elliptic curve over $\mathbb{Z}_p$ with $p \neq 2, 3$; a point P of order two is such that $P + P = \infty$, i. e. $P = -P$. If $P = (x_P, y_P)$ it should be $y_P = -y_P \Rightarrow 2y_P = 0$. As $p \neq 2$ we can state $y_P = 0$ and than:

$$E[2] = \left\{(\alpha, 0) : \ \alpha^3 + A\alpha + B \equiv 0 \pmod{p}\right\} \cup \{\infty\}, \tag{2.2}$$

and one can check easily that it is a subgroup of $E(\mathbb{Z}_p)$. It is quite obvious that the order of $E[2]$ is less than or equal to 4; in particular one can show that $E[2] \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Let now be $n = 3$ and we look for points P of order three, i. e. points such that $P + P + P = \infty$. Thus it should be $P + P = -P = (x_P, -y_P)$ or:

$$(-x_P - x_P + \lambda^2, y_{2P}) = (x_P, -y_P) \quad \text{with } \lambda = \frac{3x_P^2 + A}{2y_P}$$

$$\Rightarrow \quad -2x_P + \lambda^2 \equiv x_P \pmod{p}.$$

Hence:

$$\begin{aligned} & 3x_P \equiv \lambda^2 \equiv \frac{3x_P^2 + A}{2y_P} \pmod{p} \\ \Rightarrow \quad & 12x_P y_P \equiv (3x_P^2 + A)^2 \pmod{p} \\ \Rightarrow \quad & 12x_P(x_P^3 + Ax_P + B) \equiv (3x_P^2 + A)^2 \pmod{p} \\ \Rightarrow \quad & 3x_P^4 + 6Ax_P^2 + 12Bx_P - A^2 \equiv 0 \pmod{p}, \end{aligned} \tag{2.3}$$

and we can state:

$$E[3] = \left\{(\alpha, \beta) : \ 3\alpha^4 + 6A\alpha^2 + 12B\alpha - A^2 = 0 \equiv 0 \pmod{p}\right\} \cup \{\infty\}. \tag{2.4}$$

As each value α corresponds to two values of β, namely $\pm\beta$, we have $\#E[3] \leq 4 \times 2 + 1 = 9$. For what concerns the structure of $E[3]$ we recall a theorem from group algebra[**10**]:

Theorem 2.1 (Cauchy). *Let $\mathbb{G}$ be a group of order n and let p be a prime such that $p|n$. Then $\mathbb{G}$ has at least one element of order p.* □

Since the points of $E[3]$ have either order 3 or 1 (if $(\alpha, \beta) = \infty$), we can state that the order of $E[3]$ is either 1, or 3 or 9. Having a look at equation (2.3) we observe that the discriminant of the polynomial is $-6912(4A^3 + 27B^2)^2$,

[3] $\overline{\mathbb{Z}}_p = \bigoplus_n \mathbb{F}_{p^n}$. Since it is an algebraic closure each zero of a polynomial $f(X) \in \mathbb{Z}_p[X]$ is indeed an element of $\overline{\mathbb{Z}}_p$.

which is non-zero if the curve is non-singular. Thus we have 4 distinct roots and $E[3] \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ if $p \neq 3$.

The general situation is summarized by the following theorem[**51**]:

THEOREM 2.2 (Structure of n-Torsion). *Let E be an elliptic curve over a field $\varkappa$ and let n be a positive integer. If the characteristic of $\varkappa$ does not divide n, or is 0, then:*

$$E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_n.$$

If the characteristic of $\varkappa$ is $p > 0$ and $p|n$, write $n = p^r s$ with $p \nmid s$; then:

$$E[n] \simeq \mathbb{Z}_s \times \mathbb{Z}_s \quad \text{or} \quad E[n] \simeq \mathbb{Z}_n \times \mathbb{Z}_s.$$

□

EXAMPLE 2.2. Let $p = 7$ and $Y^2 \equiv X^3 + 2 \pmod{p}$; we compute the points of order three using equation (2.3):

$$\begin{aligned} 3\alpha^4 + 24\alpha \equiv 0 \pmod 7 &\xrightarrow{\gcd(3,7)=1} \alpha^4 + 8\alpha \equiv 0 \pmod 7 \\ &\Rightarrow \alpha^4 + \alpha \equiv 0 \pmod 7 \\ &\Rightarrow \alpha(\alpha^3 + 1) \equiv 0 \pmod 7. \end{aligned}$$

Since p is small it is quite simple to find the solutions: $\alpha = 0, -1, 3, -2$; once you know the values of α you can compute $\beta^2 \equiv \alpha^3 + 2 \pmod 7$ and, if it is possible, take the square root. It is easy to see that:

$$E[3] = \{(0, \pm 3), (-1, \pm 1), (-2, \pm 1), (3, \pm 1), \infty\}.$$

We can also write all the points of $E(\mathbb{Z}_7)$ (see table 2.2). We recall a theorem

x	x^3	$x^3 + 2$	y
0	0	2	±3
1	1	3	no
2	1	3	no
3	−1	1	±1
−3	1	3	no
−2	−1	1	±1
−1	−1	1	±1

TABLE 2.2. Points of $E(\mathbb{Z}_7)$.

from algebra[**10**]:

THEOREM 2.3. *If $\mathbb{G}$ is a group of order p^2 with p a prime, then $\mathbb{G} \simeq \mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{G} \simeq \mathbb{Z}_{p^2}$.* □

Since there are no elements of order 9 we can conclude that $E(\mathbb{Z}_7) \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$, as it is stated in theorem 2.2. □

2.2. Computational Complexity

In this section we deal with computational cost associated with representation and manipulation of elliptic curves. To define an elliptic curve is equivalent to choose A and B in $\mathbb{Z}_p$, then the memory size requirement[4] is $2\log p = O(logp)$, just like the memory space associated with a point P (two coordinates). For what concerns the addition, the computational complexity is dominated by the division in the computation of λ, thus we have $O(\log^3 p)$ if we refer to the euclidean algorithm (see appendix B); then the running time is polynomial[5]. It is possible to use projective coordinates; if this is the case the addition on $E(\mathbb{Z}_p)$ is simpler since we do not need to divide, but it is harder to check for an equality since two points are equal if they are multiple one of the other, as we have seen in chapter 1.

Now we want to define an algorithm to evaluate a point P of $E(\mathbb{Z}_p)$; the simplest (but inefficient) method is to try random points P and to verify whether $P \in E(\mathbb{Z}_p)$ or not. A good idea is to choose a value $x \in \mathbb{Z}_p$, to compute $\alpha \equiv x^3 + Ax + B \pmod p$ and to *hope* that α is a *quadratic residue* modulo p. We need a lemma:

LEMMA 2.4. *Let p be an odd prime.*

(1) *$x \in \mathbb{Z}_p$ is a quadratic residue modulo p if and only if $x^{\frac{p-1}{2}} \equiv 1 \pmod p$ (Euler's criterion).*
(2) *There are exactly $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residues in $\mathbb{Z}_p$.*

PROOF. (1)($\Rightarrow$). If $x \in \mathbb{Z}_p$ is a quadratic residue modulo p, i. e. if $x \equiv y^2 \pmod p$ for some y, we can write $y^{p-1} \equiv 1 \pmod p$ by[6] Fermat's little

[4] We recall the definition of O notation.

DEFINITION 2.4. Suppose $f(X)$ and $g(X)$ are two functions defined on some subset of the real numbers. We say

$$f(X) = O(g(X)) \text{ as } X \to \infty,$$

if and only if there exists a positive real number M and a real number x_0 such that $|f(x)| \leq M|g(x)|$, for each $x > x_0$. □

[5] In computational complexity theory, polynomial time refers to the computation time of an algorithm (with n as input) where the running-time, is no greater than a polynomial function of the input size, i. e. $O(\log(n))$.

[6] We recall this important result from elementary number theory; see also [**29**].

THEOREM 2.5 (Euler's Theorem). *Let n be a natural number; then for each $a \in \mathbb{Z}_n^*$ we can write:*

$$a^{\varphi(n)} \equiv 1 \pmod n,$$

being $\varphi(\cdot)$ the Euler's totient function (see appendix C). □

Letting $n = p$ to be a prime number in Euler's theorem yields

$$a^{p-1} \equiv 1 \pmod p,$$

theorem, hence:

$$y^{p-1} \equiv (y^2)^{\frac{p-1}{2}} \equiv 1 \equiv x^{\frac{p-1}{2}} \pmod{p}.$$

(2). Let ϕ be the map which takes $x \in \mathbb{Z}_p$ and computes $x^2 \mod p$:

$$\begin{aligned} \phi : \mathbb{Z}_p^* &\longleftrightarrow \mathbb{Z}_p^* \\ x &\longmapsto x^2, \end{aligned}$$

it is easy to see that ϕ is a group *homomorphism*[7]. Note that, since there are no non-trivial square roots of 1 modulo p (see lemma 5.1 for a proof), $Ker(\phi) = \{\pm 1\}$ and thus the assertion follows from the fundamental theorem of ring isomorphisms[8]:

$$\begin{array}{ccc} \mathbb{Z}_p^* & \xrightarrow{\phi} & \mathbb{Z}_p^* \\ \downarrow{\scriptstyle \pi} & \nearrow & \\ \mathbb{Z}_p^*/Ker(\phi) & & \end{array} \qquad \Rightarrow \#Im(\phi) = \frac{\#\mathbb{Z}_p^*}{\#Ker(\phi)} = \frac{p-1}{2}.$$

Hence there are exactly $\frac{p-1}{2}$ quadratic residues modulo p (and thus $\frac{p-1}{2}$ quadratic non-residues).

(1)($\Leftarrow$). We know that if $x \in \mathbb{Z}_p$ is a quadratic residue modulo p it must be $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, then:

$$\left(\mathbb{Z}_p^*\right)^2 \subset \left\{\text{Zeroes of the polynomial } X^{\frac{p-1}{2}} - 1 \bmod p\right\}.$$

We recall that a polynomial $f(X) \in \varkappa[X]$ (where $\varkappa$ is a field), has at most $deg(f)$ zeroes in $\varkappa$; thus the order of the second set in the previous equation

---

for each element $a \in \mathbb{Z}_p^*$. This last result is also known as *Fermat's little theorem*, since it was proved independently by Fermat.

[7] In abstract algebra, a homomorphism is a structure-preserving map between two algebraic structures (such as groups, rings, or vector spaces). See [**10**] for further details. Thus, for example, a ring homomorphism is a function between two rings which respects the operations of addition and multiplication. More precisely, if $(\mathcal{R}, +, \cdot)$ and $(\mathcal{S}, +, \cdot)$ are rings, then a ring homomorphism is a function $\phi : \mathcal{R} \to \mathcal{S}$ such that

$$\begin{aligned} \phi(a+b) &= \phi(a) + \phi(b) \\ \phi(a \cdot b) &= \phi(a) \cdot \phi(b), \end{aligned}$$

for each $a, b \in \mathcal{R}$. When ϕ is surjective, injective or bijective we speak (respectively) about *epimorphism*, *monomorphism* or *isomorphism*.

[8] We recall the theorem:

Theorem 2.6 (Fundamental Homomorphism Theorem for Rings). *Let $\phi : \mathcal{R} \to \mathcal{S}$ be a ring homomorphism. Then the image of $\mathcal{R}$, namely $\phi(\mathcal{R}) = Im(\phi)$ is a subring of $\mathcal{S}$, $\mathcal{R}/Ker(\phi)$ is a ring and we can write $\mathcal{R}/Ker(\phi) \simeq Im(\phi)$.* □

is less than or equal to $\frac{p-1}{2}$. Instead, as we have just proven, the first set has order $\frac{p-1}{2}$ and thus:

$$\left(\mathbb{Z}_p^*\right)^2 = \left\{\text{Zeroes of the polynomial } X^{\frac{p-1}{2}} - 1 \bmod p\right\},$$

so that the two sets are indeed equal. □

Thus let $\alpha \equiv x^3 + Ax + B \pmod p$, we can easily check if it is a quadratic residue modulo p using lemma 2.4 by computing $\alpha^{\frac{p-1}{2}}$ and look up that the result is 1 modulo p; hence the computational cost[9] is:

$$O\left(\log\left(\tfrac{p-1}{2}\right)\log^2(p)\right) = O(\log^3 p),$$

which is polynomial. Therefore now the problem is, given an element $\alpha \in \mathbb{Z}_p^2$, to compute the square root of α modulo p; this is an open problem, but a solution exists assuming the *Generalized Riemann Hypothesis* (GRH[10]). Nevertheless this problem is solvable in practice; here we present two solutions: the Cantor-Zassenhaus algorithm and the Tonelli-Shanks algorithm.

Let us consider the ring $\mathbb{Z}_p[X]$, we know by Fermat's little theorem that $x^{p-1} \equiv 1 \pmod p$, $\forall x \in \mathbb{Z}_p^*$, i. e.:

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Hence each $x \in \mathbb{Z}_p^*$ is either a zero of $X^{\frac{p-1}{2}} - 1$ (and then it is a quadratic residue modulo p) or a zero of $X^{\frac{p-1}{2}} + 1$ (and then it is a quadratic non-residue modulo p); furthermore, by lemma 2.4 there are $\frac{p-1}{2}$ quadratic residues and $\frac{p-1}{2}$ quadratic non-residue in $\mathbb{Z}_p^*$.

Example 2.3. Let $p = 7$ and consider $\mathbb{Z}_7$; you can check that $\{1, 2, 4\}$ are zeroes of $X^3 - 1$ and $\{3, 5, 6\}$ are zeroes of $X^3 + 1$. □

---

[9] Recall that the computational complexity associated with multiplication and division modulo an integer n is $O(\log^\mu(n))$, with $\mu = 2$ when we use standard[**48**] multiplication techniques and $\mu = 1 + \epsilon$ by employing fast[**7**] multiplication techniques. *Exponentiating by squaring* is an algorithm used for the fast computation of large integer powers of a number. It is also known as the *square-and-multiply* algorithm or *binary exponentiation*. In additive groups the appropriate name is *double-and-add* algorithm; see also [**48**]. The key idea is to write the binary expansion of the exponent, so that

$$x^e \bmod n = x^{\sum_{i=0}^{s-1} e_i 2^i} \bmod n = \prod_{i=0}^{s-1}\left(x^{2^i}\right)^{e_i} \bmod n = \left(\left(x^{e_{s-1}}\right)^2 x^{e_{s-2}}\right)^2 \ldots x^{e_0} \bmod n,$$

being $e = (e_{s-1}, e_{s-2}, \cdots, e_0)_2$, $e_i \in \mathbb{Z}_2$, the binary expansion of e. Hence we need (at most) $\log_2(e)$ modular multiplications and the computational cost is $O(\log(e)\log^\mu(n))$.

[10] The Riemann Hypothesis[**50, 16**] is one of the most important conjectures in mathematics. It is a statement about the zeroes of the Riemann zeta function (see appendix D). When the Riemann hypothesis is formulated for Dirichlet L-functions, it is known as the Generalized Riemann Hypothesis (GRH).

Note that computing $\sqrt{\alpha} = \pm\beta$ is equivalent to solve $X^2 - \alpha \equiv 0 \pmod{p}$, and thus:

$$\gcd\left(X^{\frac{p-1}{2}} - 1, X^2 - \alpha\right) =$$

$$= \begin{cases} 1 & \text{if } \pm\beta \text{ are both quadratic non-residues} \\ X^2 - \alpha & \text{if } \pm\beta \text{ are both quadratic residues} \\ X \pm \beta & \text{if either } \beta \text{ or } -\beta \text{ is a quadratic residue.} \end{cases}$$

If we are in the third case than we have found the square root of α, but this is not always the case. To solve this problem we consider the mapping:

$$\begin{aligned} \Theta : \ \mathbb{Z}_p^* &\longleftrightarrow \mathbb{Z}_p^* \\ x &\longmapsto x + i \qquad i \in \mathbb{Z}_{\geq 0}, \end{aligned}$$

which maps $X^2 - \alpha$ in $(X + i)^2 - \alpha$ whose zeroes are $\pm\beta - i$. Hence:

$$\gcd\left(X^{\frac{p-1}{2}} - 1, (X + i)^2 - \alpha\right) =$$

$$= \begin{cases} 1 & \text{if } \pm\beta - i \text{ are both quadratic non-residues} \\ X^2 - \alpha & \text{if } \pm\beta - i \text{ are both quadratic residues} \\ X \pm \beta - i & \text{if either } \beta - i \text{ or } -\beta - i \text{ is a quadratic residue.} \end{cases}$$

The key point is that the mapping given by Θ is a random mapping, and then by varying $i = 0, 1, 2, \ldots$, with high probability, after a finite number of steps, only one between $\pm\beta - i$ will be a quadratic residue modulo p and we will succeed in finding the square root $\sqrt{\alpha} = \pm\beta$. To reduce the computational cost:

$$\gcd(\varphi(X), \psi(X)) \quad \Rightarrow \quad O\left(\max(deg(\varphi), deg(\psi)) \log^2 p\right)$$

we refer to the euclidean algorithm (see appendix B).

Lemma 2.7. *Let $\varphi(X) = q(X)\psi(X) + r(X)$, with $deg(\varphi) > deg(\psi)$, than:*

$$\gcd(\varphi(X), \psi(X)) = \gcd(\psi(X), r(X))$$

Proof. In fact a polynomial $d(X)$ which is a common divisor of $\varphi(X)$ and $\psi(X)$, is also a common divisor of $r(X) = \varphi(X) - q(X)\psi(X)$; on the other hand a polynomial which is a common divisor of $\psi(X)$ and $r(X)$ is also a divisor of $\varphi(X) = q(X)\psi(X) + r(X)$. □

The previous lemma is telling us that we can execute all the computation in $\mathbb{Z}_p[X]/\left((X + i)^2 + \alpha\right) = \left\{a_1 X + a_0 : a_1, a_0 \in \mathbb{Z}_p\right\}$; the reduction costs $O(\log^3 p)$, just like the gcd evaluation and we obtain a total complexity of $O(\log^3 p)$, which is polynomial. The algorithm described above is a particular application of the (more general) *Cantor-Zassenhaus* algorithm, which is polynomial and probabilistic.

Another possibility is to use an algorithm due to A. Tonelli (Atti Accad. Lincei 1892) and D. Shanks (1970ies). The algorithm compute a square root

of a given square $a \in \mathbb{Z}_p^*$, being $p \geq 2$ a prime. For this we need to know a non-square $g \in \mathbb{Z}_p^*$. We write $p-1 = 2^m q$ with q odd and put $\zeta = g^q$. The number ζ is a generator of the 2-part of the cyclic group $\mathbb{Z}_p^*$. Putting

$$b = a^{\frac{q+1}{2}} \quad \text{and} \quad c = a^q,$$

we have

$$b^2 = ac \quad \text{with} \quad c \in \langle \zeta^2 \rangle.$$

If $c = 1$ we are done. If not, then we modify b, c and ζ as follows. Let $k, l \geq 0$ be the unique integers for which $c^2 = -1$ and $\zeta^2 = -1$ respectively. Since c is contained in the cyclic group generated by ζ^2 , we have $l > k$. Put

$$b \leftarrow b\zeta^{2^{l-k-1}}$$
$$c \leftarrow c\zeta^{2^{l-k}}$$
$$\zeta \leftarrow \zeta^{2^{l-k}}.$$

Then we still have $b^2 = ac$ and $c \in \langle \zeta^2 \rangle$. This follows from the fact that the new ζ has order 2^{k+1} , while the new ζ raised to the power $2k$ is equal to 1. Note that, in every step, the order of ζ and hence of c decreases. Eventually $c = 1$ and $b^2 = ac = a$ and we are done. The time needed to perform the computations is essentially equal to the time needed to compute a $p-1$-th power in $\mathbb{Z}_p^*$, i. e. it is bounded by $O(\log^3(p))$.

Example 2.4. Let $p = 400009$. Then $g = 19$ is a primitive root modulo p. We have $p - 1 = 400008 = 2^m q$ with $m = 3$ and $q = 50001$ and hence $\zeta = g^q = 284991$. We compute the square root of $a = 2$. We have $b = a^{\frac{q+1}{2}} = 357332$ and $c = a^q = 42676$. One checks that $b^2 = ac$ in $\mathbb{Z}_p^*$.

We make the first step. We have $c^2 = -1$ and $\zeta^4 = -1$. Therefore $k = 1$ and $l = 2$. We replace b by $b\zeta = 112747$ and c by $c\zeta^2 = -1$. We also replace ζ by $\zeta^2 = 42676$. One checks that $b^2 = ac$. Since $c \neq 1$ we make a second step. We have $c = -1$ and $\zeta^2 = -1$. Therefore $k = 0$ and $l = 1$. We replace b by $b\zeta = 282720$ and c by $c\zeta^2 = 1$. We also replace ζ by $\zeta^2 = -1$. This time $c = 1$ and $b^2 = a$. So we are done. □

Hence,

Corollary 2.8. *We have a polynomial probabilistic algorithm for computing a point $P \in E(\mathbb{Z}_p)$.* □

2.3. Morphisms

We recall that by Fermat's little theorem we have:

Proposition 2.9. *Let p be a prime, then:*

$$\mathbb{Z}_p = \left\{ x \in \overline{\mathbb{Z}}_p : \ x^p \equiv x \pmod{p} \right\}.$$

Proof. Let $\mathcal{S} = \left\{x \in \overline{\mathbb{Z}}_p : \ x^p \equiv x \pmod p\right\}$, Fermat's little theorem implies that $\mathbb{Z}_p \subset \mathcal{S}$, since $x^{p-1} \equiv 1 \pmod p$ is equivalent to $x^p \equiv x \pmod p$. On the other hand $\#\mathbb{Z}_p = p$ and $\#\mathcal{S}$ is equal to the number of solutions of $X^p - X \equiv 0 \pmod p$ in $\overline{\mathbb{Z}}_p$, i. e. $\#\mathcal{S} = p$ and thus the only possibility is $\mathbb{Z}_p = \mathcal{S}$. □

On the other hand lemma 2.4 gives us a criterion to check if an element $x \in \overline{\mathbb{Z}}_p$ is also an element of $\mathbb{Z}_p$. Consider the *Frobenius map*:

$$\begin{aligned} \sigma : \ \overline{\mathbb{Z}}_p &\to \overline{\mathbb{Z}}_p \\ x &\mapsto \sigma(x) = x^p; \end{aligned}$$

note that the Frobenius map is a group homomorphism, because:

$$\begin{aligned} \sigma(x+y) = (x+y)^p = x^p + \binom{p}{1} x^{p-1}y + \cdots + \binom{p}{p-1} xy^{p-1} + y^p = \\ = x^p + y^p = \sigma(x) + \sigma(y), \end{aligned}$$

thanks to the fact that $char(\overline{\mathbb{Z}}_p) = p$. Thus proposition 2.9 is equivalent to say that $x \in \overline{\mathbb{Z}}_p$ is an element of $\mathbb{Z}_p$ if and only if $\sigma(x) = x$. Take the group defined by:

$$E(\overline{\mathbb{Z}}_p) = \left\{(x,y) \in \overline{\mathbb{Z}}_p \times \overline{\mathbb{Z}}_p : \ y^2 \equiv x^3 + A\,x + B \pmod p\right\} \cup \{\infty\},$$

it is an infinte group and in particular $E(\mathbb{Z}_p) \subset E(\overline{\mathbb{Z}}_p)$. We give the important definition of morphism:

Definition 2.5 (Morphism or Isogeny). Let E_1 and E_2 be two elliptic curves:

$$E_1 : \ Y^2 = X^3 + A_1X + B_1 \qquad E_2 : \ Y^2 = X^3 + A_2X + B_2.$$

A *morphism* f is a map between the points of E_1 and the points of E_2:

$$\begin{aligned} f : \ E_1(\overline{\mathbb{Z}}_p) &\to E_2(\overline{\mathbb{Z}}_p) \\ (X,Y) &\mapsto \left(\frac{H_1(X,Y)}{H_2(X,Y)}, \frac{H_3(X,Y)}{H_4(X,Y)}\right) \\ \infty &\mapsto \infty, \end{aligned}$$

where H_i $(i = 1, \cdots, 4)$ are polynomials and $X, Y \in \overline{\mathbb{Z}}_p$. □

One can show that a morphism is a group homomorphism, i. e.[11] $f(P + Q) = f(P) + f(Q)$.

[11]The first addition takes place on the curve E_1, whereas the second one takes place on the curve E_2.

Example 2.5. The *identity* morphism:

$$\begin{aligned} id:\ E(\overline{\mathbb{Z}}_p) &\to E(\overline{\mathbb{Z}}_p) \\ (X,Y) &\mapsto (X,Y) \\ \infty &\mapsto \infty, \end{aligned}$$

where $X, Y \in \overline{\mathbb{Z}}_p$, is a trivial morphism. □

Example 2.6. The *inverse* morphism:

$$\begin{aligned} -id:\ E(\overline{\mathbb{Z}}_p) &\to E(\overline{\mathbb{Z}}_p) \\ (X,Y) &\mapsto (X,-Y) \\ \infty &\mapsto \infty, \end{aligned}$$

where $X, Y \in \overline{\mathbb{Z}}_p$, is another trivial morphism. □

Example 2.7. Let $E:\ Y^2 = X^3 - X$, we have $\Delta_E = 4A^3 + 27B^2 = -4$, so that the elliptic curve E is non-singular if $p \nmid 4$. Let $p = 5$, there exists an element $i \in \mathbb{Z}_5$ such that $i^2 \equiv -1 \pmod 5$, namely $i = -2$; let f be the map:

$$\begin{aligned} f:\ E(\overline{\mathbb{Z}}_5) &\to E(\overline{\mathbb{Z}}_5) \\ (X,Y) &\mapsto (-X, iY) \\ \infty &\mapsto \infty, \end{aligned}$$

where $X, Y \in \overline{\mathbb{Z}}_p$. It should be clear that f is a morphism only if the destination point is indeed a point of $E(\overline{\mathbb{Z}}_p)$; we have:

$$(iY^2) = -X^3 - (-X) \quad \Rightarrow \quad -Y^2 = -X^3 + X,$$

that is the equation of E. Thus f is a morphism; moreover applying the morphism f twice yields:

$$\begin{aligned} &E(\overline{\mathbb{Z}}_5) \xrightarrow{f} E(\overline{\mathbb{Z}}_5) \xrightarrow{f} E(\overline{\mathbb{Z}}_5) \\ &(X,Y) \mapsto (-X, iY) \mapsto (X, -Y), \end{aligned}$$

so that $f \circ f = -id$. □

Example 2.8. Point doubling is a morphism:

$$\begin{aligned} f:\ &E(\overline{\mathbb{Z}}_p) \to E(\overline{\mathbb{Z}}_p) \\ &(X,Y) \mapsto \left(-2X + \lambda^2, -Y + \lambda\left(3X - \lambda^2\right)\right) \text{ with } \lambda = \frac{3X^2 + A}{2Y}, \end{aligned}$$

since it is quite obvious that $2P \in E(\overline{\mathbb{Z}}_p)$. □

Definition 2.6. We define $[n]$ to be the morphism:

$$\begin{aligned} [n]:\ E(\overline{\mathbb{Z}}_p) &\to E(\overline{\mathbb{Z}}_p) \\ P &\mapsto nP. \end{aligned}$$

□

Example 2.9. For $n = 1$ we have $[1] = id$, for $n = -1$, $[-1] = -id$ and for $n = 0$ the morphism which maps all onto the point at infinity:

$$\begin{aligned}[0] : \ E(\overline{\mathbb{Z}}_p) &\to E(\overline{\mathbb{Z}}_p)\\ P &\mapsto +\infty.\end{aligned}$$

□

Now we define the *degree* of a morphism; informally the degree of a morphism is simply the degree of the formulas that define the morphism itself. More formally, let $E : \ Y^2 = X^3 + AX + B$ be an elliptic curve over a field $\varkappa$; as we have seen a morphism is a map f such that:

$$\begin{aligned}f : \ E(\overline{\varkappa}) &\to E(\overline{\varkappa})\\ (X, Y) &\mapsto (t(X, Y), s(X, Y)).\end{aligned}$$

If we want f to be a morphism, it is necessary that the image of a point $P \in E(\overline{\varkappa})$ is still a point of the group $E(\overline{\varkappa})$; thus it is necessary (but not sufficient) that:

$$s(X, Y), t(X, Y) \in \overline{\varkappa}[X, Y]/\left(Y^2 - X^3 - AX - B\right) = \overline{\varkappa}[E].$$

$\overline{\varkappa}[E]$ is called the *coordinate ring of the curve* E[12] (see chapter 8 for an in-depth description).

Definition 2.8 (Function Field). We define a *function field* to be:

$$\overline{\varkappa}(E) \triangleq \left\{\frac{t(X, Y)}{s(X, Y)} : \ t(X, Y), s(X, Y) \in \overline{\varkappa}[E]\right\}.$$

□

Let $f : \ E_1 \to E_2$ be a morphism between the elliptic curves $E_1 : \ Y^2 = X^3 + A_1X + B_1$ and $E_2 : \ Y^2 = X^3 + A_2X + B_2$ over $\overline{\varkappa}$; let

$$\begin{aligned}f^* : \ \overline{\varkappa}(E_2) &\hookrightarrow \overline{\varkappa}(E_1)\\ \frac{t(X, Y)}{s(X, Y)} &\mapsto \left(P \mapsto \frac{t}{s}(f(P))\right).\end{aligned}$$

This gives the strike $\overline{\varkappa}(E_1)$ is a vector space over $\overline{\varkappa}(E_2)$. We are now ready to give the (formal) definition of degree of a morphism:

---

[12] We recall the definition of ideal.

Definition 2.7 (Ideal). Let $(R, +, \cdot)$ be a ring. A subset $\mathcal{I}$ of R is called *right ideal* of R if $(\mathcal{I}, +)$ is a subgroup of $(R, +)$ and

$$x \cdot r \in \mathcal{I} \qquad \forall\, x \in \mathcal{I}, r \in R.$$

Equivalently, a subset $\mathcal{I}$ of R is called *left ideal* of R if $(\mathcal{I}, +)$ is a subgroup of $(R, +)$ and

$$r \cdot x \in \mathcal{I} \qquad \forall\, x \in \mathcal{I}, r \in R.$$

An ideal that is right and left at the same time is called *bilateral*. □

Definition 2.9 (Degree of a Morphism). Let f be a morphism; the degree of f is:

$$deg(f) = dim_{\overline{\varkappa}(E_2)}(\overline{\varkappa}(E_1)).$$

□

Example 2.10. For our purpose the less formal definition is quite good. For example if $f = id$ we have $deg(f) = 1$ and if $f = [2]$ we have $deg(f) = 4$. We will show later that when $f = [n]$ we always have $deg(f) = n^2$. □

The Frobenius endomorphism plays a crucial role:

Definition 2.10 (Frobenius). Let $E : Y^2 = X^3 + AX + B$ be an elliptic curve over $\overline{\mathbb{Z}}_p$. The *Frobenius endomorphism* is given by:

$$\begin{aligned} Frob : E(\overline{\mathbb{Z}}_p) &\to E(\overline{\mathbb{Z}}_p) \\ (X, Y) &\mapsto (X^p, Y^p). \end{aligned}$$

□

It is easy to check that *Frob* is a morphism, in fact given a point $(\alpha, \beta) \in E(\overline{\mathbb{Z}}_p)$ we claim that $(\alpha^p, \beta^p) \in E(\overline{\mathbb{Z}}_p)$, since:

$$\begin{aligned} (\beta^p)^2 \equiv (\beta^2)^p \equiv (\alpha^3 + A\alpha + B)^p \equiv (\alpha^3)^p + A^p\alpha^p + B^p \equiv \\ \equiv (\alpha^3)^p + A\alpha^p + B \equiv (\alpha^p)^3 + A(\alpha^p) + B \pmod{p}. \end{aligned}$$

Example 2.11. The degree of Frobenius is obviously: $deg(Frob) = p$. □

Let $f : E_1(\overline{\mathbb{Z}}_p) \to E_2(\overline{\mathbb{Z}}_p)$ be a morphism and let $Q \in E_2(\overline{\mathbb{Z}}_p)$; now we want to investigate the relation between the degree of f and the cardinality of Q's preimage. The question is: how many points are there in the Q's preimage? One is attempted to say that the preimage of Q consists of exactly $deg(f)$ points, but this is not true. The reason is *multiplicity*; consider the following example:

Example 2.12. Let $f = Frob$ and $E_1 \equiv E_2$. The preimage of the point $Q = (\alpha, \beta) \in E(\overline{\mathbb{Z}}_p)$ is given by the solution of:

$$\begin{cases} X^p = \alpha \\ Y^p = \beta \end{cases}$$

with $\alpha, \beta \in \overline{\mathbb{Z}}_p$. If γ is a solution of the first equation (i. e. $\gamma^p = \alpha$), then:

$$X^p \equiv \alpha \equiv \gamma^p \pmod{p} \Rightarrow X^p - \gamma^p \equiv (X - \gamma)^p \equiv 0 \mod p.$$

Hence, as the characteristic of $\overline{\mathbb{Z}}_p$ is p, γ has multiplicity p. □

In deeper detail, it is possible to show that we have multiplicity greater than one, only if the formulas which define the morphism f are p-th powers, where p is the field characteristic. This brings to the definition:

Definition 2.11 (Inseparable Degree). Given the morphism f, the *inseparable degree* of f is:

$$deg_{ins}(f) = p^a$$

with a the maximum value with the property that f is a p^a-th power. □

Example 2.13. Let us suppose that the map f:

$$\begin{aligned} f:\ E(\overline{\varkappa}) &\to E(\overline{\varkappa}) \\ (X, Y) &\mapsto (X^6 + Y^3 + X^3Y^3, Y^12 + X^3), \end{aligned}$$

is a morphism for a suitable elliptic curve E. First of all $deg(f) = 12$; furthermore:

$$(X^6 + Y^3 + X^3Y^3, Y^12 + X^3) = \left((X^3 + Y + XY)^3, (Y^4 + X)^3\right),$$

and hence the inseparable degree is $deg_{ins}(f) = 3$. □

We observe that the inseparable degree is a divisor of the morphism's degree.

Definition 2.12 (Separable Degree). Let f be a morphism, we define the *separable degree* of f to be such that:

$$deg(f) = deg_{sep}(f)deg_{ins}(f).$$

□

We say that the morphism f is *separable* if $deg_{ins}(f) = 1$. Now we are ready to state the answer to the question made above:

Proposition 2.10 ([**45**]). *Let $f:\ E_1(\overline{\mathbb{Z}}_p) \to E_2(\overline{\mathbb{Z}}_p)$ be a morphism and let $Q \in E_2(\overline{\mathbb{Z}}_p)$ be a point on the destination curve E_2. The preimage of Q is made up of $deg_{sep}(f)$ points and each point has $deg_{ins}(f)$ as multiplicity.* □

The point at infinity is in a certain sense special:

Definition 2.13 (Morphism's Kernel). Let $f:\ E_1(\overline{\mathbb{Z}}_p) \to E_2(\overline{\mathbb{Z}}_p)$ be a morphism. The *kernel* of f is given by:

$$Ker(f) = \left\{(\alpha, \beta) \in \overline{\mathbb{Z}}_p:\ f(\alpha, \beta) = \infty\right\}.$$

□

It is easy to check that the kernel of f is a subgroup of $E(\overline{\mathbb{Z}}_p)$[13].

Proposition 2.10 has a very important consequence:

Corollary 2.11. *Obviously:*

$$\#Ker(f) = deg_{sep}(f).$$

□

[13]Whereas it could not be a subgroup of $E(\mathbb{Z}_p)$.

Example 2.14. Take $f = [2]$:

$$[2]: E(\overline{\mathbb{Z}}_p) \to E(\overline{\mathbb{Z}}_p)$$
$$(X, Y) \mapsto \left(-2X + \frac{(3X^2 + A)^2}{4(X^3 + AX + B)}, \frac{(\cdot)^2}{(X^3 + AX + B)Y}\right).$$

Clearly $(x, y) \in Ker([2]) \Leftrightarrow f(x, y) = \infty$, i. e. if and only if $X^3 + AX + B$ is zero. The equation $X^3 + AX + B = 0$ has three zeroes in $\overline{\mathbb{Z}}_p$; furthermore, by definition, $f(\infty) = \infty$ and the formulas of the morphism f are not p-th powers. Hence:

$$\#Ker(f) = 4 = deg([2]) = deg_{sep}([2]).$$

□

Now let us consider the set of all possible *endomorphisms*:

$$End(E) = \left\{\text{Morphisms } f : E(\overline{\mathbb{Z}}_p) \longrightarrow E(\overline{\mathbb{Z}}_p)\right\}.$$

We can define the summation of morphisms f and g to be:

$$(f + g)(P) \triangleq f(P) + g(P),$$

and the product of morphisms f and g to be:

$$(f \cdot g)(P) \triangleq f\left(g(P)\right),$$

$\forall\, P \in E(\overline{\mathbb{Z}}_p)$. It is easy to check that $(End(E), +, \cdot)$ is a ring, and it is called the *ring of endomorphisms* associated with the curve E. The Morphism $[0]$, such that $[0]P = \infty$, $\forall\, P \in E$, plays the role of identity element for the summation and morphism $[1] = id$, such that $[1]P = P$, $\forall\, P \in E$, plays the role of identity element for the product. It is very important to study the structure of this ring.

Consider the map given by:

$$\phi: \mathbb{Z} \to End(E)$$
$$n \mapsto [n];$$

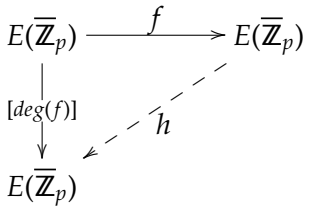
for example if $n = deg(f) \in \mathbb{Z}$, we have $\phi(n) = [deg(f)]$. We know that if $f: E(\overline{\mathbb{Z}}_p) \longrightarrow E(\overline{\mathbb{Z}}_p)$ is a morphism, then $Ker(f)$ is a subgroup of $E(\overline{\mathbb{Z}}_p)$, with $\#Ker(f) = deg_{sep}(f)$. Thus, if we take a point $P \in Ker(f)$, by Lagrange's[14] theorem, $[deg_{sep}(f)]P = [\#Ker(f)]P = \infty$. Furthermore, $deg_{sep}(f) | deg(f)$, so that if $P \in Ker(f)$, $[deg(f)]P = \infty$ too and thus $P \in Ker([deg(f)])$. We have shown that $Ker(f) \subset Ker([deg(f)])$.

Thus, by a well known result from algebraic geometry[15], $\exists\,!$ morphism $h: E(\overline{\mathbb{Z}}_p) \longrightarrow E(\overline{\mathbb{Z}}_p)$, such that:

[14] This is another fundamental result of basic algebra.

Theorem 2.12 (Lagrange's Theorem). *For any finite group $\mathcal{G}$, the order (number of elements) of every subgroup $\mathcal{H}$ of $\mathcal{G}$ divides the order of $\mathcal{G}$.* □

[15] It is an extension of the fundamental homomorphism theorem from group algebra:



$$h \cdot f = [deg(f)].$$

DEFINITION 2.14 (Dual Isogeny). We define the *dual isogeny* of the morphism f to be $f^\vee \triangleq h$. There are a lot of very interesting properties, about which we omit the proof[**51**]:

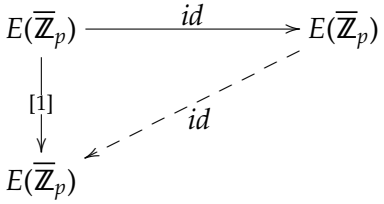
$$(f^\vee)^\vee = f \tag{2.5}$$

$$(f \cdot g)^\vee = g^\vee \cdot f^\vee \tag{2.6}$$

$$(f + g)^\vee = f^\vee + g^\vee. \tag{2.7}$$

□

EXAMPLE 2.15. Let $f = id$, it is $deg(id) = 1$ and thus:



$$id^\vee = [1] = id.$$

□

EXAMPLE 2.16. Let $f = [2]$, using equation (2.7):

$$[2]^\vee = ([1] + [1])^\vee = [1]^\vee + [1]^\vee = [1] + [1] = [2].$$

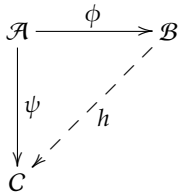
In general one can show that $[n]^\vee = [n]$. □

EXAMPLE 2.17. We show that $deg([n]) = n^2$, for each $n \in \mathbb{Z}_{\geq 0}$; in fact by definition of dual isogeny:

$$[deg([n])] = [n] \cdot [n]^\vee = [n] \cdot [n] = [n^2]$$
$$\Rightarrow deg([n]) = n^2.$$

□

THEOREM 2.13 (Fundamental Homomorphism Theorem for Groups). *Let $\phi : \mathcal{A} \to \mathcal{B}$ and $\psi : \mathcal{A} \to \mathcal{C}$ be two group homomorphisms, such that $Ker(\phi) \subset Ker(\psi)$; then $\exists!$ homomorphism $h : \mathcal{B} \to \mathcal{C}$ such that:*



$$h \cdot \phi = \psi.$$

□

We can use the definition of dual isogeny to show some very general (and very useful) facts.

Proposition 2.14. *Let E be an elliptic curve over a generic field $\varkappa$ and $f \in End(E)$. Than f is such that:*

$$f^2 - [t]f + [d] = 0,$$

where $[t] = f + f^\vee$ and $[d] = [deg(f)]$, $t, d \in \mathbb{Z}$. The integer t is called the trace of the morphism f.

Proof. We can always write:

$$\begin{aligned} & f^2 - f^2 - f^\vee f + f^\vee f = 0 \\ \Rightarrow \quad & f^2 - (f + f^\vee)f + f^\vee f = 0. \end{aligned}$$

By definition of dual isogeny we have $f^\vee f = [deg(f)] = [d]$, with $d \in \mathbb{Z}$ the degree of the morphism f. Furthermore let $(f + f^\vee) = [t]$; we claim that $t \in \mathbb{Z}$. In fact:

$$\begin{aligned} [t] = f + f^\vee &= (f + id)(f + id)^\vee - ff^\vee - id = \\ &= [deg(f + id)] - [deg(f)] - [1] = [deg(f + id) - deg(f) - 1], \end{aligned}$$

and thus $t \in \mathbb{Z}$. □

As a consequence we have shown:

Corollary 2.15. *Each $f \in End(E)$ is a zero of:*

$$X^2 - [t]X + [d] = 0,$$

where $t, d \in \mathbb{Z}$ are respectively the trace and the degree of f. □

We can find a bound for the trace t:

Lemma 2.16. *Let E be an elliptic curve over a field $\varkappa$, and let $End(E)$ be the ring of endomorphisms associated with the curve E. Then any $f \in End(E)$ is such that:*

$$|t| \leq 2\sqrt{d},$$

where $t, d \in \mathbb{Z}$ are respectively the trace and the degree of f.

Proof. Let us consider the morphism:

$$[n] - [m]f \qquad n, m \in \mathbb{Z} \text{ and } m \neq 0.$$

By definition of degree, clearly, $deg([n] - [m]f) \geq 0$; furthermore, by definition of dual isogeny,

$$\begin{aligned}
[deg([n] - m[f])] &= ([n] - [m]f)([n] - [m]f)^\vee \\
&= ([n] - [m]f)([n]^\vee - f^\vee[m]^\vee) = \\
&= \left[\begin{array}{l}\text{we can write } [n]^\vee = [n], \text{ using example 2.16, and} \\ f[m] = [m]f \text{ since } f \text{ is a group homomorphism}\end{array}\right] = \\
&= ([n] - [m]f)([n] - [m]f^\vee) = \\
&= [n]^2 - [m][n](f + f^\vee) + [m]^2 f f^\vee = \\
&= [n]^2 - [m][n][t] + [m]^2[d] = \\
&= [n^2 - nmt + m^2 d].
\end{aligned}$$

Since the map:

$$\begin{aligned}
\phi : \ \mathbb{Z} &\to End(E) \\
x &\mapsto [x],
\end{aligned}$$

is injective, we can conclude that:

$$\begin{aligned}
& deg([n] - [m]f) = n^2 - nmt + m^2 d \geq 0 \\
\Rightarrow \quad & 0 \leq \left(\frac{n}{m}\right)^2 - t\left(\frac{n}{m}\right) + d,
\end{aligned}$$

$\forall\ n, m \in \mathbb{Z}$ with $m \neq 0$. Let $\xi = \frac{n}{m} \in \mathbb{Q}$, hence:

$$\xi^2 - t\xi + d \geq 0,$$

which is true if and only if the discriminant of the parabola is less than or equal to zero, i. e. if and only if:

$$\begin{aligned}
& t^2 - 4d \leq 0 \\
\Rightarrow \quad & |t| \leq 2\sqrt{d}.
\end{aligned}$$

□

2.4. Hasse's Theorem

We are interested in a formula to compute $\#E(\mathbb{Z}_p)$. In this section we will state (and prove) the Hasse theorem which gives us a bound on the above cardinality. As we have seen in section 2.2, given an elliptic curve over $\mathbb{Z}_p$, for each $x \in \mathbb{Z}_p$ and $y^2 \equiv x^3 + Ax + B \pmod{p}$, we are not sure that the pair (x, y) is a point of $E(\mathbb{Z}_p)$: it depends on whether $x^3 + Ax + B$ is a quadratic residue modulo p or not. Hence we have a first (inefficient) way to evaluate $\#E(\mathbb{Z}_p)$: for each $x \in \mathbb{Z}_p$ we compute $x^3 + Ax + B \bmod p$ and we count zero points if we obtain a quadratic non-residue modulo p, one point if we obtain zero and two points if we obtain a quadratic residue modulo p; furthermore the point at infinity always belongs to the curve. Recall the definition of *Legrende symbol*:

Definition 2.15 (Legrende Symbol). Let $\chi_p : \mathbb{Z}_p^* \longrightarrow \{\pm 1\}$ be the function defined by:

$$\chi_p(x) = \begin{cases} 1 & \text{if } x \text{ is a quadratic residue modulo } p \\ -1 & \text{if } x \text{ is a quadratic non-residue modulo } p. \end{cases}$$

We extend χ_p to $\mathbb{Z}_p$ by asking that $\chi_p(0) \triangleq 0$ and now $\chi_p : \mathbb{Z}_p \longrightarrow \{\pm 1, 0\}$. Hence,

$$1 + \chi_p(x) = \begin{cases} 2 & \text{if } x \text{ is a quadratic residue modulo } p \\ 1 & \text{if } x \equiv 0 \pmod{p} \\ 0 & \text{if } x \text{ is a quadratic non-residue modulo } p. \end{cases}$$

□

Thus we can write:

$$\#E(\mathbb{Z}_p) = 1 + \sum_{x \in \mathbb{Z}_p} 1 + \chi_p(x^3 + Ax + B) = 1 + p + \sum_{x \in \mathbb{Z}_p} \chi_p(x^3 + Ax + B). \tag{2.8}$$

We will postpone the study of better algorithms for computing $\#E(\mathbb{Z}_p)$ to chapter 4.

Anyway, we could ask which is the value of the summation in the above equation; intuitively, varying x in $\mathbb{Z}_p$, $x^3 + Ax + B$ is a random value of $\mathbb{Z}_p$ and by lemma 2.4 half of the values will be quadratic residues modulo p and the other half will not, so that we expect a lot of cancellation. This intuition is confirmed by *Hasse's theorem*:

Theorem 2.17 (Hasse 1933). *Let $E : Y^2 = X^3 + AX + B$ be an elliptic curve over $\mathbb{Z}_p$, with p a prime. Then:*

$$\#E(\mathbb{Z}_p) = p + 1 - t,$$

with $|t| < 2\sqrt{p}$.

Stated in other words, the Hasse theorem is telling us that in equation (2.8) we have:

$$\left|\sum_{x \in \mathbb{Z}_p} \chi_p(x^3 + Ax + B)\right| = |\#E(\mathbb{Z}_p) - (p + 1)| < 2\sqrt{p}.$$

Proof. The basic idea is to see $E(\mathbb{Z}_p)$ as the kernel of a particular morphism. Let $(\alpha, \beta) \in E(\mathbb{Z}_p)$, clearly $\alpha, \beta \in \mathbb{Z}_p$, which is true if and only if α and β satisfy Fermat's little theorem:

$$\begin{aligned} & (\alpha, \beta) \in E(\mathbb{Z}_p) \\ \Rightarrow \quad & \alpha, \beta \in \mathbb{Z}_p \\ \Leftrightarrow \quad & \alpha^p = \alpha \qquad \beta^p = \beta \\ \Rightarrow \quad & (\alpha, \beta) \in E(\mathbb{Z}_p) \Leftrightarrow (\alpha^p, \beta^p) = (\alpha, \beta) \in E(\mathbb{Z}_p) \\ \Rightarrow \quad & Frob(\alpha, \beta) = [1](\alpha, \beta) = id(\alpha, \beta) \\ \Rightarrow \quad & (Frob - id)(\alpha, \beta) = 0 \quad \forall\, \alpha, \beta \in E(\mathbb{Z}_p). \end{aligned}$$

In other words $E(\mathbb{Z}_p)$ is the kernel of the morphism $Frob - id$:

$$Ker(Frob - id) = E(\mathbb{Z}_p).$$

Now we claim that $f = Frob - id$ is separable; in fact if f would not be separable, $id = Frob - f$ should be not[16] separable, which is impossible. Hence:

$$\#E(\mathbb{Z}_p) = \#Ker(f) = deg_{sep}(f) = deg(f),$$

where f is still $f = Frob - id$. Furthermore by definition of dual isogeny:

$$\begin{aligned}
[deg(Frob - id)] &= (Frob - id)(Frob - id)^\vee = \\
&= (Frob - id)(Frob^\vee - id^\vee) = \\
&= (Frob - id)(Frob^\vee - id) = \\
&= Frob \cdot Frob^\vee - Frob - Frob^\vee + id = \\
&= [deg(Frob)] - [Tr(Frob)] + [1] = \\
&= [deg(Frob) - Tr(Frob) + 1],
\end{aligned}$$

where $Tr(Frob) = t$ is the trace of Frobenius endomorphism and $deg(Frob) = d = p$ is its degree. Thus:

$$\#E(\mathbb{Z}_p) = \#Ker(Frob - id) = p + 1 - t,$$

and by lemma[17] 2.16 $|t| < 2\sqrt{d} = 2\sqrt{p}$. □

2.5. The j-Invariant

In this section we deal with the concept of *isomorphism classes* for elliptic curves over $\mathbb{Z}_p$. Let $E: Y^2 \equiv X^3 + AX + B \pmod{p}$ be a non-singular elliptic curve over $\mathbb{Z}_p$ and let (x, y) be a generic point of $E(\mathbb{Z}_p)$, i. e. (x, y) is such that

$$y^2 \equiv x^3 + Ax + B \pmod{p}.$$

Let $c \in \mathbb{Z}_p^*$, we multiply the members of the above equation by c^6, obtaining:

$$\begin{aligned}
& c^6y^2 \equiv c^6x^3 + c^6Ax + c^6B \pmod{p} \\
\Rightarrow \quad & (c^3y)^2 \equiv (c^2x)^3 + A(c^2x)c^4 + Bc^6 \pmod{p},
\end{aligned}$$

i. e. the point (c^2x, c^3y) belongs to the curve $Y^2 \equiv X^3 + c^4AX + c^6B \pmod{p}$. We have the following general proposition[18] **[51]**:

---

[16] It is a general fact that inseparable morphisms form an ideal. Furthermore if f and g are two inseparable morphisms, i. e. f and g are p-th powers, their summation is (in characteristic p) still a p-th power.

[17] Note that lemma 2.16 tells us that $|t| \leq 2\sqrt{d}$, but now $d = p$ is a prime and thus $\sqrt{p}$ is not an integer and we can replace the sign $\leq$ with $<$.

[18] Here we deal with the case of a finite field, but the result is still valid for an elliptic curve over a generic field $\varkappa$, with $c \in \overline{\varkappa}$.

PROPOSITION 2.18 (Isomorphic Curves). *Let* $E: Y^2 \equiv X^3+AX+B \pmod p$ *and* $E': Y^2 \equiv X^3 + A'X + B' \pmod p$ *be two non-singular elliptic curves over* $\mathbb{Z}_p$. *Than* E *and* E' *are isomorphic if and only if* $\exists\, c \in \mathbb{Z}_p^*$ *such that:*

$$A' = c^4 A \qquad B' = c^6 B. \tag{2.9}$$

□

Consider the quantity $\frac{A^3}{B^2}$, it is clear that this is an *invariant* for the transformation of equation (2.9), as:

$$\frac{A^3}{B^2} = \frac{\frac{(A')^3}{c^{12}}}{\frac{(B')^2}{c^{12}}} = \frac{(A')^3}{(B')^2}.$$

On the basis of this reasoning we define the j-invariant for an elliptic curve E to be:

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2}.$$

It is easy to check that the j-invariant is invariant for the transformation of equation (2.9), furthermore $j(E)$ there always exists if E is a non-singular elliptic curve (since the denominator is Δ_E).

PROPOSITION 2.19. *For each value* $j_0 \in \mathbb{Z}_p$ *there always exists an elliptic curve* E *over* $\mathbb{Z}_p$, *with* $j(E) = j_0$.

PROOF. We observe that:

$$\begin{aligned} \frac{1728}{j_0} &= 1 + \frac{27B^2}{4A^3} = 1 + \frac{(B/2)^2}{(A/3)^3} \\ \Rightarrow \quad \frac{1728 - j_0}{j_0} &= \frac{(B/2)^2}{(A/3)^3}, \end{aligned}$$

and thus it suffices to find two values of A and B which satisfies the above relation. For example:

$$\begin{aligned} A &= \frac{3j_0}{1728 - j_0} \\ B &= \frac{2j_0}{1728 - j_0}, \end{aligned} \tag{2.10}$$

as it is easy to verify. The elliptic curve E with A and B given by equations (2.10) has $j(E) = j_0$. If $j_0 = 0$ we take $E: Y^2 = X^3 + 1$ ($A = 0$); if $j_0 = 1728$ we take $E: Y^2 = X^3 + X$ ($B = 0$). □

Now it should be clear that if the elliptic curves E and E' have the same j-invariant, namely $j(E) = j(E')$, the curves are, by proposition 2.18, isomorphic. We now ask if the reverse is also valid: what about two curves with the same j-invariant? Are they isomorphic? To answer this question,

let $E:\ Y^2 \equiv X^3 + AX + B \pmod p$ and $E':\ Y^2 \equiv X^3 + A'X + B' \pmod p$ be two non-singular elliptic curves over $\mathbb{Z}_p$, with $j(E) = j(E')$. Thus:

$$\frac{1728}{j(E)} = 1 + \frac{27B^2}{4A^3} = \frac{1728}{j(E')} = 1 + \frac{27(B')^2}{4(A')^3}$$
$$\Rightarrow \quad \frac{B^2}{A^3} = \frac{(B')^2}{(A')^3} \quad \Rightarrow \quad \left(\frac{A}{A'}\right)^3 = \left(\frac{B}{B'}\right)^2.$$

Let $d = \frac{A}{A'}\frac{B'}{B}$, we have:

$$d^2 = \left(\frac{A}{A'}\right)^2\left(\frac{B'}{B}\right)^2 = \left(\frac{A}{A'}\right)^2\left(\frac{A'}{A}\right)^3 = \left(\frac{A'}{A}\right)$$
$$d^3 = \left(\frac{A}{A'}\right)^3\left(\frac{B'}{B}\right)^3 = \left(\frac{B}{B'}\right)^2\left(\frac{B'}{B}\right)^3 = \left(\frac{B'}{B}\right)$$
$$\Rightarrow \quad A' = d^2A \qquad B' = d^3B.$$

Hence E and E' are isomorphic only if d is a quadratic residue modulo p; since we know, by lemma 2.4, that half of the elements of $\mathbb{Z}_p^*$ are quadratic residues and the other half are not, we can conclude that each value of j has associated two *isomorphism classes*. There are two special cases, namely

$$A = 0 \quad \Leftrightarrow \quad j(E) = 0$$
$$B = 0 \quad \Leftrightarrow \quad j(E) = 1728,$$

for which the isomorphism classes are not two, as we will now see in deeper detail. Excluding for a while these special cases, we can say that, for each value $j_0 \in \mathbb{Z}_p$, there exists, by proposition 2.19, an elliptic curve E with $j(E) = j_0$; furthermore there are two isomorphism classes associated with that value of j_0. Let E and E' be two elements of these two isomorphism classes:

$$E:\ Y^2 \equiv X^3 + AX + B \pmod p$$
$$E':\ Y^2 \equiv X^3 + d^2AX + d^3B \pmod p.$$

If $d \in \mathbb{Z}_p^*$ is a quadratic residue modulo p, $E \simeq E'$; otherwise E and E' are not isomorphic and we say that E is the *twist* of E' (and viceversa). Let us suppose we are in the second case, i. e. that E' is the twist of E; we divide the equation of E' by d^3:

$$\frac{Y^2}{d^3} \equiv d\left(\frac{Y}{d}\right)^2 = \left(\frac{X}{d}\right)^3 + A\left(\frac{X}{d}\right) + B \pmod p$$
$$\text{define } \left(\frac{X}{d}\right) = Z \text{ and } \left(\frac{Y}{d^2}\right) = W$$
$$\Rightarrow \quad E':\ dW^2 \equiv Z^3 + AZ + B \pmod p.$$

Recall that by equation (2.8):

$$\#E(\mathbb{Z}_p) = 1 + \sum_{x\in\mathbb{Z}_p} 1 + \chi_p(x^3 + Ax + B) = 1 + p + \sum_{x\in\mathbb{Z}_p} \chi_p(x^3 + Ax + B).$$

We observe that, for a given value $s = q^2 \in (\mathbb{Z}_p^*)^2$, if d is a quadratic non residue modulo p, the fraction $\frac{s}{d}$ is a quadratic non residue modulo p; in fact if $\frac{s}{d}$ would be a quadratic residue, i. e. $\frac{s}{d} = t^2$, it should be $t^2 = \frac{q^2}{d}$ which is impossible. So if $x^3 + Ax + B$ is an element of $(\mathbb{Z}_p^*)^2$, the fraction $\frac{x^3+Ax+B}{d}$ is a quadratic non residue modulo p; in other words, if for a certain value $x \in \mathbb{Z}_p$, the curve E has two points $(x, \pm y)$ (i. e. $\chi_p(x^3 + Ax + B) = 1$), for the same value of x the twist of E has zero points (i. e. $\chi_p\left(\frac{x^3+Ax+B}{d}\right) = -1$), since $\frac{x^3+Ax+B}{d} \notin (\mathbb{Z}_p^*)^2$. Hence:

$$\#E(\mathbb{Z}_p) + \#E'(\mathbb{Z}_p) = 2 + 2p,$$

i. e. if E has $p + 1 - t$ points, its twist E' is such that

$$\#E'(\mathbb{Z}_p) = 2 + 2p - p - 1 + t = p + 1 + t,$$

and $|t| < 2\sqrt{p}$ by Hasse's bound. To sum up, for a fixed value of $j_0 \neq 0, 1728 \in \mathbb{Z}_p$, we have two curves (up to isomorphisms) with $j(E) = j_0$, namely E and its twist E', and we know that if E has $p + 1 - t$ points, E' has $p + 1 + t$ points; hence we can compute $|t|$ given a value j_0. There is not, instead, a polynomial algorithm that, starting from a value of t, yields the equation (i. e. the values A and B) of a curve E with the j-invariant corresponding to t.

Now we want to characterize exactly the isomorphism classes of $E(\mathbb{Z}_p)$. We need a lemma:

Lemma 2.20. *Let p be a prime and $d \in \mathbb{N}$. We have:*

$$\#\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^d = \gcd(p - 1, d).$$

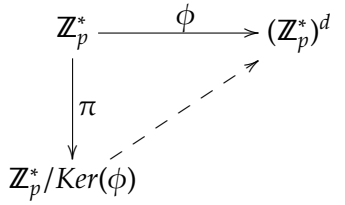
Proof. Consider the map which takes a value $x \in \mathbb{Z}_p^*$ and computes the d-th power of x:

$$\begin{aligned} \phi :\ \mathbb{Z}_p^* &\longrightarrow (\mathbb{Z}_p^*)^d \\ x &\mapsto x^d; \end{aligned}$$

it is a group homomorphism, with $Im(\phi) = (\mathbb{Z}_p^*)^d$. The kernel of ϕ is the set of elements $\alpha \in \mathbb{Z}_p^*$ such that $\alpha^d \equiv 1 \pmod{p}$, i. e.:

$$Ker(\phi) = \left\{\alpha \in \mathbb{Z}_p^* :\ \alpha^d \equiv 1 \pmod{p}\right\}.$$

Thus we can apply the fundamental homomorphism theorem for groups and conclude:



$$\Rightarrow Im(\phi) = (\mathbb{Z}_p^*)^d \simeq \mathbb{Z}_p^*/Ker(\phi).$$

Hence,

$$\#(\mathbb{Z}_p^*/Ker(\phi)) = \frac{\#\mathbb{Z}_p^*}{\#Ker(\phi)} = \#(\mathbb{Z}_p^*)^d$$

$$\Rightarrow \quad \frac{\#\mathbb{Z}_p^*}{\#(\mathbb{Z}_p^*)^d} = \#\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^d = \#Ker(\phi).$$

Then it suffices to evaluate:

$$\#Ker(\phi) = \#\left\{\alpha \in \mathbb{Z}_p^* : \ \alpha^d \equiv 1 \pmod p\right\}.$$

We claim that:

$$Ker(\phi) = \mathcal{D} = \left\{\alpha \in \mathbb{Z}_p^* : \ \alpha^\delta \equiv 1 \pmod p\right\},$$

with $\delta = \gcd(d, p-1)$. On the one hand if $\alpha^\delta \equiv 1 \pmod p$, it is also $\alpha^d \equiv 1 \pmod p$, since $\delta | d$; so it seems that $Ker(\phi) \supset \mathcal{D}$. On the other hand let $\alpha^d \equiv 1 \pmod p$; since $\delta = \gcd(d, p-1)$, by Bézout's identity[19], $\exists\, a, b$ such that $ad + b(p-1) \equiv \delta \pmod p$. Then by Fermat's little theorem:

$$\alpha^{p-1} \equiv 1 \pmod p$$

$$\Rightarrow \quad \alpha^\delta \equiv \alpha^{ad}\alpha^{b(p-1)} \equiv 1 \cdot 1 \equiv 1 \pmod p,$$

and $Ker(\phi) \subset \mathcal{D}$. We must conclude $Ker(\phi) = \mathcal{D}$, so that now we need to evaluate $\#\mathcal{D}$.

First of all $\#\mathcal{D} \leq \delta$, since $X^\delta - 1$ has degree δ. Let g be a primitive root[20] of $\mathbb{Z}_p^*$, i. e. $ord(g) = p-1$ in $\mathbb{Z}_p^*$; the element $h = g^{\frac{p-1}{\delta}}$ is such that $ord(h) = \delta$ in $\mathbb{Z}_p^*$ and thus the set $\left\{h, h^2, \ldots, h^\delta = 1\right\}$ is made up of δ *distinct* elements such that they have 1 as δ-th power. So we have shown δ distinct elements which are zeroes of $X^\delta - 1$, and we can conclude:

$$\#\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^d = \#Ker(\phi) = \#\mathcal{D} = \delta = \gcd(p-1, d).$$

---

[19] This is another well-known result from elementary number theory[**29**].

THEOREM 2.21 (Bézout's Identity). *Let $x, y \neq 0$ be two integers; then there always exists some integers a, b such that*

$$ax + by = \gcd(x, y).$$

□

Note that we can evaluate the integers a, b by means of the extended euclidean algorithm (see appendix B).

[20] It is a well-known fact that, if p is a prime, $\mathbb{Z}_p^*$ is cyclic, i. e. there are elements (called primitive roots) of order $p-1$. See theorem 7.3 for a proof.

□

Example 2.18. Let $p = 5$ and $d = 4$; each element of $\mathbb{Z}_5$ has 1 as fourth power, then:

$$\mathbb{Z}_5^*/(\mathbb{Z}_5^*)^4 \simeq \mathbb{Z}_5^* = \{1, 2, 3, 4\},$$

and $\#\mathbb{Z}_5^*/(\mathbb{Z}_5^*)^4 = \gcd(4, 4) = 4$. □

Example 2.19. Let $p = 7$ and $d = 3$, then:

$$\mathbb{Z}_7^*/(\mathbb{Z}_7^*)^3 = \mathbb{Z}_7^*/\left\{\overline{1}, \overline{2}, \overline{4}\right\},$$

and $\#\mathbb{Z}_7^*/(\mathbb{Z}_7^*)^3 = \gcd(7 - 1, 3) = 3$. □

Let us consider $j_0 \neq 0, 1728$ and suppose the elliptic curves E and E' to have the same j-invariant $j(E) = j(E') = j_0$. If this is the case, we have seen that $E : Y^2 = X^3 + AX + B$ and $E' : dY^2 = X^3 + A'X + B'$ and $E \simeq E'$ if and only if $d = \frac{(A/A')}{(B/B')}$ is a quadratic residue modulo p; hence we can choose d up to 2-th powers, i. e. $d \in \mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2$, to obtain curves that are not isomorphic. So there is a bijection:

$$\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 \longleftrightarrow \left\{ \begin{smallmatrix} E(\mathbb{Z}_p) \text{ with} \\ j(E)=j_0\neq 0,1728 \end{smallmatrix} \right\}$$

and, by lemma 2.20, $\#\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^2 = \gcd(p - 1, 2) = 2$.

Now we deal with the case $A = 0$ or $B = 0$ (A and B cannot be both zero if E is non-singular); let $A = 0$ (so that $j_0 = 0$) and let us suppose that the curves $E : Y^2 = X^3 + B$ and $E' : Y^2 = X^3 + B'$ are isomorphic. Thus by proposition 2.18, $\exists\, c \in \mathbb{Z}_p^*$ such that $B' = c^6 B$. Hence we can choose B up to 6-th powers, i. e. $B \in \mathbb{Z}_p^*/(\mathbb{Z}_p^*)^6$, to obtain curves that are not isomorphic. So there is a bijection:

$$\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^6 \longleftrightarrow \left\{ \begin{smallmatrix} E(\mathbb{Z}_p) \text{ with} \\ j(E)=j_0=0 \end{smallmatrix} \right\}$$

and by lemma 2.20:

$$\#\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^6 = \gcd(p - 1, 6) = \begin{cases} 6 & \text{if } p \equiv 1 \pmod 3 \\ 2 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

On the other hand if $B = 0$, all the curves of the kind $E : Y^2 = X^3 + AX$ have $j(E) = j_0 = 1728$. But these curves are not all isomorphic; $E : Y^2 = X^3 + AX$ and $E' : Y^2 = X^3 + A'X$ are isomorphic if $\exists\, c \in \mathbb{Z}_p^*$ such that $A' = c^4 A$. Hence we can choose A up to 4-th powers, i. e. $A \in \mathbb{Z}_p^*/(\mathbb{Z}_p^*)^4$, to obtain curves that are not isomorphic. So there is a bijection:

$$\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^4 \longleftrightarrow \left\{ \begin{smallmatrix} E(\mathbb{Z}_p) \text{ with} \\ j(E)=j_0=1728 \end{smallmatrix} \right\},$$

and by lemma 2.20:

$$\#\mathbb{Z}_p^*/(\mathbb{Z}_p^*)^4 = \gcd(p - 1, 4) = \begin{cases} 4 & \text{if } p \equiv 1 \pmod 4 \\ 2 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

PROPOSITION 2.22. *Let p be a prime. We have a formula to evaluate the number of elliptic curves over $\mathbb{Z}_p$ (up to isomorphisms):*

$$\#\left\{\begin{matrix}\text{Elliptic curves } E(\mathbb{Z}_p)\\ \text{up to}\\ \text{isomorphisms}\end{matrix}\right\} = \begin{cases} 2p+6 & \text{if } p \equiv 1 \pmod{12} \\ 2p+2 & \text{if } p \equiv 5 \pmod{12} \\ 2p+4 & \text{if } p \equiv 7 \pmod{12} \\ 2p & \text{if } p \equiv 11 \pmod{12}. \end{cases} \tag{2.11}$$

PROOF. By proposition 2.19, for each value $j_0 \in \mathbb{Z}_p$ there is always an elliptic curve with $j(E) = j_0$; thus if p is fixed we have p distinct values of j_0. So if $j_0 \neq 0, 1728$ we have $p-2$ values of j_0, and each value brings two isomorphism classes, for a total of $2(p-2)$ curves $E(\mathbb{Z}_p)$ (up to isomorphisms). If $j_0 = 0$, we have seen that there are either 6 (when $p \equiv 1 \pmod 3$) or 2 (when $p \equiv 2 \pmod 3$) isomorphism classes. Finally if $j_0 = 1728$, there are either 4 (when $p \equiv 1 \pmod 4$) or 2 (when $p \equiv 3 \pmod 4$) isomorphism classes.

Furthermore equation (2.11) contains all primes $p \neq 2, 3$ modulo 12. Hence if $p \equiv 1 \pmod{12}$, it is $p \equiv 1 \pmod 3$ *and* $p \equiv 1 \pmod 4$ and the total number of curves (up to isomorphisms) is:

$$2(p-2) + 6 + 4 = 2p + 6.$$

Similarly if $p \equiv 5 \pmod{12}$, it is $p \equiv 5 \equiv 2 \pmod 3$ *and* $p \equiv 5 \equiv 1 \pmod 4$ and the total number of curves (up to isomorphisms) is:

$$2(p-2) + 2 + 4 = 2p + 2.$$

If, instead, $p \equiv 7 \pmod{12}$, it is $p \equiv 7 \equiv 1 \pmod 3$ *and* $p \equiv 7 \equiv 3 \pmod 4$ and the total number of curves (up to isomorphisms) is:

$$2(p-2) + 6 + 2 = 2p + 4.$$

Finally if $p \equiv 11 \pmod{12}$, it is $p \equiv 11 \equiv 2 \pmod 3$ *and* $p \equiv 11 \equiv 3 \pmod 4$ and the total number of curves (up to isomorphisms) is:

$$2(p-2) + 2 + 2 = 2p.$$

□

EXAMPLE 2.20. Let $p = 13 \equiv 1 \pmod{12}$. We expect, by equation (2.11), to have $2p + 6 = 32$ elliptic curves $E(\mathbb{Z}_{13})$ (up to isomorphisms), with j_0 assuming all possible values in $\mathbb{Z}_{13}$ (see table 2.3). □

Note that $|t| < 2\sqrt{13} \approx 7,3$, as confirmed by Hasse's theorem; further all the values t such that $|t| < 2\sqrt{p}$ are present. This is, indeed, a theorem:

THEOREM 2.23. *If p is a prime, for each $t \in \mathbb{Z}$ such that $|t| < 2\sqrt{p}$, it always exists an elliptic curve over $\mathbb{Z}_p$, say $E(\mathbb{Z}_p)$, such that $\#E(\mathbb{Z}_p) = p + 1 - t$.* □

$j_0 \in \mathbb{Z}_{13}$	t
0	$\pm 1, \pm 5, \pm 7$
1	± 6
2	± 1
3	± 5
4	± 2
5	0
6	± 2
7	± 4
8	± 3
9	± 1
10	± 4
11	± 2
12	$\pm 6, \pm 4$

TABLE 2.3. Values of j-invariant and t for the elliptic curves $E(\mathbb{Z}_p)$ with $p = 13$.

CHAPTER 3

Elliptic Curves Over $\mathbb{C}$

Contents

In this chapter we deal with elliptic curves defined over $\mathbb{C}$, denoted $E(\mathbb{C})$. Elliptic curves with complex multiplication are a special kind of elliptic curves over $\mathbb{C}$; we are interested in this kind of curves, since they have a lot of applications. In particular they provide (thanks to an idea of Atkin) the most efficient algorithm to evaluate the cardinality of an elliptic curve defined over $\mathbb{Z}_p$; furthermore they are used to improve the efficiency of the Goldwasser-Kilian primality test in the *Elliptic Curve Primality Proving* (ECCP) test, which is the most efficient (deterministic) primality test known.

3.1. Lattices, Orders and the Weierstrass $\wp$-function

The theory of elliptic curves over $\mathbb{C}$ is much more strengthened[**31**] with respect to the theory of elliptic curves over $\mathbb{Z}_p$ (which is more recent). The point of view is different, since we can use the powerful means of mathematical analysis.

Definition 3.1 (Lattice). Let $\omega_1, \omega_2 \in \mathbb{C}$ be two independent[1] complex numbers. A *lattice* is defined by the equation:

$$L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z} = \{n\omega_1 + m\omega_2 : \ n, m \in \mathbb{Z}\}.$$

□

In other words, a lattice is a discrete sub-group isomorphic to $\mathbb{Z}\times\mathbb{Z}$, i. e. it is the $\mathbb{Z}$-span of two independent vectors[2] (see figure 3.1).

Example 3.1. The ring of Gauss integers (see figure 3.2) is a lattice: $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}$, with $i = \sqrt{-1}$. □

[1] We mean that $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$.

[2] More in general a lattice is a discrete sub-group of $\mathbb{R}^n$ which spans $\mathbb{R}^n$, and thus it generates $\mathbb{R}^n$ starting from a basis of $\mathbb{R}^n$ (n independent vectors of $\mathbb{R}^n$).

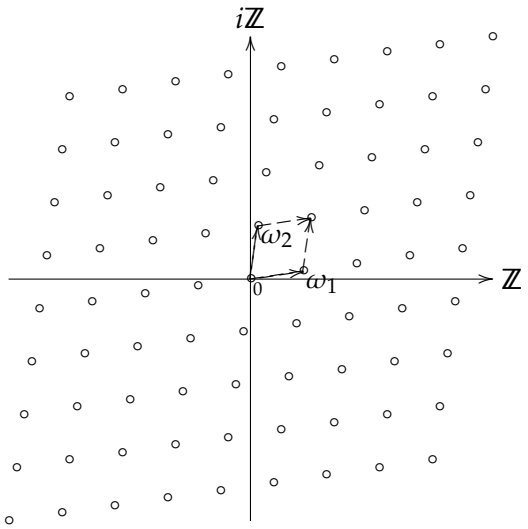


FIGURE 3.1. The lattice $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$.

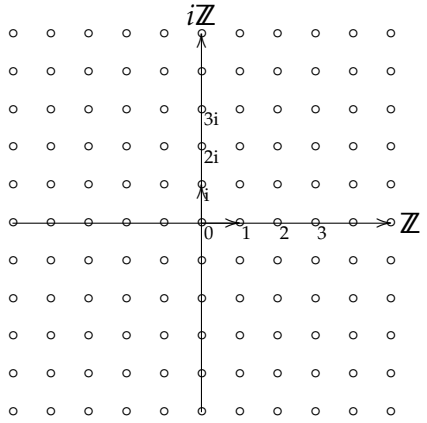


FIGURE 3.2. The lattice of Gauss integers $\mathbb{Z} + i\mathbb{Z}$.

We are interested in meromorphic[3] functions over $\mathbb{C}$ that are periodic with the lattice L.

[3]In complex analysis, a *meromorphic* function on an open subset $\mathcal{S}$ of the complex plane is a function that is *holomorphic* on all $\mathcal{S}$ except a set of isolated points, which are poles for the function. Recall that holomorphic functions are functions defined on an open subset of the complex number plane $\mathbb{C}$ with values in $\mathbb{C}$ that are complex-differentiable at every point. A function $f : \mathcal{U} \to \mathbb{C}$ from an open subset $\mathcal{U}$ of $\mathbb{C}$ to $\mathbb{C}$ is complex-differentiable at a point $z_0 \in \mathcal{U}$ if the limit

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0},$$

exists.

Definition 3.2 (Doubly Periodic Function). The function f is said to be *doubly periodic* if it is such that:

$$f:\ \mathbb{C} \longrightarrow \mathbb{C} \cup \infty$$
$$f(z+\omega) = f(\omega),$$

$\forall\, z \in \mathbb{C}, \omega \in L$. □

Such functions are easy to build-up. An example is given by the Weierstrass $\wp$-function:

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right). \tag{3.1}$$

Proposition 3.1. *Given a lattice L and the Weierstrass $\wp$-function of equation* (3.1) *the following holds.*

1. *The sum defining $\wp_L(z)$ converges absolutely and uniformly on compact sets not containing elements of L.*
2. *$\wp_L(z)$ is meromorphic in $\mathbb{C}$ and has a double pole at each $\omega \in L$.*
3. *$\wp(-z) = \wp(z)$ for all $z \in \mathbb{C}$.*
4. *$\wp(z+\omega) = \wp(z)$ for all $\omega \in L$.*
5. *The set of doubly periodic functions for L is $\mathbb{C}(\wp, \wp')$. In other words every doubly periodic function is a rational function of $\wp$ and its derivative $\wp'$.*

□

The proof of this proposition is very simple, but it is beyond the scope of this notes; so the interested reader is addressed to [**31, 51**]. Now we manipulate the term in the summation of equation (3.1):

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \omega^{-2}\left(\frac{1}{(1-z/\omega)^2} - 1 \right) =$$
$$= \omega^{-2}\left(\sum_{n=1}^{+\infty} (n+1)\frac{z^n}{\omega^n} \right),$$

and thus

$$\wp_L(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \sum_{n=1}^{+\infty} (n+1)\frac{1}{\omega^{n+2}} z^n,$$

which is a power series. Define the *Eisenstain series* to be:

$$G_k = G_k(L) = \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-k},$$

then it is easy to check, summing over ω first, than over n, that:

$$\wp_L(z) = \frac{1}{z^2} + \sum_{j=1}^{+\infty} (2j+1) G_{2j+2} z^{2j}. \tag{3.2}$$

PROPOSITION 3.2. *Let $\wp_L(z)$ be the Weierstrass $\wp$-function for a lattice L. Then:*

$$(\wp'_L(z))^2 = 4\wp^3_L(z) - 60G_4\wp_L(z) - 140G_6. \tag{3.3}$$

PROOF. From equation (3.2) we have:

$$\wp_L(z) = z^{-2} + 3G_4z^2 + 5G_6z^4 + \cdots$$
$$\wp'_L(z) = -2z^{-3} + 6G_4z + 20G_6z^3 + \cdots$$

Cubing and squaring these two equations yields:

$$\wp^3_L(z) = z^{-6} + 9G_4z^2 + 15G_6 + \cdots$$
$$(\wp'_L(z))^2 = 4z^{-6} - 24G_4z^{-2} - 80G_6 + \cdots$$

Therefore:

$$f(z) = (\wp'_L(z))^2 - 4\wp^3_L(z) + 60G_4\wp_L(z) + 140G_6 = c_1z + c_2z^2\cdots,$$

is a power series with no constant term and with no negative powers of z. But the only poles of $f(z)$ are at the poles of $\wp_L(z)$ and $\wp'_L(z)$, namely the elements of L. Since $f(z)$ is doubly periodic and has no pole at 0, we must conclude that $f(z)$ has no poles. So an application of the Liouville[4] theorem[**51**] tells us that $f(z)$ is constant. Since the power series for $f(z)$ has no constant term, $f(0) = 0$. Hence $f(z)$ is identically zero. □

Let $g_2 = 60G_4$ and $g_3 = 140G_6$; equation (3.3) is telling us that:

$$(\wp'_L(z))^2 = 4\wp^3_L(z) - g_2\wp_L(z) - g_3,$$

i. e. the points of the form $(\wp_L(z), \wp'_L(z))$ lie on the curve:

$$E:\ Y^2 = 4X^3 - g_2X - g_3.$$

Furthermore one can show that the discriminant $\Delta_E = 16(g_2^3 - 27g_3^2)$ is not zero. So we have a map from $z \in \mathbb{C}$ to the points with complex coordinates $(\wp_L(z), \wp'_L(z))$ on an elliptic curve. Since $\wp_L(z)$ and $\wp'_L(z)$ depend only on z mod L, we have a map from the torus[5] $\mathbb{C}/L$ to $E(\mathbb{C})$. The group $\mathbb{C}/L$ is a group, with the group law being addition of complex numbers modulo L. The result is indeed quite deeper[**31, 51**]:

---

[4]The Liouville theorem is a classical result in complex analysis:

THEOREM 3.3 (Liouville). *Every holomorphic function f for which there exists a positive number M such that $|f(z)| \leq M$, for all $z \in \mathbb{C}$ is constant.* □

[5]The parallelogram defined by the vertices 0, ω_1 and ω_2 of figure 3.1 is called the *fundamental parallelogram*. The quotient of $\mathbb{C}$ by $\mathbb{Z} \times \mathbb{Z}$ maps the complex plane into the fundamental parallelogram; that is, every point $z \in \mathbb{C}$ can be written as $z = r + m\omega_1 + n\omega_2$ for integers m, n and with a point r in the fundamental parallelogram. Since this mapping identifies opposite sides of the parallelogram as being the same, the fundamental parallelogram has the topology of a torus.

THEOREM 3.4. *Let L be a lattice and E be the elliptic curve*[6] $Y^2 = X^3 + AX + B$ *(with $A = -4g_2$ and $B = -16g_3$); the map:*

$$\begin{aligned} \phi : \ \mathbb{C}/L &\longrightarrow E(\mathbb{C}) \\ z &\mapsto (4\wp_L(z), 4\wp'_L(z)) \\ 0 &\mapsto \infty, \end{aligned}$$

is a group homomorphism. □

On the other hand, it is possible to show[**31**] that a point $P \in E(\mathbb{C})$ is mapped on the elliptic integral:

$$P \in E(\mathbb{C}) \mapsto \int_\infty^P \frac{dX}{\sqrt{X^3 + AX + B}} \in \mathbb{C}/L. \tag{3.4}$$

EXAMPLE 3.2. The situation described above has an equivalence of simple interpretation if we take $L \subset \mathbb{R}$ and $L = \omega\mathbb{Z}$. The functions:

$$\cos\left(\frac{\omega t}{2\pi}\right) \qquad \sin\left(\frac{\omega t}{2\pi}\right),$$

have the property to be periodic with respect to the lattice L. Furthermore there exists an explicit link between these functions, namely:

$$\sin^2(t) + \cos^2(t) = 1 = \sin^2(t) + \left(\frac{d}{dt}\sin(t)\right)^2,$$

which is the equivalent of equation (3.3). Also the result of theorem 3.4 is valid, since there is a group homomorphism such that:

$$\begin{aligned} \phi : \ \mathbb{R}/L &\longrightarrow C(X, Y) \\ t &\mapsto (\cos(t), \sin(t)), \end{aligned}$$

being $C(X, Y)$ the circle of equation $X^2 + Y^2 = 1$. Finally,

$$P = (x, y) \in C(X, Y) \mapsto \arcsin(t) = \int_0^t \frac{dX}{\sqrt{1 - X^2}} \in \mathbb{R}/L,$$

is the equivalent of equation (3.4). Hence to sum up:

$$\begin{gathered} \wp(z) \longleftrightarrow \sin(z) \\ Y^2 = X^3 + AX + B \longleftrightarrow X^2 + Y^2 = 1 \\ \int_\infty^P \frac{dX}{\sqrt{X^3 + AX + B}} \longleftrightarrow \int_0^z \frac{dX}{\sqrt{1 - X^2}}. \end{gathered}$$

□

[6] We can manipulate the equation of the elliptic curve $E : \ Y^2 = 4X^3 - g_2X - g_3$:

$$\begin{aligned} 16Y^2 = (4Y)^2 &= 16(4X^3 - g_2X - g_3) = \\ &= (4X)^3 + (-4g_2)(4X) + (-16g_3) = \\ &= X^3 + AX + B, \end{aligned}$$

with $A = -4g_2$ and $B = -16g_3$.

Theorem 3.4 tells us that every elliptic curve is indeed a torus; now we consider isomorphisms of elliptic curves. Let $L \subset \mathbb{C}$ be a lattice and $\lambda \in \mathbb{C}$. The lattice λL is called *blow-up* of the lattice L (or L's *homothety*). The functions $\wp_L(z)$ and $\wp_{\lambda L}(z)$ are, in general, different and so, a priori, it could seem that the elliptic curve isomorphic to $\mathbb{C}/L$ is different from that one isomorphic to $\mathbb{C}/\lambda L$, but

$$G'_k = G_k(\lambda L) = \sum_{\substack{\omega \in \lambda L \\ \omega \neq 0}} \omega^{-k} = \frac{1}{\lambda^k} \sum_{\substack{\omega \in L \\ \omega \neq 0}} \omega^{-k};$$

hence, if the torus $\mathbb{C}/L$ is isomorphic to the elliptic curve $E: \ Y^2 = X^3 + AX + B$ (with $A = -4g_2$ and $b = -16g_3$), the torus $\mathbb{C}/\lambda L$ is isomorphic to the curve $E': \ Y^2 = X^3 + A'X + B'$, and we have:

$$A' = -4g'_2 = (-4) \cdot 60G'_4 = \frac{1}{\lambda^4} \cdot (-4 \cdot 60)G_4 = \frac{1}{\lambda^4} A$$

$$B' = -16g'_3 = (-16) \cdot 140G'_6 = \frac{1}{\lambda^6} \cdot (-16 \cdot 140)G_4 = \frac{1}{\lambda^6} B,$$

so that $E \simeq E'$. Thus by theorem 3.4 there is a bijection:

$$\left\{ \begin{matrix} \text{Elliptic curves } E(\mathbb{C}) \\ \text{up to} \\ \text{isomorphisms} \end{matrix} \right\} \longleftrightarrow \left\{ \begin{matrix} \text{Tori } \mathbb{C}/L \\ \text{up to} \\ \text{homotheties} \end{matrix} \right\}.$$

This link implies a lot of advantages, since it make possible to use the means of mathematical analysis. In particular one can show[**51**]:

Proposition 3.5. *Let $E(\mathbb{C})$ be the elliptic curve over $\mathbb{C}$ which corresponds to the torus $\mathbb{C}/L$. Then:*

$$End(E) \simeq \{\lambda \in \mathbb{C} : \ \lambda L \subset L\}.$$

□

The set above[7] is the set of complex numbers which keeps the lattice L stable. This consequence is very deep; since $(\mathbb{C}, +)$ is a group and L is a sub-group of $\mathbb{C}$, $(\mathbb{C}/L, +)$ has the natural structure of group induced by the structure of the group $(\mathbb{C}, +)$. Thus, saying that the set of elliptic curves over $\mathbb{C}$ (up to isomorphisms) and the set of tori $\mathbb{C}/L$ (up to L's homotheties) are isomorphic implies that also the two operation of addition (the former is the one which takes place on the curve $E(\mathbb{C})$, the latter is the canonical summation of $\mathbb{C}$) must be one the equivalent of the other. So the morphism $[n] \in End(E)$ corresponds to the multiplication by n in $\mathbb{C}/L$, which is quite simpler.

We explicitly point out that:

$$\mathbb{Z} \subset \{\lambda \in \mathbb{C} : \ \lambda L \subset L\}.$$

[7] It is easy to check that the set $\mathcal{L} = \{\lambda \in \mathbb{C} : \ \lambda L \subset L\}$ is indeed a ring, since if $\lambda, \mu \in \mathcal{L}$ we have:

$$(\lambda + \mu)L \subset L, \quad \lambda\mu L \subset L, \quad (-\lambda)L \subset L.$$

In fact let $b \in \mathbb{Z}$ be an integer and let $n\omega_1 + m\omega_2$ be the generic element of L, if we evaluate $b(n\omega_1 + m\omega_2)$ we obtain:

$$b(n\omega_1 + m\omega_2) = (bn)\omega_1 + (bm)\omega_2 \in L \quad \forall\, b \in \mathbb{Z},$$

so that $\mathbb{Z} \subset \{\lambda \in \mathbb{C} : \ \lambda L \subset L\}$.

Now let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice and let

$$\tau = \frac{\omega_2}{\omega_1};$$

since ω_1 and ω_2 are linearly independent over $\mathbb{R}$, τ cannot be real and without loss of generality we can assume $\Im(\tau) > 0$. Thus τ lies in the *upper half plane* $\mathcal{H} = \{x + iy \in \mathbb{C} : \ y \geq 0\}$ and the lattice $L' = \mathbb{Z} + \tau\mathbb{Z}$ is homothetic to L. In other words the tori $\mathbb{C}/L$ and $\mathbb{C}/L'$ correspond to isomorphic curves which (thus) share the ring of isomorphisms $End(E)$. It is easy to see that $End(E) \subset L'$, since for each complex number $\lambda \in End(E)$ we have $\lambda \cdot 1 \in \mathbb{Z} + \tau\mathbb{Z}$. Hence $End(E)$ is a subring of $\mathbb{C}$, it contains $\mathbb{Z}$ and it is discrete; we have only two possibilities:

(1) $End(E) = \mathbb{Z}$.
(2) $End(E)$ is an *order*.

Definition 3.3 (Order). An *order* over $\mathbb{C}$ is a subring of $\mathbb{C}$ whose additive subgroup is a lattice. □

Since $\mathbb{C}$ is a ring with unit ($1 \in \mathbb{C}$) and since an order is a subring of $\mathbb{C}$, each order has a unit and this is the same unit of $\mathbb{C}$; thus a lattice without unit cannot be an order.

Example 3.3. The lattice $2\mathbb{Z}[i]$ of figure 3.3 is not an order, since $1 \notin 2\mathbb{Z}[i]$. The lattice of Gauss integers $\mathbb{Z}[i]$ of figure 3.2, instead, is an order, since it contains the unit 1. □

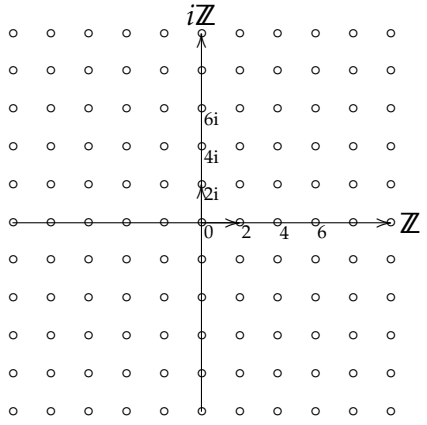


Figure 3.3. An example of a lattice that is not an order: $2\mathbb{Z}[i]$.

Now we classify the orders in $\mathbb{C}$.

Proposition 3.6. *For each order $R \subset \mathbb{C}$, $\exists!\ \Delta \in \mathbb{Z}_{<0}$, with $\Delta \equiv 0, 1 \pmod 4$, such that we can write:*

$$R = \mathbb{Z} + \delta\mathbb{Z}$$
$$\delta = \begin{cases} \dfrac{\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is even} \\ \dfrac{1+\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is odd.} \end{cases}$$

Proof. Since an order is, by definition, a lattice, it always exists a basis for which we can write:

$$R = \mathbb{Z} + \tau\mathbb{Z} \qquad \tau \in \mathcal{H}.$$

Furthermore R is a ring and $\tau \in R$, so that τ^2 is an element of R too, i. e.

$$\tau^2 = u + v\tau \qquad u, v \in \mathbb{Z}.$$

The discriminant $\Delta = v^2 + 4u$ is less than zero (since $\tau \in \mathcal{H}$), and we have $\Delta \equiv 0, 1 \pmod 4$, since $4u \equiv 0 \pmod 4$ and a quadratic residue is either zero or one modulo 4. Solving for τ we find:

$$\tau = \frac{v + \sqrt{\Delta}}{2}.$$

Since $\Delta = v^2 + 4u$, if Δ is even (odd) v is even (odd) too; hence:

$$\tau = \begin{cases} \dfrac{v}{2} + \dfrac{\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is even} \\ \dfrac{v-1}{2} + \dfrac{1+\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is odd,} \end{cases}$$

with $\frac{v}{2}, \frac{v-1}{2} \in \mathbb{Z}$. Thus τ is an integer plus δ and there exists a basis for which we can write $R = \mathbb{Z} + \delta\mathbb{Z}$. □

Example 3.4. For $\Delta = -3, -4, -7, -8, -11, -12, \cdots$ we have:

$$\delta = \frac{1+\sqrt{-3}}{2}, i, \frac{1+\sqrt{-7}}{2}, \sqrt{-2}, \frac{1+\sqrt{-11}}{2}, \sqrt{-3}, \cdots.$$

Figure 3.4 shows the order $R = \mathbb{Z} + \frac{1+\sqrt{-3}}{2}\mathbb{Z}$. □

3.2. Elliptic Curves with Complex Multiplication

Orders are sources of *special* elliptic curves, namely elliptic curves with *complex multiplication*.

Definition 3.4. An elliptic curve over $\mathbb{C}$, $E(\mathbb{C})$, is said to have *complex multiplication* if its ring of endomorphisms is larger than $\mathbb{Z}$, i. e. if it is an order in $\mathbb{C}$:

$$End(E) = R = \mathbb{Z} + \delta\mathbb{Z},$$

with δ satisfying conditions of proposition 3.6. □

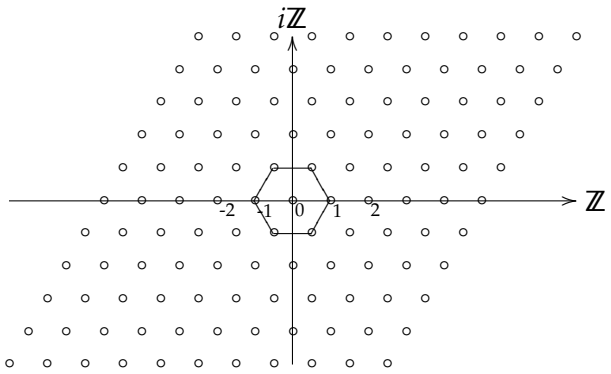


FIGURE 3.4. The order $R = \mathbb{Z} + \frac{1+\sqrt{-3}}{2}\mathbb{Z}$.

Let now $E(\mathbb{C})$ be a curve with complex multiplication, isomorphic to the torus $\mathbb{C}/L$ with L the order $L = \mathbb{Z} + \delta\mathbb{Z}$. Here we provide (without proof) some very efficient formulas to evaluate the coefficients A and B of the curve and its j-invariant. One can show[**31, 51**] that:

$$A = -3\left(1 + 240\sum_{n=1}^{+\infty}\sigma_3(n)q^n\right) = -3E_4 \tag{3.5}$$

$$B = 2\left(1 - 504\sum_{n=1}^{+\infty}\sigma_5(n)q^n\right) = 2E_6 \tag{3.6}$$

$$j(E) = \frac{\left(1 + 240\sum_{n=1}^{+\infty}\sigma_3(n)q^n\right)^3}{q\prod_{n=1}^{+\infty}(1-q^n)^{24}} = \frac{E_4^3}{\Delta}, \tag{3.7}$$

with $\sigma_r(n) = \sum_{d|n} d^r$ and $q = e^{2\pi i\delta}$. These expressions converge very quickly, for example when Δ is even we have:

$$q^n = e^{2\pi i\frac{n}{2}i\sqrt{|\Delta|}} = e^{-\pi\sqrt{|\Delta|}n} = \left(e^{-\pi\sqrt{|\Delta|}}\right)^n < \left(\frac{1}{400}\right)^n.$$

Table 3.1 shows the values of the j-invariant for different values of Δ. Note that for the first values of Δ, $j(E)$ is always an integer. This is not a case:

THEOREM 3.7. *For each order $R \subset \mathbb{C}$, the j-invariant of the curve (with complex multiplication) $E(\mathbb{C}) \simeq \mathbb{C}/R$ is an algebraic integer.* □

We recall the definition:

DEFINITION 3.5 (Algebraic Integer). The number $\alpha \in \mathbb{C}$ is *algebraic* if there exists $F(T) \in \mathbb{Q}[T]$ (with $F(T) \neq 0$) such that $F(\alpha) = 0$. If $F(T) \in \mathbb{Z}[T]$ is monic and irreducible[8], α is said to be an *algebraic integer*. □

[8]Recall that a polynomial $f(X)$ in $\varkappa[X]$ is called irreducible over $\varkappa$ if it is non-constant and cannot be represented as the product of two or more non-constant polynomials from $\varkappa[X]$.

Δ	δ	$j(E)$
-3	$\frac{1+\sqrt{-3}}{2}$	0
-4	i	1728
-7	$\frac{1+\sqrt{-7}}{2}$	-3375
-8	$\sqrt{-2}$	8000
-11	$\frac{1+\sqrt{-11}}{2}$	2^{15}
-12	$\sqrt{-3}$	-54000
-15	$\frac{1+\sqrt{-15}}{2}$	not an integer
$\dots$	$\dots$	$\dots$

TABLE 3.1. Values of $j(E)$ for the curve $E(\mathbb{C})$ (isomorphic to the torus $\mathbb{C}/L$, with $L = \mathbb{Z} + \delta\mathbb{Z}$) with complex multiplication, for different values of Δ.

EXAMPLE 3.5. The number $i \in \mathbb{C}$ is an algebraic integer, in fact $F(T) = T^2 + 1$. On the other hand, it is easy to check that $\frac{i}{2}$ is algebraic, but it is not an algebraic integer. □

COROLLARY 3.8. *If the degree of $F(T)$ is one, then $j(E)$ is an integer.*

PROOF. In fact $F(T) = T - \alpha$, with $\alpha \in \mathbb{Z}$. Since $j(E)$ is a zero of $F(T)$, it must be $j(E) = \alpha \in \mathbb{Z}$. □

Hence, to sum up, each elliptic curve over $\mathbb{C}$ is isomorphic to a torus $\mathbb{C}/L$ and the endomorphisms of $E(\mathbb{C})$ are all the complex numbers which keep the lattice L stable: $End(E) = \{\lambda \in \mathbb{C} : \lambda L \subset L\} \supset \mathbb{Z}$. Most of the times it is $End(E) = \mathbb{Z}$, but sometimes $End(E)$ is larger, i. e. it is an order $R = \mathbb{Z} + \delta\mathbb{Z}$. Note that theorem 3.7 above deals with the special case in which $L = R$ is an order and the elliptic curve $E(\mathbb{C}) \simeq \mathbb{C}/R$ is such that:

$$End(E) = \{\lambda \in \mathbb{C} : \lambda R \subset R\} = R,$$

so that $E(\mathbb{C})$ has complex multiplication. In this special case we have seen that the j-invariant is always an algebraic integer.

Now we ask which characteristics the lattice L must have, so that $\mathbb{C}/L$ is isomorphic to an elliptic curve with complex multiplication, i. e. so that $End(E)$ is an order. An example is $L = R$ (as we have just seen), for which $End(E) = R$; obviously another example is $L = cR$, with $c \in \mathbb{C}$. Since we are interested in curves up to isomorphisms we can consider the lattice of the form $L_x = \mathbb{Z} + x\mathbb{Z}$, with $x \in \mathcal{H}$. The answer to our question is given by the following proposition:

PROPOSITION 3.9. *Let R be an order with discriminant Δ and let $L_x = \mathbb{Z} + x\mathbb{Z}$ ($x \in \mathcal{H}$) be a lattice. Then the ring:*

$$End(\mathbb{C}/L_x) = \{\lambda \in \mathbb{C} : \lambda L_x \subset L_x\},$$

is equal to the order R, if and only if:

$$x = \frac{b + \sqrt{\Delta}}{2a},$$

with a and b such that there exists $c \in \mathbb{Z}$ *which satisfies:*

$$\begin{cases} b^2 - 4ac = \Delta \\ \gcd(a, b, c) = 1. \end{cases}$$

Proof. ($\Leftarrow$). Let $x = \frac{b+\sqrt{\Delta}}{2a}$, we must show that $End(\mathbb{C}/L_x) = R$. First of all we claim that the integer $\frac{b-\sqrt{\Delta}}{2}$ is an element of R. If Δ is even, $R = \mathbb{Z} + \delta\mathbb{Z}$, with $\delta = \frac{\sqrt{\Delta}}{2}$, i. e.:

$$R = \mathbb{Z} + \frac{\sqrt{\Delta}}{2}\mathbb{Z}.$$

Since $\Delta = b^2 - 4ac$ is even, b is even too and hence $\frac{b}{2} \in \mathbb{Z}$, so that:

$$\frac{b}{2} - \frac{\sqrt{\Delta}}{2} = \frac{b - \sqrt{\Delta}}{2} \in R = \mathbb{Z} + \frac{\sqrt{\Delta}}{2}\mathbb{Z}.$$

On the other hand, if Δ is odd, $R = \mathbb{Z} + \delta\mathbb{Z}$, with $\delta = \frac{1+\sqrt{\Delta}}{2}$, i. e.:

$$R = \mathbb{Z} + \frac{1 + \sqrt{\Delta}}{2}\mathbb{Z}.$$

Since $\Delta = b^2 - 4ac$ is odd, b is odd too and hence $\frac{b+1}{2} \in \mathbb{Z}$, so that:

$$\frac{b - \sqrt{\Delta}}{2} = \frac{b+1}{2} - \frac{1 + \sqrt{\Delta}}{2} \in R = \mathbb{Z} + \frac{1 + \sqrt{\Delta}}{2}\mathbb{Z}.$$

In a similar fashion, it is easy to show that $\frac{b+\sqrt{\Delta}}{2} \in R$; thus we have showed $\frac{b\pm\sqrt{\Delta}}{2} \in R$. Hence we can write:

$$R = \mathbb{Z} + \delta\mathbb{Z} = \mathbb{Z} + \frac{b - \sqrt{\Delta}}{2}\mathbb{Z} = \mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z}.$$

On the one hand we show that $R \subset \{\lambda \in \mathbb{C} : \ \lambda L_x \subset L_x\}$; note that this holds if and only if the basis $\left(1, \frac{b-\sqrt{\Delta}}{2}\right)$ of R keeps L_x stable (and hence its basis). That 1 keeps L_x stable is trivial, so it suffices to check that:

$$\frac{b - \sqrt{\Delta}}{2} \in L_x \qquad \frac{b - \sqrt{\Delta}}{2} x \in L_x,$$

since $(1, x)$ is a basis of L_x, with $x = \dfrac{b + \sqrt{\Delta}}{2a}$. Evaluating:

$$\frac{b - \sqrt{\Delta}}{2} = b \cdot 1 - a \cdot \frac{b + \sqrt{\Delta}}{2a} \in L_x$$
$$\frac{b - \sqrt{\Delta}}{2} x = \frac{b - \sqrt{\Delta}}{2} \frac{b + \sqrt{\Delta}}{2a} = \frac{b^2 - b^2 + 4ac}{4a} =$$
$$= c = c \cdot 1 + 0 \cdot \frac{b + \sqrt{\Delta}}{2a} \in L_x$$

and thus $R \subset \{\lambda \in \mathbb{C} : \ \lambda L_x \subset L_x\}$.

In a similar fashion, we can show that $\{\lambda \in \mathbb{C} : \ \lambda L_x \subset L_x\} \subset R$, so that the assertion follows easily. Let $z \in \mathbb{C}$ such that $zL_x \subset L_x$ (i. e. $z \in \{\lambda \in \mathbb{C} : \ \lambda L_x \subset L_x\}$), it suffices to point out that $z \in R$. Since $1 \in L_x$, it must be $z \in L_x$, i. e.

$$z = c + dx = c + d\frac{b + \sqrt{\Delta}}{2a} = c + \frac{d}{a}\frac{b + \sqrt{\Delta}}{2}.$$

Since we have shown that $\left(1, \frac{b+\sqrt{\Delta}}{2}\right)$ is a basis of R, we must conclude that $z \in R$ if and only if $a|d$.

Note that $z = c + dx \in \{\lambda \in \mathbb{C} : \ \lambda L_x \subset L_x\}$, so that it is obvious that both c and dx keep L_x stable. That c keeps L_x stable is trivial, as $cL_x \subset L_x$; as a consequence we have:

$$dx \in L_x \qquad dx \cdot x \in L_x,$$

since $(1, x)$ is a basis of L_x. Evaluating:

$$dx = 0 + d \cdot x \in L_x$$
$$dx^2 = d \cdot \frac{b^2 + \Delta + 2b\sqrt{\Delta}}{4a^2} = \frac{d\Delta + 2bd\sqrt{\Delta} + 2db^2 - db^2}{4a^2} =$$
$$= \frac{db}{2a^2}(\sqrt{\Delta} + b) + \frac{1}{4a^2}(d\Delta - db^2) =$$
$$= 1 \cdot \frac{d\Delta - db^2}{4a^2} + \frac{db}{a} \cdot \frac{b + \sqrt{\Delta}}{2a} \in L_x.$$

Thus it must be $\frac{db}{a} \in \mathbb{Z}$ and $\frac{d(\Delta - b^2)}{4a^2} = \frac{dc}{a} \in \mathbb{Z}$, with $c = \frac{\Delta - b^2}{4a^2}$. For this to hold a must divide (dc) and (db), i. e. $a|(d \gcd(c, b))$; but $\gcd(c, b) = 1$ by hypothesis, and $a|d$. Hence we have shown:

$$End(\mathbb{C}/L_x) = \{\lambda \in \mathbb{C} : \ \lambda L_x \subset L_x\} = R,$$

as required.

($\Rightarrow$). Similar to the other verse. □

Now it should be clear that every elliptic curve of the form $\mathbb{C}/L_x$, with $L_x = \mathbb{Z} + x\mathbb{Z}$, such that x satisfies the condition of proposition 3.9, has $End(E) = R$, being R an order of discriminant Δ, or, that is the same, $\mathbb{C}/L_x \simeq$

$E(\mathbb{C})$ with complex multiplication. Note that if we take the values of b and c fixed, there are a lot of values of a such that the conditions of proposition 3.9 are satisfied, so that it seems there are a lot of curves with complex multiplication. But we must deal with isomorphisms:

PROPOSITION 3.10. *Let $L_x = \mathbb{Z} + x\mathbb{Z}$ and $L'_x = \mathbb{Z} + x'\mathbb{Z}$ be two lattices. Then $\mathbb{C}/L_x \simeq \mathbb{C}/L'_x$ if and only if there exists a matrix $\mathcal{M} = \begin{pmatrix} \alpha & \beta \\ \gamma & \epsilon \end{pmatrix} \in SL_2(\mathbb{Z})$ such that[9]:*

$$x' = \frac{\alpha x + \beta}{\gamma x + \epsilon}.$$

PROOF. Since $\mathcal{M} \in SL_2(\mathbb{Z})$ we can evaluate its inverse:

$$\mathcal{M}^{-1} = \begin{pmatrix} \epsilon & -\beta \\ -\gamma & \alpha \end{pmatrix}.$$

($\Leftarrow$). Let $L_x = \mathbb{Z} + x\mathbb{Z}$, we apply the transformation defined by the matrix $\mathcal{M}$ to the basis $(1, x)$ of L_x:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \epsilon \end{pmatrix} \cdot \begin{pmatrix} x \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha x + \beta \\ \gamma x + \epsilon \end{pmatrix}.$$

Hence $L_x = (\alpha x + \beta)\mathbb{Z} + (\gamma x + \epsilon)\mathbb{Z}$ and

$$L'_x = \frac{1}{\gamma x + \epsilon} L_x = \mathbb{Z} + \frac{\alpha x + \beta}{\gamma x + \epsilon}\mathbb{Z} = \mathbb{Z} + x'\mathbb{Z},$$

is homeothetic to L_x. As a consequence[10] $\mathbb{C}/L_x \simeq \mathbb{C}/L'_x$.

($\Rightarrow$). It is a classical argument, see [**31**]. □

Now let us define the equivalence relation:

$$x \varrho x' \quad \Leftrightarrow \quad \exists\, \mathcal{M} = \begin{pmatrix} \alpha & \beta \\ \gamma & \epsilon \end{pmatrix} \in SL_2(\mathbb{Z}) : \; x' = \frac{\alpha x + \beta}{\gamma x + \epsilon}.$$

Fixed an order R (and then fixed a value of Δ) we consider the set:

$$Cl(\Delta) = \{x = \tfrac{b+\sqrt{\Delta}}{2a} : \; a, b, c \in \mathbb{Z}, \Delta = b^2 - 4ac, \gcd(a, b, c) = 1\}/\varrho.$$

This set characterize all the integers x which satisfies the properties of proposition 3.9, up to the action of the matrix $\mathcal{M} \in SL_2(\mathbb{Z})$ which yields

[9] Recall that the *special linear group* of degree n over a field $\varkappa$, namely $SL_n(\varkappa)$, is the set of $n \times n$ matrices with determinant 1, with the group operations of ordinary matrix multiplication and matrix inversion.

[10] Let us suppose that L_x is such that $\mathbb{C}/L_x$ has complex multiplication, i. e. $L_x = \mathbb{Z} + x\mathbb{Z}$ with x which satisfies the properties of proposition 3.9. If x' is chosen following the rules of proposition 3.10, $L'_x = \mathbb{Z} + x'\mathbb{Z}$ is such that $\mathbb{C}/L_x \simeq \mathbb{C}/L'_x$, so that $\mathbb{C}/L'_x$ must be with complex multiplication. This implies, as it is straightforward to check, that x' satisfies the conditions of proposition 3.9 too.

homeothetic lattices; hence there is a bijection:

$$\left\{\begin{array}{c}\text{Elliptic curves } E(\mathbb{C})\\ \text{with}\\ \text{complex multiplication}\\ \text{up to isomorphisms}\end{array}\right\} \longleftrightarrow Cl(\Delta).$$

There is a theorem by Gauss which is very important and whose proof is beyond the scope of this notes:

THEOREM 3.11 (Gauss). *$Cl(\Delta)$ is finite and in particular:*

$$\#Cl(\Delta) = h(\Delta),$$

being $h(\Delta)$ the class numbers of Δ (of R). Furthermore, if $F(T)$ is the minimum monic and irreducible polynomial satisfied by the j-invariant $j(E)$ of $\mathbb{C}/R$, then $deg(F(T)) = h(\Delta)$ and the zeroes of $F(T)$ are the j-invariant of all the elliptic curves with complex multiplication over R:

$$F(T) = \prod\left(T - j\left(\frac{b+\sqrt{\Delta}}{2a}\right)\right) \qquad \textit{with } \frac{b+\sqrt{\Delta}}{2a} \in Cl(\Delta),$$

and $F(T) \in \mathbb{Z}[T]$. □

EXAMPLE 3.6. $\Delta = -3, -4, -7, -8, \cdots$. For $\Delta = -4$ we can choose $b = 0$, $a = 1$ and $c = 1$ so that:

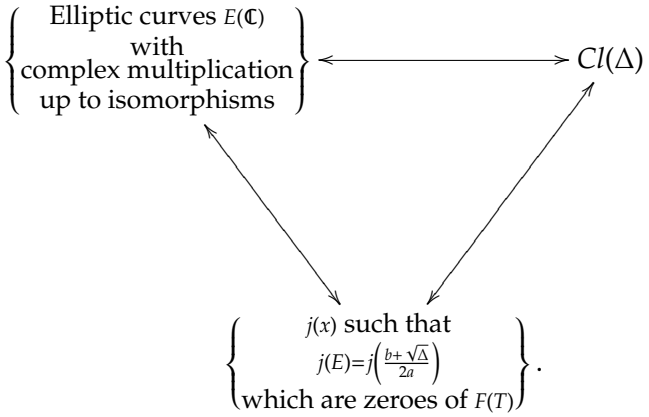
$$\begin{aligned}&\#Cl(-4) = h(-4) = 1\\ &x = \frac{b+\sqrt{\Delta}}{2a} = i\\ &F(T) = T - j(i) = T - j\left(\frac{b+\sqrt{\Delta}}{2a}\right) = T - 1728.\end{aligned}$$

For $\Delta = -15$ we have $Cl(\Delta) = \{a, b, c : \ (a = 1, b = 1, c = 4), (a = 2, b = 1, c = 2)\}$, thus:

$$\begin{aligned}&\#Cl(-15) = h(-15) = 2\\ &x_1 = \frac{1+\sqrt{-15}}{2} \qquad x_2 = \frac{1+\sqrt{-15}}{4}\\ &F(T) = (T - j(x_1))\,(T - j(x_2)) \in \mathbb{Z}[T],\end{aligned}$$

but $j(x_1), j(x_2) \notin \mathbb{Z}$. □

Hence theorem 3.11 is telling us that there is another bijection with the set of j-invariants which are zeroes of $F(T)$:



CHAPTER 4

$E(\mathbb{Z}_p)$ Points Counting

Contents

In this chapter we present the most efficient algorithms for the computation of the cardinality of the group $E(\mathbb{Z}_p)$. As we have seen in section 2.4, equation (2.8) gives us a formula for evaluating $\#E(\mathbb{Z}_p)$; to evaluate the summation requires p steps, so we have exponential complexity $O(p) = O(e^{\log(p)})$. In the following we describe three others (more efficient) algorithms: the *Baby-Steps and Giant-Steps* algorithm, *Schoof*'s algorithm and *Atkin*'s algorithm.

4.1. Baby-Steps and Giant-Steps

The crucial idea behind this algorithm is due to Shanks[**44**]. Let $E: Y^2 = X^3 + AX + B$ a non-singular elliptic curve over $\mathbb{Z}_p$ and let $N = \#E(\mathbb{Z}_p)$; Hasse's theorem 2.17 tells us that N lies in the interval $\mathcal{I} = [p - 1 - 2\sqrt{p}, p - 1 + 2\sqrt{p}]$; furthermore by Lagrange's theorem we know that $NP = \infty$. The key idea is to consider a point $P \in E(\mathbb{Z}_p)$ and to look for the point NP (see figure 4.1); the easiest way is to try all values of N in the range $\mathcal{I}$ and see which one satisfies $NP = \infty$. This takes around $4\sqrt{p}$ steps; Shanks' idea allows to speed up this approach.

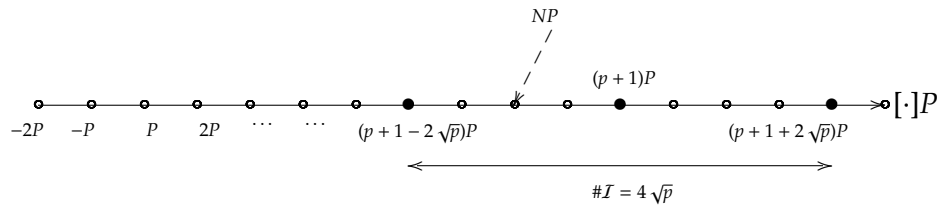


FIGURE 4.1. Baby-steps and giant-steps.

Let $a \approx \sqrt{2}p^{1/4}$, we evaluate and store in a list the *baby-steps*:

$$\pm P, \pm 2P, \pm 3P, \cdots, \pm aP.$$

Then we compute the center of the critical interval $\mathcal{I}$, namely $R = (p+1)P$; if the point R belongs to the list of baby-steps, it is straightforward to deduce the value of N. If this is not the case we compute the *giant-steps*:

$$R \pm Q, R \pm 2Q, R \pm 3Q, \cdots, R \pm tQ,$$

with $Q = (2a+1)P$ and $t = \left\lfloor 2\sqrt{p}/(2a+1) \right\rfloor$; by Hasse's theorem one of the point $R + iQ$, for some $i = 0, \pm 1, \pm 2, \cdots, \pm t$, will be equal to one of the elements of our baby-steps' list. Hence,

$$R + iQ = jP,$$

for some $j \in \{0, \pm 1, \pm 2, \cdots, \pm a\}$ and $i \in \{0, \pm 1, \pm 2, \cdots, \pm t\}$. Thus:

$$\begin{aligned} & (p + 1 + i(2a+1) - j)P = \infty \\ \Rightarrow \quad & N = \#E(\mathbb{Z}_p) = p + 1 + i(2a+1) - j. \end{aligned}$$

The algorithm fails if there are two distinct integers N and N' in the interval $\mathcal{I}$, such that $NP = N'P = \infty$; this rarely happens in practice. If it does, then $(N - N')P = \infty$ and one knows the order d of P; so it suffices to repeat the algorithm with another random point of $E(\mathbb{Z}_p)$: the fact that $d|N$, usually, speed up the second computation considerably. Mestre's algorithm[**14**] provide a trick to avoid this complication.

Now we look at computational cost. Baby-steps cost a additions, so we have $O(a \log^3(p))$. To evaluate $R = (p+1)P$ costs $O(\log(p) \log^3(p))$, using the binary expansion of $p + 1$. Giant-steps requires (at most) $2t = 4\sqrt{p}/(2a+1)$ steps, so we have $O(\frac{4\sqrt{p}}{2a} \log^3(p))$. It is important that one can efficiently search among the points in the list of baby steps; one should sort this list or use some kind of *hash coding*[1]. Note that if a is small we will need just a few baby-steps and much more giant-steps; on the other hand if a is large, the situation is tipped over. The optimum choice is to balance the load and take $a = 4\sqrt{p}/(2a)$, which yields $a = \sqrt{2}p^{1/4}$. Hence the complexity is dominated by:

$$\text{Running-Time} \;\Rightarrow\; O(p^{1/4} \log^3(p)),$$

which is reasonable if $p < 10^{25}$.

Example 4.1. We show the Shanks' algorithm in action, by computing the cardinality of $E(\mathbb{Z}_{557})$, for the curve $E: Y^2 = X^3 - 10X + 21$. First of all we

[1] A *hash table* is a data structure for storing a set of items, so that we can quickly determine whether an item is in the set or not. The basic idea is to pick a hash function $h(\cdot)$ that maps every possible item x to a small integer $h(x)$. Then we store x in slot $h(x)$ in an array. The array is the hash table.

find a point $P \in E(\mathbb{Z}_p)$; for example we choose $P = (2, 3)$. Let $a \approx \sqrt{2}p^{1/4} \approx 5$, we evaluate the baby-steps:

$$\begin{aligned} P &= (2,3) & -P &= (2,-3) \\ 2P &= (58,164) & -2P &= (58,-164) \\ 3P &= (44,294) & -3P &= (44,-294) \\ 4P &= (56,339) & -4P &= (56,-339) \\ 5P &= (132,364) & -5P &= (132,-364). \end{aligned}$$

Note that $ord(P) > 5$. Now we compute the center of interval $\mathcal{I}$, finding:

$$R = (p+1)P = (557+1)P = 578P = (418, 33),$$

which does not belong to the list.

Now we start evaluating the giant-steps:

$$\begin{aligned} R + Q &= (58,164) & R - Q &= (238,63) \\ R + 2Q &= (137,252) & R - 2Q &= (538,6) \\ R + 3Q &= \cdots & R - 3Q &= \cdots. \end{aligned}$$

Hence $(R + Q) = (p + 1 + (2a + 1))P \equiv 2P$, i. e. $i = 1$ and $j = 2$, and

$$\#E(\mathbb{Z}_p) = N = p + 1 + (2a + 1)i - j = 557 + 1 + 11 - 2 = 567.$$

□

4.2. Schoof's Algorithm

Schoof's algorithm[**42**] is the first deterministic and polynomial algorithm for evaluating $\#E(\mathbb{Z}_p)$. Since Hasse's theorem tells us that $\#E(\mathbb{Z}_p) = p + 1 - t$ with $|t| < 2\sqrt{p}$, if we succeed in evaluating t, we are done. Schoof's idea is to evaluate t modulo all the primes ℓ less than or equal to a certain bound L and to use the *Chinese Remainder Theorem*[2] to obtain the desired value of t. If

$$\prod_{\substack{\ell \le L \\ \ell \text{ prime}}} \ell \ge 4\sqrt{p},$$

[2]The Chinese Remainder Theorem is a result about congruences in number theory and its generalizations in abstract algebra.

THEOREM 4.1 (Chinese Remainder Theorem[**29**]). *Let $n_1, n_2, \cdots, n_k$ be positive integers, with $\gcd(n_i, n_j) = 1$ whenever $i \neq j$, and let $a_1, a_2, \cdots, a_k$ be any integers. Then the solutions of the simultaneous congruences*

$$x \equiv a_1 \pmod{n_1}, \quad x \equiv a_2 \pmod{n_2}, \quad \ldots, \quad x \equiv a_k \pmod{n_k},$$

form a single congruence class modulo n, where $n = \prod_{i=1}^{k} n_i$. □

the value of t modulo the product of the values ℓ is unique. By the *Prime Number Theorem* (see appendix A) we have:

$$\prod_{\substack{\ell \le L \\ \ell \text{ prime}}} \ell \approx e^L > 4\sqrt{p}$$
$$\Rightarrow \quad L = \log(4\sqrt{p}) = O(\log(p)).$$

Hence the primes ℓ are less than $\log(p)$ (and this is obvious) and we need at most $\log(p)$ of these values ℓ. Note that if $p \approx 10^{500}$, $\ell < 1000$. Now we show the joint of the algorithm in the trivial case when $\ell = 2$. We recall a theorem[**10**] from abstract algebra:

THEOREM 4.2 (Cauchy). *If $\mathbb{G}$ is a finite group and ℓ is a prime, then $\ell | \#G$ if and only if $\exists\, g \in \mathbb{G}$ with $ord(g) = \ell$.* □

Let us consider the elliptic curve $E : \ Y^2 = X^3 + AX + B$; we already know, by equation (2.2), that points (x, y) of order two of $E(\mathbb{Z}_p)$ are such that $y = 0$, so that the abscissa x must be a zero of $X^3 + AX + B$. If we are in $\overline{\mathbb{Z}}_p$ there always are 3 zeroes, but if we restrict our attention to $\mathbb{Z}_p$ we must pay attention that the point (x, y) belongs to $E(\mathbb{Z}_p)$. Since $\mathbb{Z}_p = \left\{\alpha \in \overline{\mathbb{Z}}_p : \ \alpha^p \equiv \alpha \pmod p\right\}$ by Fermat's little theorem, the point (x, y) is a point of $E(\mathbb{Z}_p)$ of order two if and only if x is both a zero of $X^3 + AX + B$ and $X^p - X$. Thus we compute:

$$\gcd(X^p - X, X^3 + AX + B);$$

if the result is not 1, there exists an element of order $\ell = 2$, and theorem 4.2 implies $\#E(\mathbb{Z}_p) = p + 1 - t \equiv 0 \pmod 2$, so that $t \equiv 0 \pmod 2$ since $p + 1$ is even. If, instead, the result is 1, there are no points of order $\ell = 2$ and $t \equiv 1 \pmod 2$. This completes the description of the case $\ell = 2$. Note that the size of p, namely $p \approx 10^{500}$, makes hard the calculation of the gcd. However we can refer to the key idea of the euclidean algorithm and evaluate:

$$\gcd(X^3 + AX + B, (X^p - X) \bmod (X^3 + AX + B)),$$

which yields the same result. Definitely we must be able to evaluate X^p in the quotient ring $\mathbb{Z}_p[X]/(X^3 + AX + B)$, which is finitely generate and with order p^3, since the remainder of the division by $X^3 + AX + B$ has degree (at most) two, i. e. it is a polynomial with 3 coefficients and each coefficient is an element of $\mathbb{Z}_p$. Hence we need a memory space of $3\log(p) = O(\log(p))$ to store an element of $\mathbb{Z}_p[X]/(X^3 + AX + B)$; furthermore multiplication requires $9\log^2(p) = O(\log^2(p))$ steps and to compute a p-th power requires $\log(p)(3\log(p))^2 = O(\log^3(p))$ steps, as the time needed to evaluate one gcd. Thus all have polynomial complexity.

Now we deal with the general case $\ell > 2$; it should be clear that here we need points of order ℓ, so that the analysis is much more complicated.

Consider the group of points of order ℓ:

$$E[\ell] = \left\{P \in E(\overline{\mathbb{Z}}_p) : \ [\ell]P = \infty\right\},$$

which is a sub-group of $E(\overline{\mathbb{Z}}_p)$. As we have seen in section 2.1, equations (2.2) and (2.4) represent an explicit formula for the cases when $\ell = 2, 3$; so we can conclude that, for each ℓ, there is a polynomial whose zeroes are the elements of $E[\ell]$. The general case is dealt with by the following proposition:

Proposition 4.3. *Let E be an elliptic curve over $\mathbb{Z}_p$ and $\ell > 2$ be a prime such that $p \nmid \ell$. Then $E[\ell]$ is isomorphic to $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and there exists a polynomial $\Psi_\ell(X)$ whose zeroes are exactly the points of $E[\ell]$ (less than the point at infinity). Furthermore:*

$$deg(\Psi_\ell) = \frac{\ell^2 - 1}{2}.$$

Proof. The idea is to write $E[\ell]$ as the kernel of an endomorphism; since $E[\ell]$ is, by definition, the set of elements in $E(\overline{\mathbb{Z}}_p)$ such that $[\ell]P = \infty$ we have:

$$E[\ell] = Ker([\ell]).$$

Now we claim that, if $\ell \neq p$ (that is our case since $\ell \nmid p$ and ℓ, p are both primes), then $[\ell]$ is separable. If this holds, the assertion is proven since, by corollary 2.11:

$$\begin{aligned} \#E[\ell] = \#Ker([\ell]) = deg_{sep}([\ell]) = \\ = [\text{see example 2.17}] = deg([\ell]) = \ell^2, \end{aligned}$$

but the only two groups of order ℓ^2, with ℓ a prime, are $\mathbb{Z}_{\ell^2}$ and $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and since there are no elements of order ℓ^2 in $E[\ell]$ (i. e. all the elements are nullified by $[\ell]$) we must conclude $E[\ell] \simeq \mathbb{Z}_\ell \times \mathbb{Z}_\ell$. Thus since $deg([\ell]) = \ell^2$, the points (x, y) of $E[\ell]$ are such that x is a zero of a polynomial Ψ_ℓ whose degree is $deg(\Psi_\ell) = \frac{\ell^2-1}{2}$, since $\#E[\ell] = \ell^2$ and since $E[\ell]$ is made up of opposite points (i. e. points with the same abscissa) plus the point at infinity (that is not a zero of Ψ_ℓ).

Now it remains to show that $[\ell]$ is separable. We claim that $[\ell]$ is separable only if $[p]$ is not, i. e. if the formulas defining $[p]$ are p-th powers. Since $\gcd(\ell, p) = 1$ we have, by Bézout's identity:

$$\begin{aligned} & a\ell + bp = 1 \qquad \text{for some } a, b \in \mathbb{Z} \\ \Rightarrow \quad & a[\ell] + b[p] = [1]. \end{aligned}$$

Hence if $[p]$ is not separable, $[\ell]$ must be separable, otherwise the identity morphism $[1]$ would be not separable, that is not true.

Thus it remains to show that $[p]$ is not separable. Let *Frob* be the Frobenius endomorphism; its dual isogeny is such that $Frob^\vee Frob = [deg(Frob)] =$

$[p]$. Since $Frob^\vee$ is a morphism, it is such that:

$$Frob^\vee = \left(\frac{H_1(X,Y)}{H_2(X,Y)}, \frac{H_3(X,Y)}{H_4(X,Y)}\right),$$

with H_i $(i = 1, \cdots, 4)$ polynomials. Hence

$$[p](X,Y) = (Frob^\vee Frob)(X,Y) = \left(\left(\frac{H_1(X,Y)}{H_2(X,Y)}\right)^p, \left(\frac{H_3(X,Y)}{H_4(X,Y)}\right)^p\right),$$

and $[p]$ is not separable. □

Example 4.2. When $\ell = 3$ we already know, by equation (2.4), that:

$$\Psi_3(X) = 3X^4 + 6AX^2 + 12BX + A^2 \quad \text{and} \quad deg(\Psi_3) = \frac{3^2 - 1}{2} = 4.$$

□

The polynomials $\Psi_\ell(X)$ are called *division polynomials* and can be evaluated in a recursive fashion[3].

We now estimate the complexity[4] associated with the evaluation of Ψ_ℓ; to compute the morphism $[i](x,y)$ implies to evaluate two polynomials of degree $deg([i]) = i^2$ in the elements x and y. Hence we need a memory space of $O(i^2 \log(p))$ bits. Since the computation of:

$$[i+1](x,y) = [i](x,y) + (x,y),$$

[3]We recall the following general result:

Theorem 4.4 ([**51**]). *Let E be given by $Y^2 = X^3 + Ax + B$, over a field whose characteristic is not 2. Then we can write:*

$$[n]P = \left(\frac{\phi_n(X,Y)}{\Psi_n^2(X,Y)}, \frac{\omega_n(X,Y)}{\Psi_n^3(X,Y)}\right).$$

The functions ϕ_n, ω_n and Ψ_n in $\mathbb{Z}[X,Y]$ are defined recursively by:

$$\begin{aligned}
\Psi_0 &= 0\\
\Psi_1 &= 1\\
\Psi_2 &= 2Y\\
\Psi_3 &= 3X^4 + 6AX^2 + 12BX - A^2\\
\Psi_4 &= 4Y(X^6 + 5AX^4 + 20BX^3 - 5A^2X^2 - 4ABX - 8B^2 - A^3)\\
\Psi_{2n+1} &= \Psi_{n+2}\Psi_n^3 - \Psi_{n-1}\Psi_{n+1}^3\\
\Psi_{2n} &= \frac{\Psi_n}{2Y}\left(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2\right),
\end{aligned}$$

and

$$\begin{aligned}
\phi_n &= X\Psi_n^2 - \Psi_{n+1}\Psi_{n-1}\\
\omega_n &= \frac{1}{4Y}\left(\Psi_{n+2}\Psi_{n-1}^2 - \Psi_{n-2}\Psi_{n+1}^2\right).
\end{aligned}$$

□

[4]As it will be clear in the following the bottleneck of the algorithm is the last part, thus the computation of the polynomials Ψ_ℓ can be done in the simplest (but less efficient) way.

has a cost of $O(i^2 \log(p) \log(p)) = O(i^2 \log^2(p))$ steps, the complexity associated with the evaluation of $[\ell]P$ is:

$$\sum_{i=1}^{\ell} i^2 \log^2(p) = O(\ell^3 \log^2(p)),$$

i. e. $O(\log^5(p))$, since $\ell < \log(p)$. Thus the time needed to evaluate $\Psi_\ell(X, Y)$ is $O(\log^5(p))$ and the memory requirement is $O(\ell^2 \log(p))$.

The last part of the algorithm is based on the following result:

PROPOSITION 4.5. *Let $\tau \in \mathbb{Z}$. Then:*

$$\left(X^{p^2}, Y^{p^2}\right) + [p](X, Y) = [\tau]\left(X^p, Y^p\right) \tag{4.1}$$

in $\mathbb{Z}_p[X, Y]/\left(Y^2 - X^3 - AX - B, \Psi_\ell(X)\right)$, if and only if $\tau \equiv t \pmod{\ell}$.

PROOF. ($\Leftarrow$). This direction is trivial; in fact we already know, by proposition 2.14 that each morphism f is such that it satisfies an equation of the kind $f^2 - [t]f + [d] = 0$, with $d = deg(f)$. In particular when $f = Frob$:

$$\begin{aligned} & Frob^2 - [t]Frob + [p] = 0 \\ \Rightarrow \quad & \left(X^{p^2}, Y^{p^2}\right) - [t]\left(X^p, Y^p\right) + [p] = 0 \end{aligned}$$

and if $\tau \equiv t \pmod{\ell}$ we can conclude

$$\left(X^{p^2}, Y^{p^2}\right) - [\tau]\left(X^p, Y^p\right) + [p] = 0.$$

($\Rightarrow$). Since we have:

$$\left(X^{p^2}, Y^{p^2}\right) + [p](X, Y) = [\tau]\left(X^p, Y^p\right)$$

in $\mathbb{Z}_p[X, Y]/\left(Y^2 - X^3 - AX - B, \Psi_\ell(X)\right)$, and since it must be:

$$\left(X^{p^2}, Y^{p^2}\right) + [p](X, Y) = [t]\left(X^p, Y^p\right),$$

we can conclude that

$$[t]\left(X^p, Y^p\right) = [\tau]\left(X^p, Y^p\right),$$

in $\mathbb{Z}_p[X, Y]/\left(Y^2 - X^3 - AX - B, \Psi_\ell(X)\right)$. Note that $f(X) \equiv f'(X) \pmod{g(X)}$, implies $f(X) = f'(X) + h(X)g(X)$ (for some polynomial $h(X)$) and thus if $g(\alpha) = 0$ we have $f(\alpha) = f'(\alpha)$. Here the situation is identical: if (α, β) is a solution of both the equations which generate the ideal $\left(Y^2 - X^3 - AX - B, \Psi_\ell(X)\right)$ (i. e. if $(\alpha, \beta) \in E(\mathbb{Z}_p) \cap E[\ell]$), we can write:

$$[t]\left(\alpha^p, \beta^p\right) = [\tau]\left(\alpha^p, \beta^p\right),$$

$\forall\ (\alpha, \beta) \in E(\mathbb{Z}_p) \cap E[\ell]$. Thanks to the fact that we are in $E(\mathbb{Z}_p)$ we have:

$$\begin{aligned} & [t](\alpha, \beta) = [\tau](\alpha, \beta) \\ \Rightarrow \quad & [t - \tau](\alpha, \beta) = \infty \\ \Rightarrow \quad & (\alpha, \beta) \in Ker([t - \tau]). \end{aligned}$$

Hence $Ker([\ell]) \subset Ker([t-\tau])$ and there exists (and it is unique) the dual isogeny of $[\ell]$, such that

$$[\ell]^{\vee}[\ell] = [t-\tau],$$

that is possible only if ℓ divides $t-\tau$, i. e. only if $\tau \equiv t \pmod{\ell}$. □

Thus, for each value of $2 < \ell < L$ the algorithm tries the values $\tau = 3, 4, \cdots, \ell - 1$ and checks if relation (4.1) is satisfied; the value of τ which satisfies that relation is such that $t \equiv \tau \pmod{\ell}$. To sum up Schoof's algorithm proceeds as follow:

(1) We choose an integer L, such that:

$$\prod_{\substack{\ell<L \\ \ell \text{ prime}}} \ell > 4\sqrt{p}.$$

As we have seen the size of each prime ℓ is $O(\log(p))$ and the numbers of such primes is $O(\log(p))$.

(2) We evaluate $t \bmod 2$.

(3) We compute the *division polynomials* Ψ_ℓ for each value of ℓ.

(4) For each prime $\ell = 3, 5, 7, \cdots$ we look for the value of $\tau \in [0, \ell - 1]$ such that:

$$Frob^2 - [\tau]Frob + [p] = 0,$$

which happens only if:

$$\left(X^{p^2}, Y^{p^2}\right) + [p](X, Y) = [\tau]\left(X^p, Y^p\right),$$

in $\mathbb{Z}_p[X, Y]/\left(Y^2 - X^3 - AX - B, \Psi_\ell(X)\right)$. This value of τ is such that $t \equiv \tau \pmod{\ell}$ by proposition 4.5.

(5) Finally we build-up the value of $t \bmod \prod_{\ell<L} \ell$ by the Chinese Remainder Theorem, which yields $\#E(\mathbb{Z}_p)$.

It remains to estimate the complexity of the algorithm. Consider step 4 of the algorithm, we have already seen that each element of the quotient set $\mathbb{Z}_p[X, Y]/\left(Y^2 - X^3 - AX - B, \Psi_\ell(X)\right)$ requires $O(\ell^2 \log(p))$ bits to be represented, so that to evaluate a p^2-th power requires a number of steps given by

$$O(\log^2(p)(\ell^2 \log(p))^2) = O(2\ell^4 \log^3(p)),$$

just like the evaluation of $[p]$. Hence the running-time needed to evaluate the left member of equation (4.1) is $2O(2\ell^4 \log^3(p)) = O(\ell^4 \log^3(p))$, which is $O(\log^7(p))$ since $\ell < \log(p)$. Note that this complexity dominates the one associated with the evaluation of Ψ_ℓ. In a similar fashion the running-time evaluation of the right member of equation (4.1) is:

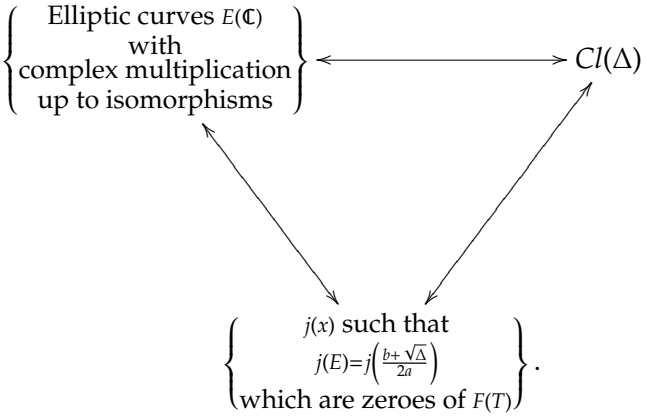
$$O(\ell(\ell^2 \log(p))^2) = O(\ell^5 \log^2(p)) = O(\log^7(p)).$$

Since we have to repeat step 4 for each prime $\ell < \log(p)$ the total complexity is:

$$\text{Running-Time: } \Rightarrow \quad O(\log(p) \log^7(p)) = O(\log^8(p)).$$

4.3. Atkin's Algorithm

We have studied the (very basic) properties of elliptic curves with complex multiplication in section 3.2. In particular we have seen that there is a bijection:



Furthermore, by theorem 3.11, we know that $F(T) \in \mathbb{Z}[T]$, so that we can reduce $F(T)$ modulo a prime p. The following proposition, whose proof uses a little bit of *class field theory*[5] and that is beyond the scope of this notes, is of central importance:

Proposition 4.6. *Let R be an order of discriminant Δ and let p be a prime. If Δ is a quadratic residue modulo p, the following statements are equivalent.*

(1) *The polynomial $F(T)$ associated with the order R has one zero in $\mathbb{Z}_p$.*
(2) *The polynomial $F(T)$ associated with the order R has all the zeroes in $\mathbb{Z}_p$.*
(3) *$\exists\, \varphi \in R$ such that $|\varphi|^2 = p$.*

□

Thus, given an order R and a prime p, if we succeed in finding a value $\varphi \in R$ such that $|\varphi|^2 = p$, then $F(T) \in \mathbb{Z}[T]$ has all its zeroes on $\mathbb{Z}_p$; since the zeroes of $F(T)$ are all the j-invariants of the elliptic curves with complex multiplication over R, we can write:

$$F(j_0) \equiv 0 \pmod{p},$$

being $j(E) = j_0$ the j-invariant of an elliptic curve $E(\mathbb{C})$ with complex multiplication over R. The surprising fact is that, if we reduce the curve $E(\mathbb{C})$ modulo p, we find a curve $E(\mathbb{Z}_p)$ that is still a curve with complex multiplication[6]:

$$End(E(\mathbb{Z}_p)) \simeq R.$$

[5] Class field theory is a major branch of algebraic number theory; see [3] for an introduction.

[6] This result, that we stated informally, is indeed a theorem by Deuring.

Consider now the Frobenius endomorphism over $E(\mathbb{Z}_p)$; recall that:

$$Frob^2 - [t]Frob + [p] = 0$$
$$Frob \cdot Frob^\vee = [p]$$
$$Frob + Frob^\vee = [t]$$
$$Ker(Frob - id) = E(\mathbb{Z}_p),$$

and thus

$$\Rightarrow \quad \#E(\mathbb{Z}_p) = \#Ker(Frob - id) = deg(Frob - id).$$

We need a lemma:

LEMMA 4.7 ([**31**]). *Let E be an elliptic curve with complex multiplication over an order R. If $c \in R \subset \mathbb{C}$ is the element corresponding to a given morphism f, then c^* is the element of R associated with the dual isogeny of f.* □

Let thus $\varphi \in R$ be the element corresponding to the Frobenius endomorphism, we can write:

$$Frob \cdot Frob^\vee = [p] \quad \Leftrightarrow \quad \varphi\varphi^* = p,$$

so that since $(Frob - id)(Frob - id)^\vee = [deg(Frob - id)]$ we can conclude that

$$\#E(\mathbb{Z}_p) = deg(Frob - id) = (\varphi - 1)(\varphi - 1)^* = |\varphi - 1|^2.$$

This is Atkin's idea: once you have found the value $\varphi \in R$ which corresponds to $Frob \in End(E)$ for the elliptic curve $E(\mathbb{Z}_p)$ with complex multiplication[7] over R, it is straightforward to evaluate $\#E(\mathbb{Z}_p)$. The problem is that, agreeing with proposition 4.6, there could be more values $\varphi \in R$ such that $|\varphi|^2 = p$; in other words we are not sure that a number φ which satisfies the condition of proposition 4.6 corresponds to the Frobenius endomorphism, we only know that there is a bijection:

$$Frob \in End(E) \quad \longleftrightarrow \quad \varphi \in R \text{ such that } |\varphi|^2 = p.$$

EXAMPLE 4.3. Let $p = 5$ and $R = \mathbb{Z}[i]$. A value $\varphi \in R$ is of the form $\varphi = a + b \cdot i$, with $a, b \in \mathbb{Z}$. Hence $|\varphi|^2 = p$ if and only if $a^2 + b^2 = 5$. As it is showed in figure 4.2, the solutions are given by the intersection of the lattice $\mathbb{Z}[i]$ and a circle of radius $\sqrt{5}$. In particular, if $\varphi \in R$ is a solution, $-\varphi$, φ^*, $-\varphi^*$, $i\varphi$, $-i\varphi$, $i\varphi^*$ and $-i\varphi^*$ are solutions too. □

Thus now, fixed an order R of discriminant Δ and a prime p, we look for all the elements φ of R such that $|\varphi|^2 = p$. The key property is that these values of φ are just a few:

PROPOSITION 4.8. *Let $R \subset \mathbb{C}$ be an order of discriminant Δ and p a prime. Then:*

[7] This idea is suitable for the evaluation of $\#E(\mathbb{Z}_p)$ when $E(\mathbb{Z}_p)$ is an elliptic curve over $\mathbb{Z}_p$ with complex multiplication. So its validity may seem limited; in spite of that we will see that this idea plays a role of central importance in the Atkin-Goldwasser-Kilian primality proving algorithm.

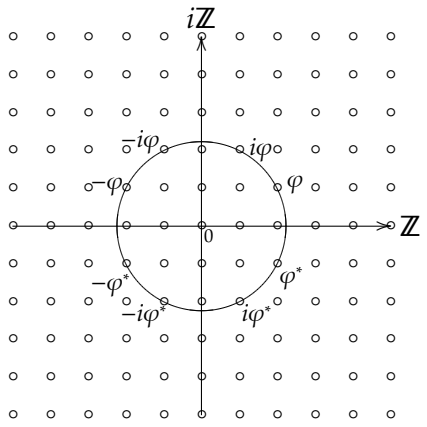


FIGURE 4.2. Solutions of the equation $a^2 + b^2 = 5$.

(1) *$u \in R$ is invertible in R if and only if $uu^* = 1$.*
(2) *If $\varphi \in R$ is such that $|\varphi|^2 = p$, then the ideal generated by φ in R is a prime ideal*[8].
(3) *If $\exists\ \varphi \in R$ such that $|\varphi|^2 = p$, then φ is uniquely determined, up to conjugation and multiplication by units.*

PROOF. (1). Clearly, if $uu^* = 1$, u is invertible in R and $u^{-1} = u^*$. On the other hand, let us suppose that u is invertible, i. e. there exists $v \in R$ such that $uv = 1$. Thus it is also $u^*v^* = 1$ and we can write:

$$(uv)(u^*v^*) = 1(uu^*)(vv^*).$$

Since $u \in R$ we know that it is of the form:

$$u = a + b\delta \qquad \delta = \begin{cases} \dfrac{\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is even} \\ \dfrac{1+\sqrt{\Delta}}{2} & \text{if } \Delta \text{ is odd.} \end{cases}$$

Let us suppose that Δ is even; hence

$$uu^* = \left(a + b\frac{\sqrt{\Delta}}{2}\right)\left(a - b\frac{\sqrt{\Delta}}{2}\right) = a^2 - b^2\frac{\Delta}{4},$$

[8]We recall the definition of *prime ideal*.

DEFINITION 4.1 (Prime Ideal). An ideal $\mathcal{I} \neq R$ of a ring $(R, +, \cdot)$ is *prime*, if for each $a, b \in R$

$$a \cdot b \in \mathcal{I} \quad \Rightarrow \quad a \in \mathcal{I} \text{ or } b \in \mathcal{I}.$$

□

which is an element of $\mathbb{Z}$ since $\Delta \equiv 0 \pmod 4$. On the other hand, if Δ is odd

$$\begin{aligned} uu^* &= \left(a + b \cdot \frac{1+\sqrt{\Delta}}{2}\right)\left(a + b \cdot \frac{1-\sqrt{\Delta}}{2}\right) = \\ &= \left(a + \frac{b}{2} + \frac{\sqrt{\Delta}}{2}b\right)\left(a + \frac{b}{2} - \frac{\sqrt{\Delta}}{2}b\right) = \\ &= \left(a + \frac{b}{2}\right)^2 - \frac{\Delta}{4}b^2 = a^2 + ab + b^2\left(\frac{1-\Delta}{4}\right), \end{aligned}$$

which is an element of $\mathbb{Z}$, since $\Delta \equiv 1 \pmod 4$. Thus $uu^*, vv^* \in \mathbb{Z}$, but $(uu^*)(vv^*) = 1$, so that it must be $uu^* = vv^* = 1$.

Before proving (2) we determine the units of R. Let Δ be even, then:

$$uu^* = a^2 - \frac{b^2}{4}\Delta = a^2 + \frac{b^2}{4}|\Delta|,$$

and this must be equal to 1 if we want u to be a unit. If $|\Delta| > 4$, it must be $b = 0$, so that $a = \pm 1$ and $u = \pm 1$. Let us suppose that $|\Delta| = 4$, then $a^2 + b^2 = 1$ and hence:

$$\begin{cases} a = \pm 1 \\ b = 0 \end{cases} \quad \text{or} \quad \begin{cases} a = 0 \\ b = \pm 1 \end{cases}$$

which yields $u = \pm 1$ or $u = \pm i$. On the other hand, let us suppose that Δ is odd, then:

$$uu^* = a^2 + ab + b^2\frac{1+|\Delta|}{4},$$

and this must be equal to 1 if we want u to be a unit. If $|\Delta| > 3$, it should be $uu^* = a^2 + ab + cb^2 = 1$, with $c \geq 2$, thus it is easy to check that this requires $b = 0$, so that $u = \pm 1$. Let us suppose that $|\Delta| = 3$, we find:

$$uu^* = a^2 + ab + b^2 = 1;$$

one solution is $b = 0$ and $a = \pm 1$, which yields $u = \pm 1$. If $b = \pm 1$ and $a = 0$ we have:

$$u = 0 + \frac{1 \pm \sqrt{-3}}{2} = \frac{1 \pm \sqrt{-3}}{2}.$$

Finally we can also take $a = -1$ which yields:

$$\begin{aligned} a = -1 \quad &\Rightarrow \quad 1 - b + b^2 = 1 \quad \Rightarrow \quad b(b-1) = 0 \\ &\Rightarrow \quad u = -1 + \frac{1+\sqrt{-3}}{2} = \frac{-1+\sqrt{-3}}{2} \end{aligned}$$

and $b = -1$ which yields:

$$\begin{aligned} b = -1 \quad &\Rightarrow \quad a^2 - a + 1 - 1 = 0 \quad \Rightarrow \quad a(a-1) = 0 \\ &\Rightarrow \quad u = \frac{-1-\sqrt{-3}}{2}. \end{aligned}$$

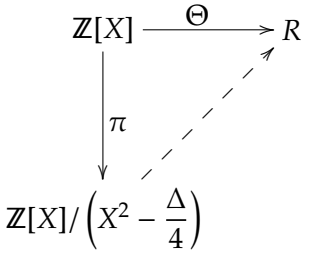
We have hence determined all the units in R:

$$u = \begin{cases} \pm 1 & \text{if } |\Delta| > 4 \\ \pm 1, \pm i & \text{if } |\Delta| = 4 \\ \pm 1, \dfrac{\pm 1 \pm \sqrt{-3}}{2} & \text{if } |\Delta| = 3. \end{cases}$$

(2). Let $\varphi \in R$ be such that $|\varphi|^2 = p$, being p a prime. The ideal generated by φ is prime if and only[9] if $R/(\varphi)$ is an integral domain. In the following we discuss only the case when Δ is even (the case of odd Δ is similar); thus let $R = \mathbb{Z} + \frac{\sqrt{\Delta}}{2}$ and let Θ be the map:

$$\Theta : \ \mathbb{Z}[X] \longleftrightarrow R$$
$$f(x) \mapsto f\left(\frac{\sqrt{\Delta}}{2}\right) \in R.$$

Note that $Ker(\Theta)$ is the ideal generated by $X^2 - \frac{\Delta}{4}$, namely $Ker(\Theta) = (X^2 - \frac{\Delta}{4})$. Hence, by the fundamental homomorphism theorem for rings:



$$\Rightarrow R \simeq \mathbb{Z}[X]/\left(X^2 - \frac{\Delta}{4}\right).$$

Moreover $\varphi \in R$ is such that $\varphi = a + b\frac{\sqrt{\Delta}}{2}$ is mapped through Θ into the element $a + bX$ of $\mathbb{Z}[X]$. Thus

$$R/(\varphi) \simeq \mathbb{Z}[X]/\left(X^2 - \frac{\Delta}{4}, a + bX\right).$$

Now we evaluate the ideal $\left(X^2 - \frac{\Delta}{4}, a + bX\right)$. First of all

$$\left(X^2 - \tfrac{\Delta}{4}, a + bX\right) = \left(X^2 - \tfrac{\Delta}{4}, a + bX, p\right),$$

since $a^2X^2 - \frac{\Delta}{4}a^2$ belongs to the ideal and hence also $p = \varphi\varphi^* = a^2 - \frac{\Delta}{4}b^2$ is an element of the ideal. Note that $\frac{a^2}{b^2} \equiv \frac{\Delta}{4} \pmod{p}$, so that $(a + bX) \big| \left(X^2 - \frac{\Delta}{4}\right)$; as a consequence

$$R/(\varphi) \simeq \mathbb{Z}[X]/\left(a + bX, p\right) \simeq \mathbb{Z}_p[X]/(a + bX) \simeq \mathbb{Z}_p.$$

Since $\mathbb{Z}_p$ is a field, and hence an integral domain, the ideal (φ) is prime.

[9] We recall the following important fact.

THEOREM 4.9 ([**10**]). *Let R be a commutative ring and let $\mathcal{I}$ be an ideal of R. Then $\mathcal{I}$ is a prime ideal if and only if $R/\mathcal{I}$ is an integral domain.* □

(3). It is quite obvious that φ is unique up to conjugation, since if $|\varphi|^2 = p$, then also $|\varphi^*|^2 = p$. Further φ is unique up to multiplication by units, since if u is a unit (i. e. if $|u|^2 = 1$) we have $|u\varphi|^2 = |u||\varphi|^2 = p$. Let now φ, ψ be two element of R such that $|\varphi|^2 = |\psi|^2 = p$, but $\psi \neq \varphi, \varphi^*, u\varphi$. Thus $\psi\psi^* = \varphi\varphi^*$, so that $\varphi|(\psi\psi^*)$ and since φ generates a prime ideal we can conclude that either $\varphi|\psi$ or $\varphi|\psi^*$, i. e. either $v\varphi = \psi$ or $w\varphi = \psi^*$. Hence

$$\begin{aligned} & |\psi| = |v||\varphi| = |\psi^*| = |w||\varphi| \\ \Rightarrow \quad & |v| = |w| \\ \Rightarrow \quad & \psi = \varphi. \end{aligned}$$

□

Definitely, if $E(\mathbb{Z}_p)$ is an elliptic curve such that $End(E) = R$, being R an order of discriminant Δ, i. e. if E has complex multiplication over R, and if Δ is a quadratic residue modulo p (with p a prime), we know by proposition 4.6 that there exists a value $\varphi \in R$ such that $|\varphi|^2 = p$. Moreover we have shown in proposition 4.8 that if such a value of φ exists, then it must be unique up to conjugation and multiplication by units. Hence:

$$\#E(\mathbb{Z}_p) = \begin{cases} |\pm\varphi - 1|^2 & \text{if } |\Delta| > 4 \\ |\pm\varphi - 1|^2, |\pm i\varphi - 1|^2 & \text{if } |\Delta| = 4 \\ |\pm\varphi - 1|^2, |\frac{\pm 1 \pm \sqrt{-3}}{2}\varphi - 1|^2 & \text{if } |\Delta| = 3. \end{cases} \tag{4.2}$$

Note that this result is perfectly compatible with the isomorphism classes of $E(\mathbb{Z}_p)$, as we have discussed in section 2.5. In particular the case $|\Delta| = 3$ corresponds to $j(E) = 0$ for which there are up to 6 isomorphism classes, the case $|\Delta| = 4$ corresponds to $j(E) = 1728$ for which there are up to 4 isomorphism classes and the case $|\Delta| > 4$ corresponds to $j(E) \neq 0, 1728$ for which there are only 2 isomorphism classes, the one represented by E and the one represented by its twist. Thus, given the equation of an elliptic curve over $\mathbb{Z}_p$ (with complex multiplication over an order R) for which we want to determine the cardinality, it suffices to find a value $\varphi \in R$ such that $|\varphi|^2 = p$ and to use equation (4.2) (with the proper value of Δ) to evaluate $\#E(\mathbb{Z}_p)$. In this way, in the worst case, we must choose between 6 values; the choice is straightforward, since it suffices to take a point $P \in E(\mathbb{Z}_p)$ and to use Lagrange's theorem to check that:

$$P^{\#E(\mathbb{Z}_p)} = \infty.$$

We conclude this section presenting an algorithm able to find the desired value of φ. Given an order $R = \mathbb{Z} + \delta\mathbb{Z} \subset \mathbb{C}$ and a prime integer p, we want to determine an element $\varphi \in R$ such that $|\varphi|^2 = p$.

Example 4.4. As we have already seen in a previous example if $R = \mathbb{Z}[i]$, $\varphi = a + ib$ must be such that $a^2 + b^2 = p$, so that the problem is the same of writing p as a sum of 2 squares. □

The idea we discuss in the following is due to the Italian mathematician G. Cornacchia[**15**] and it is called *Cornacchia's algorithm*. We need a lemma:

LEMMA 4.10. *If such an element φ exists, then Δ must be a quadratic residue modulo p.*

PROOF. Let us suppose that Δ is even, so that $\varphi = a + b\frac{\sqrt{\Delta}}{2}$, with $a, b \in \mathbb{Z}$. Hence,

$$\begin{aligned} & \varphi\varphi^* = a^2 - \frac{\Delta}{4}b^2 = p \\ \Rightarrow \quad & a^2 - \frac{\Delta}{4}b^2 \equiv 0 \pmod{p} \\ \Rightarrow \quad & \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2 \equiv \frac{\Delta}{4} \pmod{p} \end{aligned}$$

and thus Δ is a quadratic residue modulo p (the division by b is allowed, because $p \nmid b \in \mathbb{Z}$ and then b is invertible in $\mathbb{Z}_p$).

On the other hand, let us suppose that Δ is odd, so that $\varphi = a + \frac{1+\sqrt{\Delta}}{2}b$ with $a, b \in \mathbb{Z}$. Hence,

$$\begin{aligned} & \varphi\varphi^* = a^2 + ab + b^2\left(\frac{1-\Delta}{4}\right) = p \\ \Rightarrow \quad & a^2 + ab + \frac{b^2}{4} - \frac{\Delta}{4}b^2 \equiv 0 \pmod{p} \\ \Rightarrow \quad & 4a^2 + 4ab + b^2 \equiv b^2\Delta \pmod{p} \\ \Rightarrow \quad & \Delta \equiv 4\left(\frac{a}{b}\right)^2 + 4\left(\frac{a}{b}\right) + 1 = \left(2\frac{a}{b} + 1\right)^2 \pmod{p} \end{aligned}$$

and thus Δ is a quadratic residue modulo p (the division by b is still valid since $a^2 + ab + b^2(1-\Delta)/4 = p$ implies $p \nmid b \in \mathbb{Z}$). □

Hence, the first step of the algorithm is to test whether Δ is a quadratic residue modulo p or not. This is possible evaluating:

$$\Delta^{\frac{p-1}{2}} \equiv \begin{cases} +1 & \text{if } \Delta \in \mathbb{Z}_p^2 \\ -1 & \text{if } \Delta \notin \mathbb{Z}_p^2 \\ 0 & \text{if } p|\Delta, \end{cases} \pmod{p},$$

which implies a complexity of $O(\log^3(p))$. The next step is the computation of a square root of Δ modulo p, that can be done using either the Cantor-Zassenhaus or the Tonelli-Shanks algorithms of section 2.2 (both with polynomial complexity). Now suppose we have determined $t \equiv \sqrt{\Delta} \pmod{p}$; we show a way to evaluate (if there exists) $\varphi = a + b\delta \in R$ such that $|\varphi|^2 = p$. Let $0 < t < 2p$ and let us suppose $\Delta \neq 0$ and $p \neq 2$. We take the succession of the remainders of the euclidean algorithm with inputs t and

$2p$:

$$\begin{aligned} x_0 &= 2p = r_0 \\ x_1 &= t = r_1 \\ x_2 &= \text{remainder of the division of } x_0 \text{ by } x_1 = r_1 \\ &\cdots \\ x_{k+1} &= \text{remainder of the division of } x_{k-1} \text{ by } x_k = r_k \\ &\cdots \\ \gcd(2p, t) &= 1, 2 = r_n, \end{aligned}$$

where the last equality holds since $\gcd(p, t) = 1$. Let j be the minimal integer such that $x_j < 2\sqrt{p}$, then if there axists $z \in \mathbb{Z}$ such that

$$x_j^2 - 4p = \Delta z^2,$$

we can write:

$$\varphi = \frac{x_j + z\sqrt{\Delta}}{2} \in R.$$

When Δ is even the equations are even simpler. Indeed, since $t^2 \equiv \Delta \pmod{p}$, $(p-t)^2 \equiv \Delta \pmod{p}$ too, but since t is even, $p - t$ is odd (and viceversa), so that $t \equiv \Delta \pmod{2}$. Hence if Δ is even, t is even too and we can write $\left(\frac{t}{2}\right)^2 = (t')^2 \equiv \frac{\Delta}{4} \pmod{p}$, so that:

$$\begin{aligned} x_0 &= p = r_0 \\ x_1 &= t' = r_1 \\ x_2 &= \text{remainder of the division of } x_0 \text{ by } x_1 = r_1 \\ &\cdots \\ x_{k+1} &= \text{remainder of the division of } x_{k-1} \text{ by } x_k = r_k \\ &\cdots \\ \gcd(p, t') &= 1 = r_n. \end{aligned}$$

Thus, if x_j is the minimal value such that $x_j < \sqrt{p}$ and if there exists $z \in \mathbb{Z}$ such that

$$x_j^2 - p = \frac{\Delta}{4} z^2,$$

we can write:

$$\varphi = x_j + z\sqrt{\frac{\Delta}{4}} \in R.$$

Example 4.5. Take $R = \mathbb{Z}[i]$ and $p = 400009 \equiv 1 \pmod{4}$; thus $\Delta = -4$ is even and $\Delta^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, so that Δ is a quadratic residue modulo p. Now we look for the value t' such that:

$$(t')^2 \equiv \frac{\Delta}{4} \pmod{p}.$$

It is easy to check that this yields $t' \equiv 42676 \pmod{p}$. We use the euclidean algorithm:

$$\begin{aligned} x_0 &= p = 400009 \\ x_1 &= t' = 42676 \\ x_2 &= 15925 \\ x_3 &= 10826 \\ x_4 &= 5099 \\ x_5 &= 628 < \sqrt{p} \quad \Rightarrow \quad x_j = x_5. \end{aligned}$$

Note that

$$x_5^2 - p = -5625 = (-1)75^2 = \frac{\Delta}{4} z^2,$$

with $z = 75$. Finally $\varphi = 628+75i$; recall that, since $R = \mathbb{Z}[i]$ this is equivalent to write p as sum of two squares: $400009 = 75^2 + 628^2$. □

We have already observed that t and Δ are both even or odd, so that $\frac{t-\sqrt{\Delta}}{2} \in R$. Consider the lattice:

$$L = \left\{ np + m\frac{t - \sqrt{\Delta}}{2} : \ n, m \in R \right\} \subset R,$$

it is not difficult to see that L is an ideal $\mathcal{I}$ of R, i. e. if $\lambda \in R$ and $x \in \mathcal{I}$ we have $\lambda x \in \mathcal{I}$. We already know that if Δ is even $R \simeq \mathbb{Z}[X]/\left(X^2 - \frac{\Delta}{4}\right)$, so that:

$$R/\mathcal{I} \simeq \mathbb{Z}[X]/\left(X^2 - \frac{\Delta}{4}, \frac{t}{2} - X\right).$$

But,

$$\left(\frac{t}{2}\right)^2 - \frac{\Delta}{4} = \frac{t^2 - \Delta}{4} \equiv 0 \pmod{p},$$

thus $\left(\frac{t}{2} - X\right) \mid \left(X^2 - \frac{\Delta}{4}\right)$ and

$$R/\mathcal{I} \simeq \mathbb{Z}[X]/\left(X^2 - \frac{\Delta}{4}, p\right) \simeq \mathbb{Z}_p.$$

We can always generate $\mathcal{I}$ from a single element[10], i. e. $\mathcal{I} = (\varphi)$, with $\varphi = a + bi$, hence:

$$\#R/\mathcal{I} = \#\mathbb{Z}_p = p = \#R/(\varphi) = a^2 + b^2\frac{|\Delta|}{4} = \varphi\varphi^*.$$

In other words, if there exists a generator φ of $\mathcal{I}$, this is really that value $\varphi \in R$ such that $|\varphi|^2 = p$; on the other hand, if $\mathcal{I} \neq (\varphi)$, we can be sure that there are no elements $\varphi \in R$ such that $|\varphi|^2 = p$.

[10] Such an ideal is a *principal ideal*, i. e. an ideal generated by a single element.

EXAMPLE 4.6. In this example we show that Cornacchia's algorithm is suitable for solving the (more general) problem of *lattice basis reduction*[**14**]. Let $p = 41$, $R = \mathbb{Z}[i]$ and $t = 9$. Thus $\frac{t-\sqrt{\Delta}}{2} = t - i = 9 - i$ and $(41, 9 - i)$ is a basis for:

$$L = \left\{ np + m\frac{t - \sqrt{\Delta}}{2} : \ m, n \in \mathbb{Z} \right\}.$$

If we apply Cornacchia's algorithm we find $\varphi = 5 + 4i$ (which yields $41 = 5^2 + 4^2$). Let $\mathcal{I}$ be the principal ideal generated by φ:

$$\mathcal{I} = \mathbb{Z}41 + \mathbb{Z}(9 - i),$$

i. e. an element $x \in \mathcal{I}$ is such that $x = \lambda(5 + 4i)$ and $|x| = |\lambda|\sqrt{41}$. Hence φ is the smallest element of $\mathcal{I}$: the algorithm reduces the basis $(41, 9 - i)$ to a more orthogonal basis $(\varphi, i\varphi)$ with shorter vectors (see figure 4.3).

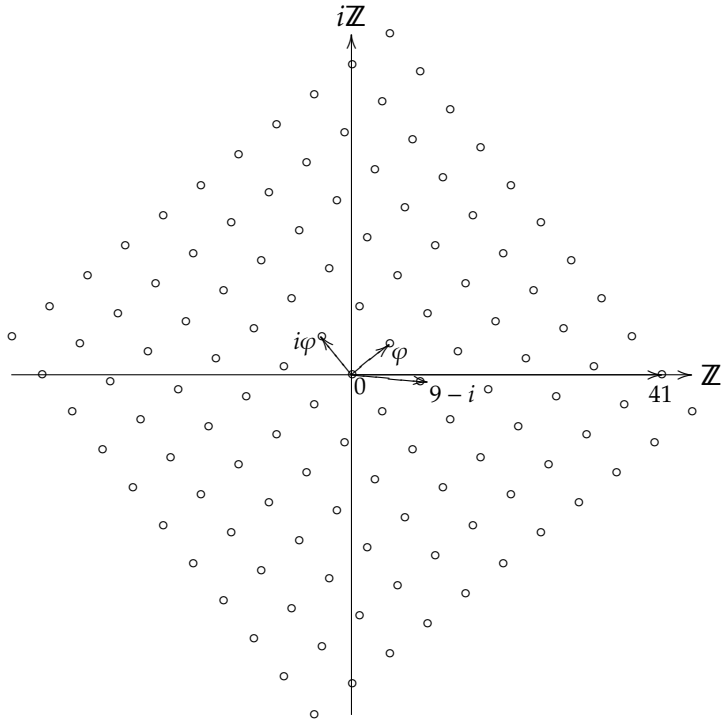


FIGURE 4.3. Lattice basis reduction for L.

The situation is quite similar to the computation of the gcd in $\mathbb{R}$:

$$n = 18, m = 12 \in \mathbb{Z} \quad \Rightarrow \quad \mathcal{I} = 18\mathbb{Z} + 12\mathbb{Z} = \gcd(12, 18)\mathbb{Z} = 6\mathbb{Z}.$$

Cornacchia's algorithm is equivalent to the computation of one gcd in R: $\gcd(p, 9 - i) = 5 + 4i$, but (a priori) we are not sure that there is a solution. □

CHAPTER 5

Primality Proving

Contents

In this chapter we deal with primality proving in general, which is very useful in cryptography. First of all we present an efficient, but probabilistic, test; then we will follow an historical survey of this task, starting from Euler and Fermat.

5.1. Miller and Rabin

The algorithm we are going to discuss is probabilistic; it proves with high probability (very quickly) that n is not prime. On the other hand, if n passes the test, it is merely likely to be prime. Repeating the basic steps of the algorithm several times, the probability that a composite number is not recognized as such can be made arbitrarily small. The original idea was an idea of Artjuhov[**4**]; then Rabin [**39**] proposed the probabilistic version. Miller[**35**] showed that, assuming the Generalized Riemann Hypothesis (GRH), the probabilistic test can be transformed into a primality *proving* test.

In a certain sense, the Miller-Rabin test tries to extend the *Fermat test*. Recall that, by Fermat's little theorem, if p is a prime then, for each $x \in \mathbb{Z}_p^*$, we have $x^{p-1} \equiv 1 \pmod{p}$. Thus, if we want to prove the primality of an odd number n we could think to choose an element $x \in \mathbb{Z}_n^*$ and check whether $x^{n-1} \equiv 1 \pmod{n}$ or not. The problem with this idea is that Fermat's little theorem gives us only a necessary condition for n primality; in fact there are numbers, called *Fermat pseudo-primes* base x, such that $x^{n-1} \equiv 1 \pmod{n}$, even if n is composite. Moreover there are numbers, called *Carmichael numbers*, such that the above relation holds for each value $x \in \mathbb{Z}_n^*$, regardless of n primality or compositeness. The idea behind the

Miller-Rabin algorithm is to improve the success probability of the Fermat test. We need a couple of lemmas:

LEMMA 5.1. *Let $p > 2$ be a prime. There are no non-trivial roots of 1 modulo p.*

PROOF. Note that 1 and -1 always yield 1 when squared modulo p; we call these elements *trivial* square roots of 1. Let us suppose that $x \in \mathbb{Z}_p$ is a non-trivial square root of 1 modulo p, then

$$x^2 \equiv 1 \pmod{p} \quad \Rightarrow \quad (x+1)(x-1) \equiv 0 \pmod{p}.$$

Since x is non-trivial, we have $x \not\equiv \pm 1 \pmod{p}$, that is to say $x+1$ and $x-1$ are coprime to p, i. e. neither $x+1$ nor $x-1$ is divisible by p. But if a prime divides neither of two integers, it cannot divide their product and we can conclude

$$(x+1)(x-1) \not\equiv 0 \pmod{p},$$

so that we have reached a contradiction. Hence the only square roots of 1 modulo p are trivial. □

LEMMA 5.2. *Let n be an odd prime, and write $n - 1 = 2^s d$, with d an odd integer and $s \geq 1$. For each $x \in \mathbb{Z}_n^*$ either $x^d \equiv 1 \pmod{n}$ or $x^{2^r d} \equiv -1 \pmod{n}$ for some $0 \leq r < s$.*

PROOF. Since n is prime, Fermat's little theorem holds and we can write $x^{n-1} \equiv 1 \pmod{n}$. Lemma 5.1 tells us that, taking square roots of x^{n-1}, we will get either 1 or -1. If we get -1 the second equality of the assertion holds and we are done; in the case when we have taken out every power of 2 and the second equality never held, that is to say $x^{2^r d} \not\equiv -1 \pmod{p}$ for each $r = 0, 1, \cdots, s-1$, we are left with the first equality which also must be equal to 1 or -1, as it too is a square root: $x^d \equiv \pm 1 \pmod{n}$. However for $r = 0$ we have $x^d \not\equiv -1 \pmod{n}$, thus in case the second equality does not hold, the first equality must. □

In analogy to pseudo-primes, we can now define a *strong pseudo-prime* base x to be an odd integer $n > 3$ for which the condition of lemma 5.2 is satisfied. If we choose a random value $x \in \mathbb{Z}_n^*$ and the condition of above lemma is not true, we can conclude that n is composite; on the other hand, if the condition is satisfied for a value x, we cannot conclude that n is prime, but n is a strong pseudo-prime base x. The hope is that possibly fewer composites pass the strong probable prime test. Here is the key ingredient:

THEOREM 5.3. *Let $n > 9$ be an odd positive composite integer. We write $n - 1 = 2^s d$ for some exponent $s \geq 1$ and some odd integer d. Let*

$$B = \left\{ x \in \mathbb{Z}_n^* : \ x^d = 1 \text{ or } x^{2^r d} = -1 \text{ for some } 0 \leq r < s \right\}.$$

Then we have

$$\frac{\#B}{\varphi(n)} \leq \frac{1}{4},$$

being $\varphi(n) = \#\mathbb{Z}_n^*$ the Euler's φ-function.

Proof. The set B can be viewed naturally as a disjoint union of certain subsets. Indeed, we have

$$\#B = \#\left\{x \in \mathbb{Z}_n^* : \ x^d \equiv 1\right\} + \sum_{r=0}^{s-1} \#\left\{x \in \mathbb{Z}_n^* : \ x^{2^r d} \equiv -1\right\}.$$

An element $x \in \mathbb{Z}_n^*$ satisfies $x^{2^r d} \equiv -1$ in $\mathbb{Z}_n^*$ if and only if $x^{2^r d} \equiv -1 \pmod{q}$ for all prime powers q dividing n. Furthermore, we have $x^{2^r d} \equiv -1 \pmod{q}$ if and only if $x^{2^{r+1} d} \equiv 1 \pmod{q}$ and $x^{2^r d} \not\equiv 1 \pmod{q}$.

For a given $r \geq 0$, there are *no* (by Lagrange's theorem) such elements unless $2r+1$ divides $q-1$ for all prime powers $q > 1$ dividing n. Since $\mathbb{Z}_q^*$ is cyclic, there are in the latter case precisely $\gcd(2^{r+1}d, \varphi(q)) - gcd(2^r d, \varphi(q)) = 2^r \gcd(d, \varphi(q))$ such elements. By the Chinese Remainder Theorem there are therefore $\prod_{q|n} 2^r \gcd(d, \varphi(q))$ elements $x \in \mathbb{Z}_n^*$ for which $x^{2^r d} \equiv -1$ in $\mathbb{Z}_n^*$.

Writing μ for the largest integer for which $2\mu + 1$ divides $q - 1$ for all prime powers q dividing n and t for the number of different primes dividing n, it follows that

$$\begin{aligned}
\#B &= \gcd(d, \varphi(n)) + \sum_{r=0}^{\mu} \prod_{q|n} 2^r \gcd(d, \varphi(q)) = \\
&= \gcd(d, \varphi(n)) + \gcd(d, \varphi(n)) \sum_{r=0}^{\mu} 2^r t = \\
&= \gcd(d, \varphi(n)) \left(1 + \frac{2^{(\mu+1)t} - 1}{2^t - 1}\right).
\end{aligned}$$

It is easy to see that the right hand side is equal to $n-1$ when n is prime. In view of the formula above, we want to show for $n \neq 9$ that

$$1 + \frac{2^{(\mu+1)t} - 1}{2^t - 1} \leq \frac{1}{4} \frac{\varphi(n)}{\gcd(d, \varphi(n))}.$$

Indeed, when $t = 1$ and $n = p^a$ for some prime p and $a \geq 2$, the left hand side is equal to 2^μ while the right hand side is $2^{\mu-2} p^{a-1}$. This means that $p^{a-1} \geq 4$, which is true when $n \neq 9$. When $t \geq 3$, we have $\gcd(d, \varphi(n)) \geq \frac{\varphi(n)}{2^{(\mu+1)t}}$ and hence the right hand side is at least $2^{(\mu+1)t-2}$. A short computation shows that the left hand side does not exceed this.

When $t = 2$ and the 2-adic[1] valuations of $\varphi(q)$ for the two prime powers of q are distinct, then we have $\gcd(d, \varphi(n)) \leq \frac{\varphi(n)}{2^{2\mu+3}}$ so that the right hand side is at least $\frac{1}{2^{2\mu+1}}$ and the inequality follows easily. Finally, when $t = 2$ and the 2-adic valuations of $\varphi(q)$ for the two prime powers of q are equal, then the fact that the two primes are different implies that the odd parts of d and $\varphi(n)$ cannot be the same. It follows that $\gcd(d, \varphi(n)) \leq \frac{\varphi(n)}{3 \cdot 2^{2\mu+2}}$ and the inequality follows easily. □

The above theorem can be transformed in a probabilistic primality testing as follows. Fix a random value $x \in \mathbb{Z}_n^*$ and check if $x \in B$. If this is not the case we can conclude that n is composite, else n is probably prime. For a single instance of the test, the probability that $x \in B$ with n composite is at most $\frac{1}{4}$; this probability can be reduced to $\left(\frac{1}{4}\right)^k$ repeating the test k times.

Checking that $x \in B$ involves raising $x \in \mathbb{Z}_n^*$ to an exponent that is no more than n. Hence, using the binary expansion of the exponent, this takes $O(\log(n)(\log(n))^\mu)$, with $\mu = 2$ when we use the usual multiplication algorithm in $\mathbb{Z}_n$ and $\mu = 1 + \epsilon$ by employing fast multiplication techniques.

Under assumption of the Generalized Riemann Hypothesis (GRH) for quadratic Dirichlet characters, the Miller–Rabin test can be transformed into a *deterministic* polynomial-time primality test.

THEOREM 5.4 (GRH). *Let n be an odd positive composite integer and write $n - 1 = 2^s d$ for some exponent $s \geq 1$ and some odd integer d. If for all integers*

---

[1]The p-adic order or additive p-adic valuation of a number n is the highest exponent v such that p^v divides n. The most important application of the p-adic order is in constructing the field of p-adic numbers**[25]**. The p-adic number systems were first described by K. Hensel in 1897.

The real numbers can be defined as equivalence classes of *Cauchy sequences* of rational numbers. Recall that a sequence $x_1, x_2, x_3, \ldots$ of real (complex or rational) numbers is called *Cauchy*, if for every positive real (complex or rational) number ε, there is a positive integer N such that for all natural numbers $m, n > N$ we have $|x_m - x_n| < \varepsilon$. However, the definition of a Cauchy sequence relies on the metric chosen and, by choosing a different one, numbers other than the real numbers can be constructed. The usual metric which yields the real numbers is called the *Euclidean metric* (i. e. the ordinary distance between two points that one would measure with a ruler, which can be proven by repeated application of the Pythagorean theorem.). For a given prime p, we define the p-adic absolute value in $\mathbb{Q}$ as follows: for any non-zero rational number x, there is a unique integer n allowing us to write $x = p^n \frac{a}{b}$, where neither of the integers a and b is divisible by p. Unless the numerator or denominator of x in lowest terms contains p as a factor, n will be 0. Now define $\|x\|_p = p^{-n}$ and $\|0\|_p = 0$. The p-adic absolute value defines a metric d_p on $\mathbb{Q}$ by setting

$$d_p(x, y) = \|x - y\|_p.$$

The field $\mathbb{Q}_p$ of p-adic numbers can then be defined as the completion of the metric space $(\mathbb{Q}, d_p)$; its elements are equivalence classes of Cauchy sequences, where two sequences are called equivalent if their difference converges to zero. In this way, we obtain a complete metric space which is also a field and contains $\mathbb{Q}$.

$1 < x < 2(\log(n))^2$ *one has:*

$$x^d \equiv 1 \pmod{n} \qquad x^{2^r d} \equiv -1 \pmod{n} \text{ for some } 0 \leq r < s,$$

then n is a prime number. □

Proof. The interested reader is addressed to [**43**]. □

5.2. Fermat and Mersenne

During $1500-1600$, before Euler and at times of Fermat, there was a few number theory and a lot of numerology. Mathematicians looked for prime numbers of special form.

Proposition 5.5. *The following holds:*

(1) *If* $2^n - 1$ *is prime, then n must be prime.*
(2) *If* $2^n + 1$ *is prime, then n is a power of* 2.

Proof. (1). Let us suppose that n is not a prime, and let $1 < d < n$ be a divisor of n and $e = 2^d - 1$. Thus

$$\begin{aligned} & 2^d - 1 = e \\ \Rightarrow \quad & 2^d - 1 \equiv 0 \pmod{e} \\ \Rightarrow \quad & 2^d \equiv 1 \pmod{e} \\ \Rightarrow \quad & \left(2^d\right)^{\frac{n}{d}} \equiv 1 \pmod{e} \\ \Rightarrow \quad & 2^n \equiv 1 \pmod{e}, \end{aligned}$$

and $2^n - 1$ is not prime.

(2). Let us suppose that n is not a power of 2, i. e. $n = 2^t m$ with $m \neq 1$ odd; then n has an odd divisor: $d|n$ and d is odd. We claim that if $e = 2^{2^t} + 1$, then $e|(2^n + 1)$ so that $2^n + 1$ is not prime. In fact:

$$\begin{aligned} & 2^{2^t} + 1 = e \\ \Rightarrow \quad & 2^{2^t} + 1 \equiv 0 \pmod{e} \\ \Rightarrow \quad & 2^{2^t} \equiv -1 \pmod{e} \\ \Rightarrow \quad & \left(2^{2^t}\right)^m \equiv (-1)^m \pmod{e} \\ \Rightarrow \quad & 2^{2^t m} \equiv -1 \pmod{e} \\ \Rightarrow \quad & 2^n + 1 \equiv 0 \pmod{e}, \end{aligned}$$

since m is odd. Hence $2^n + 1$ is composite. □

Example 5.1. The integer $2^{15} - 1 = 32767$ is divisible by $7 = 2^3 - 1$ and for $31 = 2^5 - 1$. □

Another fact of interest were the concept of *perfect number*.

Definition 5.1 (Perfect Number). A *perfect* number n, is a positive integer which is the sum of its proper positive divisors, that is, the sum of the positive divisors excluding the number itself. Equivalently, a perfect number is a number that is half the sum of all of its positive divisors (including itself). If we indicate with $\sigma(n)$ the sum of *all* positive divisors of n we can write:

$$\sigma(n) = 2n.$$

□

Example 5.2. For example $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$. □

The following result is due to Euler[2].

Proposition 5.6 (Euler). *If* $2^n - 1$ *is prime, then* $2^{n-1}(2^n - 1)$ *is perfect.*

Proof. Let $n = p^a q^b \cdots$ be the prime factorization of n, we note that all the positive divisors of n are the elements of the form $p^\alpha q^\beta \cdots$ with $\alpha = 0, 1, \cdots, a$, $\beta = 0, 1, \cdots, b$ and so on. Thus[3]

$$\sigma(n) = \sum_{\alpha=0}^{a} p^\alpha \sum_{\beta=0}^{b} q^\beta \cdots = (1 + p + \cdots p^a)(1 + q + \cdots + q^b) \cdots.$$

Now $2^n - 1$ is prime by hypothesis, so that:

$$\sigma(2^{n-1}(2^n - 1)) = (2^n - 1 + 1)(1 + 2 + 2^2 + \cdots + 2^{n-1}) =$$
$$= (2^n)(2^n - 1) = 2 \cdot 2^{n-1}(2^n - 1),$$

and $2^{n-1}(2^n - 1)$ is perfect. □

Other special numbers were *Fermat numbers* and *Mersenne numbers*.

Definition 5.2 (Mersenne Numbers). Let p be a prime. The p-th Mersenne number is $M_p = 2^p - 1$. □

Definition 5.3 (Fermat Numbers). Let $t \geq 0$. The t-th Fermat number is $F_t = 2^{2^t} + 1$. □

Note that the first part of proposition 5.5 is about Mersenne numbers' primality; in fact this proposition is telling us that if M_n is prime also n is prime, whereas if n is prime we are not sure about the primality of M_n. Moreover proposition 5.6 is equivalent to state that if M_n is a Mersenne prime, i. e. a prime of the form $M_n = 2^n - 1$, then $\frac{M_n(M_n+1)}{2}$ is a perfect number. Further during the XVII century Euler proved that all even perfect

[2]The same proposition was proved also by Euclid.

[3]Recall the summation of the geometric series:

$$\sum_{k=0}^{n} ar^k = \frac{a(1 - r^{n+1})}{1 - r}.$$

numbers are of that form, whereas it is unknown whether there are any odd perfect numbers or not. Various results have been obtained, but none that has helped to locate one or otherwise resolve the question of their existence. Carl Pomerance has presented a heuristic argument which suggests that no odd perfect numbers exist[4].

Look now at the first five Fermat numbers, namely: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$; Fermat believed that all numbers of the form $F_t = 2^{2^t} + 1$ were primes. He was wrong, but was not able to factor $F_5 = 4294967297$. The following result is due to Gauss:

THEOREM 5.7 (Gauss 1796). *Let m be a positive integer, then a regular polygon with m edges is constructible by ruler and compass alone if and only if:*

$$m = 2^k \prod_{t=1}^{n} F_t,$$

for some $k, n \in \mathbb{Z}$. □

Let us examine the first Mersenne numbers, listed in table 5.1. We will see that the factors of these numbers are very special.

p	M_p
2	3
3	7
5	31
7	127
11	$2047 = 23 \cdot 89$
13	8191
17	131071

TABLE 5.1. Mersenne numbers M_p for $p = 2, 3, 5, 7, 11, 13, 17$.

Let us start with an elementary observation: every prime (less 2) is such that $p \equiv 1, 3 \pmod 4$. More precisely one can show that prime numbers are equally distributed in these two sets. Thus let us look for the divisors of $x^2 + 1$, listed in table 5.2.

Looking at table 5.2 one is tempted to say that all primes p such that $p|(x^2 + 1)$ are of the form $p \equiv 1 \pmod 4$. This intuition is confirmed by the following proposition:

PROPOSITION 5.8. *Let q be a prime, then $q|(x^2+1)$ if and only if $q \equiv 1 \pmod 4$.*

[4] `http://oddperfect.org/pomerance.html`.

x	x^2+1	$\equiv 1 \pmod 4$	$\equiv 3 \pmod 4$
8	$65 = 5 \cdot 13$	5	3
10	101	13	7
12	$145 = 5 \cdot 29$	17	11
13	$170 = 2 \cdot 5 \cdot 17$	29	19

TABLE 5.2. Some values of $x^2 + 1$ for $x = 8, 10, 12, 13$ and distribution of prime numbers $p \equiv 0, 1 \pmod 4$.

PROOF. ($\Rightarrow$). Let us suppose that q is prime and $q|(x^2 + 1)$ for a fixed $x \in \mathbb{Z}$. Thus

$$\begin{aligned} & x^2 + 1 \equiv 0 \pmod q \\ \Rightarrow \quad & x^2 \equiv -1 \pmod q \\ \Rightarrow \quad & x^4 \equiv 1 \pmod q, \end{aligned}$$

so that $ord(x) = 4$ in $\mathbb{Z}_q^*$ and by Lagrange's theorem $4|\#\mathbb{Z}_q^* = q - 1$, i. e. $q \equiv 1 \pmod 4$.

($\Leftarrow$). Let q be such that $q \equiv 1 \pmod 4$; hence $4|(q-1) = \#\mathbb{Z}_q^*$. $\mathbb{Z}_q^*$ is a cyclic group, hence let g be a generator, i. e. g is such that $ord(g) = q - 1$ in $\mathbb{Z}_q^*$. Since $4|(q-1)$, there exists an element $x \in \mathbb{Z}_q^*$ such that

$$\begin{aligned} & x = g^{\frac{q-1}{4}} \\ \Rightarrow \quad & x^2 \equiv g^{\frac{q-1}{2}} \equiv -1 \pmod q \quad \text{since } ord(q) \neq 2 \\ \Rightarrow \quad & x^2 + 1 \equiv 0 \pmod q \quad \text{i. e. } q|(x^2+1). \end{aligned}$$

□

Fermat and Mersenne numbers satisfy similar properties.

PROPOSITION 5.9. *If p is a prime and if q is a prime divisor of $M_p = 2^p - 1$, then $q \equiv 1 \pmod p$.*

PROOF. Let q be a prime divisor of M_p, then

$$2^p \equiv 1 \pmod q.$$

Hence $ord(2) = p$ in $\mathbb{Z}_q^*$ and by Lagrange's theorem $p|\#\mathbb{Z}_q^* = q - 1$, i. e. $q \equiv 1 \pmod p$. □

EXAMPLE 5.3. For $p = 11$, $M_{11} = 2^{11} - 1 = 23 \cdot 89$ and we have $23 \equiv 1 \pmod{11}$ and $89 \equiv 1 \pmod{11}$. □

This property is really interesting: if we are looking for a prime divisor of M_p, with p a prime, it must be such that $q \equiv 1 \pmod p$.

Now consider Fermat numbers. Euler was the first who succeeded in finding a factor of $F_5 = 641 \cdot 6700417$, but he did not know if the co-factor

6700417 was prime. However he succeeded in finding a proper factorization thanks to the following result:

PROPOSITION 5.10. *If $t \geq 0$ and q is a prime divisor of $F_t = 2^{2^t} + 1$, then $q \equiv 1 \pmod{2^{t+1}}$.*

PROOF. Let q be a prime divisor of the t-th Fermat number F_t, then:

$$\begin{aligned} & 2^{2^t} \equiv -1 \pmod{q} \\ \Rightarrow \quad & (2^{2^t})^2 \equiv 1 \pmod{q} \\ \Rightarrow \quad & (2^{2^{t+1}}) \equiv 1 \pmod{q}. \end{aligned}$$

Thus we can conclude that $ord(2)|2^{t+1}$. But $ord(2) \nmid 2^t$, since $2^{2^t} \equiv -1 \pmod{q}$, so that $ord(2) = 2^{t+1}$ in $\mathbb{Z}_q^*$ and Lagrange's theorem yields $2^{t+1}|\#\mathbb{Z}_q^* = q - 1$, i. e. $q \equiv 1 \pmod{2^{t+1}}$. □

EXAMPLE 5.4. For $t = 5$ we have $q \equiv 1 \pmod{64}$: Euler tried to find a divisor q of F_5 using steps of size 64. In other words q was one among $65, 129, 193, 257, \cdots, 641, \cdots$. □

In 1772 Euler showed also that M_{31} is prime; M_{31} was the largest known prime number until 1867. The *Great Internet Mersenne Prime Search* (GIMPS[5]) association, today, is looking for large Mersenne primes; the largest is $2^{43112609} - 1$ ($13 \cdot 10^6$ digits). On the other hand we have seen that F_t is prime for $t = 0, 1, \cdots, 4$; the other values of $t = 5, \cdots, 31$ are such that F_t is composite, whereas nothing is known about the primality of F_t for $t \geq 33$ ($2.5 \cdot 10^9$ digits).

Now we deal with Mersenne and Fermat numbers primality proving. We have partially characterized (see lemma 2.4) the structure of quadratic residues modulo a prime p; in particular we know that $\#\mathbb{Z}_p^* = p - 1$ and we have half quadratic residues and half quadratic non-residues in $\mathbb{Z}_p^*$. Further $x \in \mathbb{Z}_p^*$ is a quadratic residue modulo p if and only if $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Now we change the point of view, namely we choose a value $a \in \mathbb{Z}$ and we ask which properties must satisfy a prime p so that a is quadratic residue modulo p. The case $a = 1$ is trivial: 1 is always a quadratic residue modulo each prime number p. Let $a = -1$, a is a quadratic residue if $\exists\, x \in \mathbb{Z}$ such that $x^2 \equiv -1 \pmod{p}$, which yields either $p = 2$ or $p|(x^2 + 1)$ and by proposition 5.8 we know that this implies $p \equiv 1 \pmod{4}$. Hence we can conclude that $a = -1$ is a quadratic residue modulo a prime p either if $p = 2$ or if $p \equiv 1 \pmod{4}$. For $a = 2$ the situation is a little bit harder and we need the *Eisenstein criterion*.

[5] See `http://www.mersenne.org/`.

DEFINITION 5.4. Let p be a prime. We will denote with $\mathcal{E}$ a set of $\frac{p-1}{2}$ elements of $\mathbb{Z}_p^*$:

$$\mathcal{E} = \left\{ e_1, e_2, \cdots, e_{\frac{p-1}{2}} : \ e_i \in \mathbb{Z}_p^* \right\},$$

such that $\mathbb{Z}_p^* = \{\pm e_i\}$. □

EXAMPLE 5.5. For example $\mathcal{E} = \left\{1, 2, \cdots, \frac{p-1}{2}\right\}$, in fact

$$\mathbb{Z}_p^* = \left\{-\tfrac{p-1}{2}, \cdots, -2, -1, 1, 2, \cdots, \tfrac{p-1}{2}\right\}.$$

□

Let now $a \in \mathbb{Z}_p^*$, it is clear that $a \cdot e_i$ (with $e_i \in \mathcal{E}$) is still an element of $\mathbb{Z}_p^*$, but we are not sure whether $a \cdot e_i$ is still an element of $\mathcal{E}$ or not. Thus we write:

$$a \cdot e_i = \pm e_j = \epsilon(i) \cdot e_j,$$

being $e_i, e_j \in \mathcal{E}$ and denoting with $\epsilon(i) \in \{\pm 1\}$ the value $+1$ if $a \cdot e_i \in \mathcal{E}$ and the value -1 when this is not the case. Then we have a lemma:

LEMMA 5.11. *We can write:*

$$a^{\frac{p-1}{2}} = \prod_{i=1}^{\frac{p-1}{2}} \epsilon(i). \tag{5.1}$$

PROOF. We evaluate the product:

$$ae_1 \cdot ae_2 \cdot \cdots \cdot ae_{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \prod_{i=1}^{\frac{p-1}{2}} e_i =$$

$$= \prod_{i=1}^{\frac{p-1}{2}} \epsilon(i) \cdot \prod_{i=1}^{\frac{p-1}{2}} e_i.$$

Hence

$$a^{\frac{p-1}{2}} = \prod_{i=1}^{\frac{p-1}{2}} \epsilon(i).$$

□

We now use lemma 5.11 to evaluate when $a = 2$ is a quadratic residue modulo p.

PROPOSITION 5.12. *Let $p \geq 2$ be a prime, then $a \in \mathbb{Z}_p^*$ is a quadratic residue modulo p if and only if $p \equiv 1, 7 \pmod 8$.*

Proof. We use definition 5.4 to write:

$$\mathcal{E} = \left\{1, 2, \cdots, \frac{p-1}{2}\right\}$$
$$\overline{\mathcal{E}} = \left\{\frac{p+1}{2}, \frac{p+2}{2}, \cdots, p-1\right\}$$
$$\Rightarrow \quad \mathbb{Z}_p^* = \mathcal{E} \cup \overline{\mathcal{E}}.$$

Since $p \neq 2$ we know that p is either 1 or 3 modulo 4; we want to determine the values of $\epsilon(i)$ in lemma 5.11. Let us start supposing that $p \equiv 1 \pmod 4$; it is straightforward to see that if $1 \leq e_i \leq \frac{p-1}{4}$, then $ae_i = 2e_i$ has $\epsilon(i) = 1$, i. e. $ae_i \in \mathcal{E}$. On the other hand, if $\frac{p-1}{4} < e_i \leq \frac{p-1}{2}$, then $ae_i = 2e_i$ has $\epsilon(i) = -1$. Therefore the elements $\epsilon(i) = -1$ of equation (5.1) are exactly $\frac{p-1}{2} - \frac{p-1}{4} = \frac{p-1}{4}$.

Now we repeat this reasoning when $p \equiv 3 \pmod 4$. It is clear that if $1 \leq e_i \leq \frac{p-3}{4}$, then $ae_i = 2e_i$ has $\epsilon(i) = 1$, whereas when $\frac{p-3}{4} < e_i \leq \frac{p-1}{2}$, then $ae_i = 2e_i$ has $\epsilon(i) = -1$. Hence the elements with $\epsilon(i) = -1$ are in number of $\frac{p-1}{2} - \frac{p-3}{4} = \frac{p+1}{4}$.

Thus, on the one hand, we know, by lemma 2.4, that $2 \in \mathbb{Z}_p^*$ is a quadratic residue modulo p if and only if $2^{\frac{p-1}{2}} \equiv 1 \pmod p$; on the other hand, equation (5.1) yields:

$$2^{\frac{p-1}{2}} = \prod_{i=1}^{\frac{p-1}{2}} \epsilon(i).$$

It remains to determine the sign of the right member of the above equation. When $p \equiv 1 \pmod 4$ we can conclude that 2 is a quadratic residue modulo p if and only if $\frac{p-1}{4}$ is even, whereas when $p \equiv 3 \pmod 4$, 2 is a quadratic residue modulo p if and only if $\frac{p+1}{4}$ is even. Thus it suffices to evaluate $p \bmod 8$, have a look at table 5.3. If $p \equiv 1 \pmod 8$, then $8|(p-1)$, hence

$p \bmod 8$	$\sum_{i:\, \epsilon(i)=-1} \epsilon(i)$	Is $a = 2$ a quadratic residue modulo p?
1	$\frac{p-1}{4}$ (even)	Yes
3	$\frac{p+1}{4}$ (odd)	No
5	$\frac{p-1}{4}$ (odd)	No
7	$\frac{p+1}{4}$ (even)	Yes

Table 5.3. Cases when $a = 2$ is a quadratic residue modulo p or not, for each $p \equiv 1, 3, 5, 7 \pmod 8$.

$4|(p-1)$, so that $p \equiv 1 \pmod 4$ which implies that $\frac{p-1}{4}$ is even and 2 is a quadratic residue modulo p. If $p \equiv 3 \pmod 8$, then $8|(p-3)$, hence $4|(p-3)$, so that $p \equiv 3 \pmod 4$ and $\frac{p+1}{4} = \frac{3+8k+1}{4} = 2k+1$ which is odd; thus 2 is

a quadratic non residue modulo p when $p \equiv 3 \pmod 8$. Repeating this arguments for the cases $p \equiv 5, 7 \pmod 8$ yields the assertion. □

Example 5.6. Take $p = 17 \equiv 7 \pmod 8$, it is easy to see that $2 \equiv 6^2 \pmod{17}$. For $p = 23 \equiv 1 \pmod 8$, it is easy to see that $2 \equiv 5^2 \pmod{23}$. □

In a similar fashion we can deal with the case when $a = 3$ and obtain the following[6]:

Proposition 5.14. *If $p \neq 2, 3$ is a prime, the $a = 3 \in \mathbb{Z}_p^*$ is a quadratic residue modulo p if and only if $p \equiv 1, 11 \pmod{12}$.* □

We can use these results to improve the result of proposition 5.10:

Proposition 5.15. *If $t \geq 2$ and q is a prime divisor of the t-th Fermat number $F_t = 2^{2^t} + 1$, then $q \equiv 1 \pmod{2^{t+2}}$.*

Proof. By proposition 5.10 we know that $q \equiv 1 \pmod{2^{t+1}}$, so that $q \equiv 1 \pmod 8$ since $t \geq 2$. Thus, by proposition 5.12, 2 is a quadratic residue modulo q, i. e. there exists $q = \sqrt{2} \in \mathbb{Z}_q^*$. We have seen in proposition 5.10 that $ord(2) = 2^{t+1}$ in $\mathbb{Z}_q^*$, hence

$$\begin{aligned} & ord(\sqrt{2}) = 2ord(2) = 2^{t+2} \quad \text{in } \mathbb{Z}_q^* \\ \Rightarrow \quad & (\sqrt{2})^{2^{t+2}} \equiv 1 \pmod q \\ \Rightarrow \quad & 2^{t+2} | \#\mathbb{Z}_q^* = q - 1 \\ \Rightarrow \quad & q \equiv 1 \pmod{2^{t+2}}. \end{aligned}$$

□

We are now ready to discuss the *Pépin test* for Fermat numbers. The key ingredient is:

---

[6]More in general, in number theory one studies the so called *quadratic reciprocity*. Gauss's lemma gives a condition for an integer to be a quadratic residue:

Lemma 5.13 (Gauss's Lemma). *For any odd prime p let a be an integer that is coprime to p. Consider the integers*

$$a, 2a, 3a, \cdots, \frac{p-1}{2}a$$

and their least positive residues modulo p (these residues are all distinct, so there are $\frac{p-1}{2}$ of them). Let n be the number of these residues that are greater than $\frac{p}{2}$. Then

$$\left(\frac{a}{p}\right) = \chi_p(a) = (-1)^n.$$

Proof. It suffices to note that by Euler's criterion of lemma 2.4 $\chi_p(a) = a^{\frac{p-1}{2}}$, and by lemma 5.11:

$$a^{\frac{p-1}{2}} = \prod_{i=1}^{\frac{p-1}{2}} \epsilon(i) = (-1)^n,$$

since n is the number of residues in $a, 2a, 3a, \cdots, \frac{p-1}{2}a$ that are greater than $\frac{p}{2}$. □

PROPOSITION 5.16 (Pépin 1877). *The t-th Fermat number $F_t = 2^{2^t} + 1$ is prime if and only if:*

$$3^{2^{2^t-1}} \equiv -1 \pmod{F_t}.$$

PROOF. ($\Rightarrow$). Let us suppose that $n = F_t = 2^{2^t} + 1$ is prime. Thus $\frac{n-1}{2} = 2^{2^t-1}$ and we must show that

$$3^{\frac{n-1}{2}} \equiv -1 \pmod{n}.$$

Hence by Euler's criterion this is the same as claiming that 3 is a quadratic non-residue modulo n. Thus by proposition 5.14 it suffices to check if $n \equiv 1, 11 \pmod{12}$. We use the Chinese Remainder Theorem and compute:

$$\begin{aligned} & 2^{2^t} + 1 \equiv 1 \pmod 4 \quad \text{if } t \geq 1 \\ & 2^{2^t} + 1 \equiv (-1)^{2^t} + 1 \equiv 2 \pmod 3 \quad \text{since } -1 \equiv 2 \pmod 3 \\ \Rightarrow \quad & F_t = n = 2^{2^t} + 1 \equiv 5 \pmod{12}, \end{aligned}$$

and 3 is a quadratic non-residue modulo n.

($\Leftarrow$). On the other hand, let q be a prime divisor of $F_t = n$; we show that $F_t = q$, i. e. F_t is prime, when $3^{\frac{n-1}{2}} \equiv -1 \pmod{n}$. We can write:

$$\begin{aligned} & 3^{\frac{n-1}{2}} \equiv -1 \pmod q \\ \Rightarrow \quad & 3^{n-1} \equiv 1 \pmod q, \end{aligned}$$

hence $ord(3) | (n-1) = 2^{2^t}$, i. e. the order of 3 in $\mathbb{Z}_q^*$ is a power of two. However, since $3^{\frac{n-1}{2}} = 3^{2^{2^t-1}} \equiv -1 \pmod q$ we can conclude that $ord(3) = 2^{2^t} = n - 1$ in $\mathbb{Z}_q^*$. Thus, on the one hand $n - 1 | \#\mathbb{Z}_q^* = q - 1$ by Lagrange's theorem, i. e. $n - 1 \leq q - 1$ which yields $n \leq q$, and on the other hand $q | n$ by hypothesis, i. e. $q \leq n$. The only possibility is, therefore, $q = n = F_t$ and F_t is indeed prime. □

The running-time of this test is clearly:

$$\text{Running-Time: } \Rightarrow \quad O\left(\log(2^{2^t-1})(\log(F_t))^2\right) = O(2^{3t}),$$

which is polynomial in F_t, but exponential in t. Thus this test is too slow for $t = 33$.

The following test is related to Mersenne numbers. Before introducing it we recall some elementary facts about *finite field extensions*. The following theorem is crucial:

THEOREM 5.17 ([**10**]). *Let q be a prime and consider the field $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$. Then for every degree $d \in \mathbb{N}$ there exists a unique (up to isomorphisms) extension of $\mathbb{Z}_q$, namely $\mathbb{F}_{q^d}$, such that $\mathbb{F}_q = \mathbb{Z}_q \subset \mathbb{F}_{q^d}$ and $\#\mathbb{F}_{q^d} = q^d - 1$.* □

$\mathbb{F}_{q^d}$ can be thought of in the same way we define the field of complex numbers $\mathbb{C}$ starting from $\mathbb{R}$:

$$\mathbb{C} = \mathbb{R}(\sqrt{-1}) = \mathbb{R}(i) = \left\{x + iy : \ x, y \in \mathbb{R} \text{ and } i = \sqrt{-1}\right\}.$$

Hence, let $a \in \mathbb{Z}_q$ be such that a is a quadratic non residue modulo q; we build-up the field extension of $\mathbb{F}_q = \mathbb{Z}_q$, namely $\mathbb{F}_{q^d}$, adding $\sqrt{a}$ to $\mathbb{F}_q$:

$$\mathbb{F}_{q^d} = \mathbb{Z}_q(\sqrt{a}) = \left\{x \pm \sqrt{a}y : \ x, y \in \mathbb{Z}_q\right\}.$$

It could seem that $\mathbb{F}_{q^d}$ changes with a; in fact this is the case, but theorem 5.17 is telling us that all these extensions are isomorphic. Thus we can state that each element of $\mathbb{Z}_q(\sqrt{a})$ is a zero of a polynomial of degree 2, i. e.:

$$f(T) = [T - (x + \sqrt{a}y)][T - (x - \sqrt{a}y)] = T^2 - 2xT + (x^2 - ay^2).$$

Definition 5.5. We define the *trace* and the *norm* of an element $x + \sqrt{a}y \in \mathbb{Z}_q(\sqrt{a})$ to be respectively:

$$Tr(x + \sqrt{a}y) = 2x$$
$$N(x + \sqrt{a}y) = (x + \sqrt{a}y)(x + \sqrt{a}y)^* = x^2 - ay^2,$$

so that $f(T) = T^2 - Tr(\alpha)T + N(\alpha)$, with $\alpha = x + \sqrt{a}y \in \mathbb{Z}_q(\sqrt{a})$. □

Lemma 5.18. *If $f(\alpha) = 0$ for an element $\alpha \in \mathbb{Z}_q(\sqrt{a})$, then $f(\alpha^q) = 0$ as well.*

Proof. Let $\alpha = x + \sqrt{a}y$ be the generic element of $\mathbb{Z}_q(\sqrt{a})$, we can write:

$$\begin{aligned} & f(\alpha) = \alpha^2 - Tr(\alpha)\alpha + N(\alpha) = \alpha^2 - 2x\alpha + x^2 - ay^2 = 0 \\ \Rightarrow \quad & f^q(\alpha) = 0 \\ \Rightarrow \quad & (\alpha^2 - 2x\alpha + x^2 - ay^2)^q = 0 \\ \Rightarrow \quad & (\alpha^q)^2 - (2x)^q\alpha + (x^2 - ay^2)^q = 0, \end{aligned}$$

since $char(\mathbb{Z}_q(\sqrt{a})) = q$. Finally, since $x, y \in \mathbb{Z}_q$, we can use Fermat's little theorem to conclude:

$$f(\alpha^q) = (\alpha^q)^2 - (2x)\alpha + (x^2 - ay^2) = 0,$$

as required. □

Note that $f(T)$ has degree two, thus lemma 5.18 implies that either $\alpha^q = x + \sqrt{a}y$ or $\alpha^q = x - \sqrt{a}y$. We claim that the only possibility is the latter; in fact if α^q would be equal to $x + \sqrt{a}y$, we could state that $\alpha^q = \alpha$. Recall that $\mathbb{Z}_q = \left\{\alpha \in \overline{\mathbb{Z}}_q : \ \alpha^q = \alpha\right\}$, so that $\alpha^q = \alpha$ would imply $y = 0$ and $\mathbb{F}_{q^d}$ would collapse in $\mathbb{F}_q$. Hence

$$\begin{aligned} \alpha = x + \sqrt{a}y \quad & \Rightarrow \quad \alpha^q = x - \sqrt{a}y \\ & \Rightarrow \quad N(\alpha) = \alpha\alpha^q = \alpha^{q+1}, \end{aligned}$$

i. e. $\alpha^* = \alpha^q$ in $\mathbb{Z}_q(\sqrt{a})$.

EXAMPLE 5.7. Let $q = 3$, so that $(\mathbb{Z}/q\mathbb{Z})^* = \{1, -1\}$ and take $a = -1$ with $\sqrt{-1} = i$. We have:

$$\mathbb{F}_{3^2} = \mathbb{F}_9 = \mathbb{Z}_3(i) = \{x + iy : \ s, y \in \mathbb{Z}_3\}.$$

Further, for $\alpha = 1 + i \in \mathbb{Z}_3(i)$, we have $(1 + i)^3 = 1^3 + i^3 = 1 - i = (1 + i)^*$. □

Now we introduce the *Lucas-Lehmer* primality test for Mersenne numbers of the form $n = M_p = 2^p - 1$, with p a prime. Note that when n is prime, 3 is a quadratic non-residue modulo n; in fact, by proposition 5.14 it suffices to evaluate 3 mod 12. We use the Chinese Remainder Theorem to compute:

$$n \equiv 2^p - 1 \equiv (-1)^p - 1 \equiv [p \text{ is odd}] \equiv -2 \equiv 1 \pmod 3$$
$$n \equiv 2^p - 1 \equiv [\text{let us suppose } p > 2] \equiv 0 - 1 \equiv 3 \pmod 4,$$

hence $n \equiv 7 \pmod{12}$ and 3 is a quadratic residue modulo n. Therefore we can build-up the field extension of $\mathbb{Z}_n$ adding $\sqrt{3}$, which yields $\mathbb{Z}_n(\sqrt{3})$.

Let now $s_0 \equiv 4 \pmod n$ and define:

$$s_{i+1} \equiv s_i^2 - 2 \pmod n,$$

for $i \geq 0$. We need a lemma:

LEMMA 5.19. *Let* $\omega = 2 + \sqrt{3} \in \mathbb{Z}_n(\sqrt{3})$. *Then:*

$$s_i = \omega^{2^i} + (\omega^*)^{2^i}.$$

PROOF. We use induction[7] on i. The basis case is OK since:

$$i = 1 \qquad \Rightarrow \qquad s_0 = \omega + \omega^*.$$

Let us suppose, now, that $s_i = \omega^{2^i} + (\omega^*)^{2^i}$; hence

$$\begin{aligned} s_{i+1} = s_i^2 - 2 &= (\omega^{2^i} + (\omega^*)^{2^i})^2 - 2 = \\ &= \omega^{2^{i+1}} + (\omega^*)^{2^{i+1}} + 2(\omega\omega^*)^{2^i} - 2 = \\ &= \omega^{2^{i+1}} + (\omega^*)^{2^{i+1}} + 2((2 + \sqrt{3})(2 - \sqrt{3}))^{2^i} - 2 = \\ &= \omega^{2^{i+1}} + (\omega^*)^{2^{i+1}} + 2 \cdot 1 - 2 = \\ &= \omega^{2^{i+1}} + (\omega^*)^{2^{i+1}}. \end{aligned}$$

□

The key ingredient is given by the following proposition:

[7]The simplest and most common form of mathematical induction proves that a statement involving a natural number n holds for all values of n. The proof consists of two steps:

(1) *The basis* (base case): showing that the statement holds when $n = 0$.
(2) *The inductive step*: showing that if the statement holds for some n, then the statement also holds when $n + 1$ is substituted for n.

The assumption in the inductive step that the statement holds for some n is called the *induction hypothesis* (or inductive hypothesis). To perform the inductive step, one assumes the induction hypothesis and then uses this assumption to prove the statement for $n + 1$.

PROPOSITION 5.20 (Lucas 1856). *With the notation as introduced above* $s_{p-2} \equiv 0 \pmod{n}$ *if and only if* n *is prime.*

PROOF. ($\Rightarrow$). Since n is prime, as we have just seen, 3 is a quadratic non-residue modulo n, hence we can consider $\omega = 2 + \sqrt{3}$ as an element of $\mathbb{Z}_n(\sqrt{3})$. We must show that $s_{p-2} = \omega^{2^{p-2}} + (\omega^*)^{2^{p-2}} \equiv 0 \pmod{n}$; multiplying both sides for $\omega^{2^{p-2}}$ and recalling that $\omega\omega^* = 1$:

$$\begin{aligned} & \omega^{2^{p-2}} + (\omega^*)^{2^{p-2}} \stackrel{?}{\equiv} 0 \\ \Rightarrow \quad & \omega^{2^{p-1}} + (\omega\omega^*)^{2^{p-2}} \stackrel{?}{\equiv} 0 \\ \Rightarrow \quad & \omega^{2^{p-1}} + 1 \stackrel{?}{\equiv} 0 \\ \Rightarrow \quad & \omega^{2^{p-1}} \stackrel{?}{\equiv} -1 \quad \text{in } \mathbb{Z}_n(\sqrt{3}). \end{aligned}$$

Since $n = 2^p - 1$, we have $2^{p-1} = \frac{n+1}{2}$, so that we must show if:

$$(2 + \sqrt{3})^{\frac{n+1}{2}} \stackrel{?}{\equiv} -1 \quad \text{in } \mathbb{Z}_n(\sqrt{3}).$$

We evaluate $(1 + \sqrt{3})^2 = 1 + 3 + 2\sqrt{3} = 2(2 + \sqrt{3}) = 2\omega$ in $\mathbb{Z}_n(\sqrt{3})$ and we compute the $\frac{n+1}{2}$-th power of the result:

$$(1 + \sqrt{3})^{n+1} = 2^{\frac{n+1}{2}}(2 + \sqrt{3})^{\frac{n+1}{2}}.$$

On the left side, since $1 + \sqrt{3} \in \mathbb{Z}_n(\sqrt{3})$ and since n is prime we can write $(1 + \sqrt{3})^* = (1 + \sqrt{3})^n$ which yields $(1 + \sqrt{3})^{n+1} = (1 + \sqrt{3})(1 + \sqrt{3})^* = -2$. On the right side, $2^{\frac{n+1}{2}} = 2 \cdot 2^{\frac{n-1}{2}}$, and since $n \equiv 7 \pmod{8}$ (as it is easy to check) 2 is a quadratic residue modulo n (by proposition 5.12), and Euler's criterion yields $2^{\frac{n-1}{2}} \equiv 1 \pmod{n}$; hence

$$2^{\frac{n+1}{2}} \equiv 2 \quad \text{in } \mathbb{Z}_n(\sqrt{3}).$$

Finally

$$(2 + \sqrt{3})^{\frac{n+1}{2}} = \frac{(1 + \sqrt{3})^{n+1}}{2^{\frac{n+1}{2}}} = -1 \quad \text{in } \mathbb{Z}_n(\sqrt{3}).$$

($\Leftarrow$). On the other hand, let $s_{p-2} \equiv 0 \pmod{n}$. As we have just seen this is equivalent to state that:

$$(2 + \sqrt{3})^{\frac{n+1}{2}} \equiv -1 \quad \text{in } \mathbb{Z}_n(\sqrt{3}).$$

Now we show that n is prime. Let q be a prime divisor of n and at the end of the day we hope $q = n$. Since $q|n$, the above relation holds in $\mathbb{Z}_q(\sqrt{3})$ too:

$$\omega^{\frac{n+1}{2}} \equiv -1 \quad \text{in } \mathbb{Z}_q(\sqrt{3}) \simeq \mathbb{Z}_q[X]/(X^2 - 3).$$

Note that we are not sure whether $\mathbb{Z}_q(\sqrt{3})$ is a field or not, since we do not know if $X^2 - 3$ is irreducible in $\mathbb{Z}_q[X]$. Nevertheless we can evaluate the

2-nd power of both members:

$$\omega^{n+1} \equiv 1 \quad \text{in } \mathbb{Z}_n(\sqrt{3}).$$

Thus $ord(\omega) = n + 1 = 2^p$, since $\omega^{\frac{n+1}{2}} = \omega^{2^{p-1}} \equiv -1$ in $\mathbb{Z}_q(\sqrt{3})$. Hence $2^p \leq \#\mathbb{Z}_q(\sqrt{3})$ and, trivially, $\#\mathbb{Z}_q(\sqrt{3}) \leq q^2$, which yields

$$q^2 \geq 2^p = n + 1 \quad \Rightarrow \quad q > \sqrt{n},$$

for each q prime divisor of n. Hence we have reached a contradiction and we must conclude $q = n$. □

Example 5.8. We try $p = 5$, so that $M_5 = 2^5 - 1 = 31$ and $p - 2 = 3$. We evaluate

$$\begin{aligned} s_0 &= 4 & s_1 &= 14 \\ s_2 &= 194 \equiv 8 \pmod{n} & s_3 &= 62 \equiv 0 \pmod{n}. \end{aligned}$$

Thus proposition 5.20 implies that M_5 is prime. □

We estimate the computational cost; a multiplication costs $O(\log^2(n)) \approx O(p^2)$, and we need p of these multiplications:

$$\text{Running-Time: } \Rightarrow \quad O(p^3),$$

which is exponential in p and polynomial in M_p. With this test, in 1856, Lucas discovered a prime larger than Euler's $M_{31} = 2^{31} - 1$. He used his proposition to prove the primality of $M_{127} = 2^{127} - 1$, evaluating by hand (this tooks about 19 years, working only on Sundays) $\omega^{2^{126}} \bmod (2^{127} - 1)$.

5.3. The Pocklington Test

This section and the following deals with the *Pocklington* test and its improvements which brought the most efficient primality proving test today known. Unlike the previous tests, this one is suitable for general numbers, not only for Mersenne and Fermat numbers. In 1918 an English teacher of name Pocklington published an article with this result:

Theorem 5.21 (Pocklington, 1918). *Let s be a positive integer such that, for every prime divisor q of s, there exists an element $a \in \mathbb{Z}_n$ which satisfies*[8]*:*

$$\begin{cases} a^s \equiv 1 \pmod{n} \\ \gcd(a^{s/q} - 1, n) = 1. \end{cases} \tag{5.2}$$

Then each divisor d of n is such that $d \equiv 1 \pmod{s}$.

[8]Note that the second condition is equivalent to say that $a^{s/q} \not\equiv 1 \pmod{d}$ for each divisor d of n.

Proof. Let p be a *prime* divisor of n; proving the assertion is clearly equivalent to show that $p \equiv 1 \pmod{s}$, since if this relation holds for every prime divisor of n, it also holds for all divisors d of n. Let $q^{i(q)}$ be the largest power of q such that $q^{i(q)}|s$, for each prime divisor q of s, in other words

$$s = \prod_{\substack{q|s \\ q \text{ prime}}} q^{i(q)}.$$

We claim that showing $p \equiv 1 \pmod{s}$ is equivalent to show that $p \equiv 1 \pmod{q^{i(q)}}$ for each q, since if $q^{i(q)}$ divides $p-1$ for each prime divisor q of s, $s|(p-1)$.

With this in mind, let $b = s^{\frac{s}{q^{i(q)}}}$, so that $a^s = b^{q^{i(q)}}$; we write equation (5.2) in terms of b:

$$\begin{cases} b^{q^{i(q)}} \equiv 1 \pmod{n} \\ \gcd(b^{q^{i(q)-1}} - 1, n) = 1. \end{cases}$$

Since $p|n$, the former relation is the same of $b^{q^{i(q)}} \equiv 1 \pmod{p}$. The latter relation is telling us that there are no common divisors between $b^{q^{i(q)-1}} - 1$ and n, that is possible only if:

$$b^{q^{i(q)-1}} \not\equiv 1 \pmod{p}.$$

Thus the order of b modulo p is a power of q and since $q^{i(q)-1}$ is not sufficient we can conclude $ord(b \bmod p) = q^{i(q)}$. Hence Lagrange's theorem yields

$$\begin{aligned} & q^{i(q)} | \#\mathbb{Z}_p^* = p - 1 \\ \Rightarrow \quad & q^{i(q)} | p - 1 \\ \Rightarrow \quad & p \equiv 1 \pmod{q^{i(q)}}, \end{aligned}$$

and this holds for every prime divisor q of s. □

The following corollary explains us how to use the above theorem to prove primality.

Corollary 5.22. *If $s > \sqrt{n}$, then n is prime.*

Proof. In fact theorem 5.21 tells us that every divisor (prime or not) d of n is such that $d \equiv 1 \pmod{s}$, that is to say $d > s$. But we have $s > \sqrt{n}$ by hypothesis, so that $n = d$ must be prime. □

Now we discuss how to use these results to build-up a primality proving test. First of all the integer s must be such that there exists a value $a \in \mathbb{Z}_n$ that satisfies equation (5.2). Possible candidates for s are (by Lagrange's theorem) the divisors of $n-1$, since, if $s|(n-1)$, we have $a^s \equiv 1 \pmod{n}$. Thus either $s = n-1$ or $n - 1 = s \cdot r$, with s completely factorizable (since we must know the prime divisors q of s to find a) and r not factorizable in practice. Hence theorem 5.21 and its corollary imply the primality of n if we

can write $n-1 = s \cdot r$ (with s completely factorizable and r not factorizable in practice) and $s > \sqrt{n}$.

Thus the idea is trying to factor $n-1$ in such a way that we can write $n-1 = s \cdot r$; then there are three possibilities:

(1) $s > \sqrt{n}$.
(2) $s < \sqrt{n}$ and the Miller-Rabin test tells that r is composite.
(3) $s < \sqrt{n}$ and the Miller-Rabin test tells that r is probably prime.

If we are in case (1), we just need to find integers a and s such that equation (5.2) holds; if we succeed, theorem 5.21 and its corollary tell us that n is prime. We claim that, if n is prime, it suffices to set $s = n-1 = \#\mathbb{Z}_n^*$. Note that if n is prime $\mathbb{Z}_n$ is a field and $\mathbb{Z}_n^*$ is cyclic. Let $g \in \mathbb{Z}_n^*$ be a generator, i. e. g is such that $ord(g) = n-1$. Hence we can always set $a = g$; in fact $a^s = g^{n-1} \equiv 1 \pmod{n}$ by Fermat's little theorem and

$$a^{s/q} = g^{\frac{n-1}{q}} \not\equiv 1 \pmod{n},$$

for every prime divisor q of s, since $ord(g) = n-1$ in $\mathbb{Z}_n^*$. Lastly, since n is prime, it has no other divisors beyond 1 and itself and we can conclude that $\gcd(a^{s/q} - 1, n) = 1$. Thus we have proven the primality of n.

If we are in case (2) we cannot conclude anything about the primality of n.

If we are in case (3) we cannot conclude immediately that n is prime, but we can exchange the roles of s and r and proceed by induction. In fact if $n-1 = s \cdot r$ with $s < \sqrt{n}$, we have $r > \sqrt{n}$. Further the Miller-Rabin test tells us that r is probably prime; if this is the case and if we can find an element $a \in \mathbb{Z}_n$ such that[9]:

$$\begin{cases} a^r \equiv 1 \pmod{n} \\ \gcd(a-1, n) = 1, \end{cases}$$

then we can conclude that n is prime. Hence, now, the problem is to prove the primality of r and we can repeat the Pocklington test with r in place of n; if we can prove the primality of r we can be sure that n is prime too. Note that this time $r \ll n$ and we have the same three possibilities of above; in particular, if we are in case (1) we have proven the primality of r and hence of n, whereas if we are in case (2) we cannot prove that r (and hence n) is prime. Let us suppose that we are again in case (3), i. e. $r = s' \cdot r'$ with $s' > \sqrt{r}$ and the Miller-Rabin test tells that r' is prime. If r' is prime and if we can find an element $a \in \mathbb{Z}_n$ such that:

$$\begin{cases} a^{r'} \equiv 1 \pmod{n} \\ \gcd(a-1, n) = 1, \end{cases}$$

then we can conclude that r is prime. Hence, now, the problem is to prove the primality of r' and we can repeat the Pocklington test with r' in place of r and so on.

[9]Note that when r is prime, $q = r$ is the unique divisor of r different from 1.

Typically case (1) happens hardly ever, case (2) often happens and case (3) happens (roughly speaking) with probability $\approx \frac{1}{\log(n)}$. The conclusion is that the Pocklington test works only if you are very lucky.

5.4. Goldwasser and Kilian

The brilliant idea of Goldwasser and Kilian[**24**], in 1986, was to translate theorem 5.21 replacing $\mathbb{Z}_n$ with $E(\mathbb{Z}_n)$, being $E: Y^2 = X^3 + AX + B$ an elliptic curve. The advantage is that, if you fail with a certain curve E, you can use another one, whereas $\mathbb{Z}_n$ is unique. Now we translate theorem 5.21; note that

$$\begin{aligned} \gcd(a^{s/q} - 1, n) = 1 \quad &\Leftrightarrow \quad a^{s/q} \equiv 1 \pmod{p} \ \forall \text{ prime } p|n \\ p \equiv 1 \pmod{s} \quad &\Leftrightarrow \quad s|\#\mathbb{Z}_p^* = p - 1. \end{aligned}$$

Proposition 5.23. *Let $n \geq 1$ and $E: Y^2 = X^3 + AX + B$ be an elliptic curve such that*[10] $\gcd(\Delta_E, n) = 1$. *Further let s be a positive integer; if, for every prime divisor q of s, there exists a point $P \in E(\mathbb{Z}_n)$ such that:*

$$\begin{cases} [s]P = \infty & \text{in } E(\mathbb{Z}_n) \\ [s/q]P \neq \infty & \text{in } E(\mathbb{Z}_p) \ \forall \text{ prime } p|n, \end{cases}$$

then every prime divisor p of n is such that $s|\#E(\mathbb{Z}_p)$.

Proof. The proof remains the same. We write:

$$s = \prod_{\substack{q|s \\ q \text{ prime}}} q^{i(q)},$$

and we note that it suffices to show that $q^{i(q)}|\#E(\mathbb{Z}_p)$. Let

$$Q = [s/q^{i(q)}]P \in E(\mathbb{Z}_n),$$

be another point of the curve. We claim that Q has order $q^{i(q)}$ in $E(\mathbb{Z}_p)$. In fact

$$[q^{i(q)}]Q = [q^{i(q)}][s/q^{i(q)}]P = [s]P = \infty \text{ in } E(\mathbb{Z}_n),$$

and this is also true in $E(\mathbb{Z}_p)$ for every prime divisor p of n. Moreover:

$$[q^{i(q)-1}]Q = [q^{i(q)-1}][s/q^{i(q)}]P = [s/q]P \neq \infty \text{ in } E(\mathbb{Z}_p),$$

by hypothesis, so that we can conclude $ord(Q) = q^{i(q)}$ in $E(\mathbb{Z}_p)$ (for each prime p divisor of n). Finally, by Lagrange's theorem, this yields that $q^{i(q)}|\#E(\mathbb{Z}_p)$ for each prime divisor q of s, and hence

$$s|\#E(\mathbb{Z}_p) \quad \forall \ p \text{ prime divisor of } n.$$

□

Corollary 5.24. *If $s > (\sqrt[4]{n} + 1)^2 \approx \sqrt{n}$, then n is prime.*

[10] That is to say, $E(\mathbb{Z}_n)$ and $E(\mathbb{Z}_p)$ are non-singular for each prime divisor p of n.

Proof. Proposition 5.23 tells us that $s|\#E(\mathbb{Z}_p)$, i. e. $s \leq \#E(\mathbb{Z}_p)$. Further, by Hasse's theorem, $\#E(\mathbb{Z}_p) < p + 1 + 2\sqrt{p}$, i. e.

$$\begin{aligned}(\sqrt[4]{n} + 1)^2 < s \leq \#E(\mathbb{Z}_p) < p + 1 + 2\sqrt{p} = (\sqrt{p} + 1)^2 \\ \Rightarrow \quad \sqrt[4]{n} + 1 < \sqrt{p} + 1 \\ \Rightarrow \quad \sqrt[4]{n} < \sqrt{p},\end{aligned}$$

and this relation holds for every prime divisor p of n. Thus, necessarily, $n = p$ is prime. □

Exactly like in the Pocklington test, the idea is trying to factor $\#E(\mathbb{Z}_n) = s \cdot r$, with s completely factorizable and r not factorizable in practice. Then there are three possibilities:

(1) $s > (\sqrt[4]{n} + 1)^2 \approx \sqrt{n}$. If this is the case n is prime, as it is easy to check by choosing $s = \#E(\mathbb{Z}_n)$ and by using any point P on the curve $E(\mathbb{Z}_n)$.
(2) $s < (\sqrt[4]{n}+1)^2 \approx \sqrt{n}$ and the Miller-Rabin test says that r is composite. We cannot conclude anything about the primality of n with this curve; *but we can change the curve and try again*.
(3) $s < \sqrt{n}$ and the Miller-Rabin test says that r is probably prime. We can exchange the roles of s and r and proceed by induction. In fact if $\#E(\mathbb{Z}_n) = s \cdot r$ with $s < (\sqrt[4]{n} + 1)^2 \approx \sqrt{n}$, we have $r > \sqrt{n}$. Further the Miller-Rabin test tells us that r is probably prime; if this is the case and if we can find an element $P \in E(\mathbb{Z}_n)$ such that:

$$\begin{cases}[r]P = \infty & \text{in } E(\mathbb{Z}_n) \\ P \neq \infty & \text{in } E(\mathbb{Z}_p)\ \forall \text{ prime } p|n,\end{cases}$$

then we can conclude that n is prime. Hence, now, the problem is to prove the primality of r (with $r \ll n$) and we can repeat the Pocklington test with r in place of n; if we can prove the primality of r we can be sure that n is prime too.

It remains to understand how we can check that:

$$[s/q]P \neq \infty \quad \text{in } E(\mathbb{Z}_p)\ \forall \text{ prime } p|n.$$

In the basic version of Pocklington test, it was enough to see that $\gcd(a^{s/q} - 1, n) = 1$. The best way to do this is to use projective coordinates. A point $P = (x : y : z)$, with $(x : y : z) \in \mathbb{P}^2(\mathbb{Z}_n)$ such that $\gcd(x, y, z) = 1$, is a point of $E(\mathbb{Z}_n)$ if $zy^2 \equiv x^3 + Axz^2 + Bz^3 \pmod{n}$. The point at infinity corresponds to $z \equiv 0 \pmod{n}$, which implies $x \equiv 0 \pmod{n}$, so that the point at infinity is $(0 : 1 : 0) \in E(\mathbb{Z}_n)$. In a similar fashion, for each prime divisor p of n,

$$\infty \in E(\mathbb{Z}_p) \Leftrightarrow z \equiv 0 \pmod{p} \Rightarrow x, y \equiv 0 \pmod{p}.$$

Thus we can simply evaluate $[s/q]P = (x : y : z)$ and verify that $\gcd(z, n) \neq 1$, which yields $[s/q]P \neq \infty$ in $E(\mathbb{Z}_p)$ (for each prime divisor p of n).

The algorithm above is called the *Goldwasser-Kilian* primality test. Note that the algorithm requires to evaluate $\#E(\mathbb{Z}_n)$; the original version of the algorithm used Schoof's algorithm of section 4.2. Now we estimate the computational complexity of the Goldwasser-Kilian algorithm; we refer to the worst case in which $\#E(\mathbb{Z}_n) = 2 \cdot r$ with r a Miller-Rabin pseudo-prime. Hence

$$r = \frac{1}{2}\#E(\mathbb{Z}_n) \leq \frac{1}{2}(n + 1 + 2\sqrt{n}) \approx \frac{n}{2},$$

and we can observe that, each time we repeat the algorithm with r in place of n, r' in place of r, r'' in place of r' and so on, the number to test is one bit shorter. Thus, in the worst case, we should repeat the test $\log_2(n) = O(\log(n))$ times, to prove the primality of n. Now we evaluate the work load for each step. First of all we should understand how many curves we have to try so that $\#E(\mathbb{Z}_n) = 2 \cdot r$, with r prime. To answer this question we need a result about the distribution of the curves $E(\mathbb{Z}_n)$ (when n is prime) in function of their number of points. Note that, by Hasse's theorem $\#E(\mathbb{Z}_n) = n + 1 - t$, with $|t| < 2\sqrt{n}$, so that the number of points of any curve $E(\mathbb{Z}_p)$ belongs to an interval of size $4\sqrt{n}$. The following result[**45**] is crucial:

THEOREM 5.25 (Deuring, 1940). *Let p be a prime. We can write:*

$$\#\{\textit{Elliptic curves } E \textit{ with } p + 1 - t \textit{ points}\} = \frac{p-1}{2} H(t^2 - 4p),$$

being $H(\Delta)$ the Hurwitz class number, representing the number of equivalence class of binary quadratic forms with discriminant Δ. □

Moreover one can use analytic number theory[**2**] to show that:

$$H(t^2 - 4p) \approx \frac{\sqrt{4p - t^2}}{\pi} \cdot L,$$

with L a random variable we can approximate to 1. Thus, theorem 5.25 is telling us that, fixed a prime n, there are just a few curves with $n + 1 \pm 2\sqrt{n}$ points, whereas the curves with $n+1$ points are much more (see also example 2.20 and figure 5.1).

Hence we can conclude that, if we are far from the edges of the critical interval the distribution is almost uniform; in other words if we choose a curve at random, $\#E(\mathbb{Z}_n)$ will be random too. Now the question is: how many curves $E(\mathbb{Z}_n)$ are such that $\#E(\mathbb{Z}_n) \in (n + 1 - 2\sqrt{n}, n + 1 + 2\sqrt{n})$ is of the form $2 \cdot r$ (with r prime)? This is equivalent to compute the probability that

$$r \in \left(\frac{n + 1 - 2\sqrt{n}}{2}, \frac{n + 1 + 2\sqrt{n}}{2} \right),$$

is prime. The interval is centered in $\frac{n+1}{2} \approx \frac{n}{2}$, thus by corollary A.2 of appendix A we can conclude that we must try a number of curves that is $O(\log(n/2)) = O(\log(n))$. Hence we need to prove $O(\log(n))$ curves as to

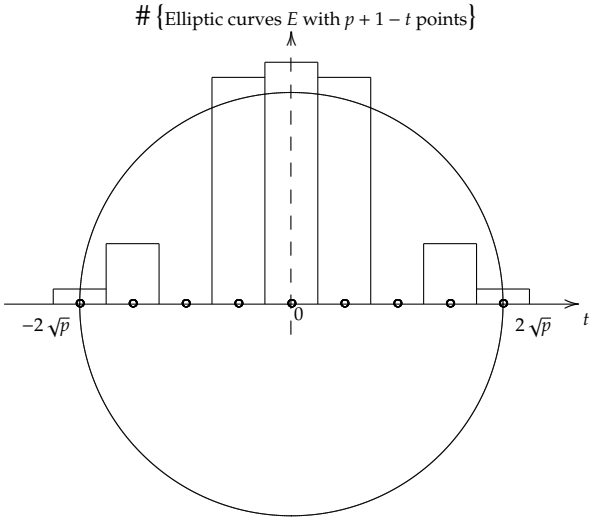


FIGURE 5.1. Number of elliptic curves with cardinality $p+1-t$ in function of $t \in \mathcal{I}$.

have $\#E(\mathbb{Z}_n) = 2 \cdot r$ with r prime; further the cost of Schoof's algorithm is $O(\log^8(n))$ and in the worst case we need to repeat these steps $O(\log(n))$ times. Thus the total cost is:

$$\text{Running-Time: } \Rightarrow \quad O(\log(n)\log(n)\log^8(n)) = O(\log^{10}(n)),$$

which is polynomial, but not practical because of the high value of the exponent.

5.5. Atkin and the ECPP

The main idea of Atkin is to improve the efficiency of the Goldwasser-Kilian algorithm replacing Schoof's algorithm with Atkin's algorithm (we discussed in section 4.3) for evaluating $\#E(\mathbb{Z}_n)$. This idea leads to a powerful *practical* algorithm. In his article[**5**] Atkin suggested to choose more carefully the curves E in the Goldwasser-Kilian algorithm; he considered suitable elliptic curves over the complex numbers with complex multiplication by imaginary quadratic orders of relatively small discriminant. He reduces the curves modulo n and uses only these in his primality proof. The main point is that, as we have seen, it is very easy to count the number of points on these elliptic curves modulo n.

Let n be, as usual, the integer we want to test for primality; we can suppose that n is prime, since we first test it with the Miller-Rabin test. Let R be an order of discriminant Δ; we start trying different values of $\Delta = -3, -4, -7, -8, \cdots$ and using Cornacchia's algorithm and equation (4.2) we evaluate the cardinality of the curve $E(\mathbb{C}) \simeq \mathbb{C}/R$ until this splits in a product $s \cdot r$ with s completely factorizable and r not factorizable in practice.

That is to say, for a fixed value of Δ, we first check that Δ is a quadratic residue[11] modulo n, and then, we look for the complex number φ which corresponds to the Frobenius endomorphism in $End(E)$. This value φ is such that $|\varphi|^2 = \varphi\varphi^* = n$ and it is unique up to conjugation and multiplication by units. As we have seen in section 4.3, there is a different number of possibilities for φ depending on the value of Δ. However, if a such value φ exists, we can conclude that there is a curve with complex multiplication such that $End(E) = R$ and with j-invariant that is a zero of $F(T)$ (theorem 3.11) and we can reduce $F(T)$ modulo n. Without loss of generality we can assume $\Delta \neq -3, -4$, so that $\#E(\mathbb{Z}_n)$ is, by equation (4.2), either $|\varphi - 1|^2$ or $|-\varphi - 1|^2$. At this point we try to factor $\#E(\mathbb{Z}_n)$ as the product $r \cdot s$, if we fail we start again with a different value of Δ. Note that we do not know which between $|\varphi - 1|^2$ and $|-\varphi - 1|^2$ is the cardinality of $E(\mathbb{Z}_n)$, but this is not important at this point, since we will write the equation of the elliptic curve only at the end of the algorithm. Moreover the cases $\Delta = -3, -4$ are better since we have more possibilities for $\#E(\mathbb{Z}_n)$ and so is more probable to find a factorization of the form $s \cdot r$. Once we have found the above value of Δ we have the same three possibilities of the Goldwasser-Kilian algorithm, namely:

(1) $s > (\sqrt[4]{n} + 1)^2 \approx \sqrt{n}$.
(2) $s < (\sqrt[4]{n}+1)^2 \approx \sqrt{n}$ and the Miller-Rabin test says that r is composite.
(3) $s < \sqrt{n}$ and the Miller-Rabin test says that r is probably prime.

If we are in case (3), we can proceed by induction, exchanging the values of s and r and so on, exactly like in the Goldwasser-Kilian algorithm. To complete the last part of the test we need to write the equation of the elliptic curve; hence we use equations (3.5), (3.6) and (3.7) to evaluate the values A, B and the j-invariant of the curve. Here we must be sure that the value we used for the cardinality corresponds to the equation of the curve, but this control is straightforward by Lagrange's theorem, as we have already seen in section 4.3.

The analysis of complexity is quite hard, even assuming some unproven conjectures on the distribution of prime numbers in small intervals; see **[37]** for details. However it seems that complexity is polynomial:

$$\text{Running-Time: } \Rightarrow \quad O((\log(n))^{4+\epsilon}),$$

using fast multiplication technique.

5.6. Agrawal-Kayal-Saxena (AKS)

The final answer to the long-standing open problem of primality proving, was given by three Indian Institute of Technology Kanpur computer scientists**[1]**; the authors received many accolades, including the 2006 Fulkerson Prize for this work.

[11] If this is not the case one can see that $E(\mathbb{Z}_n) = n + 1$ that is not an interesting case.

The key significance of AKS is that it was the first published primality-proving algorithm to be simultaneously *general*, *polynomial*, *deterministic*, and *unconditional*. Previous algorithms have achieved any three of these properties, but not all four. In fact, as we have seen in this chapter, Lucas-Lehmer test and Pépin test are not general, the Miller-Rabin test is polynomial, but its answer is only probabilistic (or it is deterministic assuming the GRH) whereas the ECPP test is deterministic but is not known to have polynomial time bounds for all inputs (even if the complexity seems to be polynomial). The situation is summarized in table 5.4.

	Miller-Rabin	ECCP	AKS
Answer	Probabilistic	Deterministic	Deterministic
Running-Time	Polynomial	Probabilistic	Polynomial

TABLE 5.4. A comparison between the Miller-Rabin test, the ECPP and the AKS algorithms

Let n be the integer to test for primality (it has passed a certain number of Miller-Rabin test, so that n is prime with high probability, but we need to prove that it is a prime). The key ingredient is given by the following theorem:

THEOREM 5.26 (Agrawal, Kayal and Saxena). *Let n be an odd positive integer and r a prime. If:*

(1) *n is not divisible by any prime $\leq r$;*
(2) *the order of n in $\mathbb{Z}_r^*$ is:*

$$ord(n) \geq \left(\frac{\log(n)}{\log(2)}\right)^2;$$

(3) *$\forall\ 0 \leq a \leq r$ we can write*

$$(X+a)^n = X^n + a \qquad in\ \mathbb{Z}_n[X]/\left(\frac{X^r-1}{X-1}\right);$$

then n is a prime power. □

We will postpone the proof of this theorem at the end of this section; we discuss some practical and theoretical aspects first.

Let r be a prime, we recall that the r-th *cyclotomic polynomial*[12] is

$$\Phi_r(X) = \frac{X^r-1}{X-1} = X^{r-1} + \cdots + X^2 + X + 1,$$

[12]Cyclotomic polynomials[**10**] are a very interesting class of polynomials, with coefficients in $\mathbb{Z}$ and that are irreducible over $\mathbb{Q}$. Such polynomials are linked with the problem of *cyclotomy*: the division of the circle into a given number of equal segments, and the construction of regular polygons. The n-th cyclotomic polynomial is given by

$$\Phi_n(X) = \prod_{i=1}^{\varphi(n)} (X - \zeta_i),$$

so that we can write

$$\mathbb{Z}_n[X]/\left(\frac{X^r-1}{X-1}\right) = \mathbb{Z}_n[X]/(\Phi_r(X)) = \\ = \left\{a_{r-2}X^{r-2} + \cdots + a_1X + a_0 : \ a_i \in \mathbb{Z}_n\right\}.$$

The ring above is finite and we can write

$$\#\mathbb{Z}_n[X]/(\Phi_r(X)) = n^{r-1},$$

since each element in that quotient ring is a polynomial with $r-1$ coefficients in $\mathbb{Z}_n$. Hence the number of bits we need to represent an element of $\mathbb{Z}_n[X]/(\Phi_r(X))$ is $O((r-1)\log(n)) = O(r\log(n))$.

The first observation we make is that, if n is prime, and if there exists a prime r which satisfies conditions (1) and (2) of theorem 5.26, then also condition (3) holds. In fact, when n is prime, all the binomial coefficients of $(X+a)^n$ are zero in $\mathbb{Z}_n[X]/(\Phi_r(X))$ and by Fermat's little theorem

$$(X+a)^n = X^n + a^n = X^n + a \qquad \text{in } \mathbb{Z}_n[X]/(\Phi_r(X)),$$

and there is no dependence from r. On the other hand, this theorem is a generalization of the Fermat test; if $(X+a)^n \equiv X^n + a$ we can conclude that n is prime without any doubt, but the evaluation of $(X+a)^n$ is too expensive when n is large. The brilliant idea of Agrawal, Kayal and Saxena was to evaluate $(X+a)^n$ modulo the r-th cyclotomic polynomial.

We can use theorem 5.26 to build-up the following primality proving algorithm:

(1) Check that n is not a power of some integer.
(2) Using the values $r = 2, 3, \cdots$ find the smallest prime r such that r does not divide n and does not divide any of the element $n^i - 1$ (for $i = 0, 1, \cdots, \left(\frac{\log(n)}{\log(2)}\right)^2$). In symbols

$$r \nmid n \cdot \prod_{i=1}^{\left(\frac{\log(n)}{\log(2)}\right)^2} (n^i - 1).$$

(3) Check that condition (3) of theorem 5.26 holds.

If n passes the test we can conclude that n is prime, otherwise n is composite. Now we give proof of correctness. If n is prime, clearly, it passes the test by Fermat's little theorem; on the other hand suppose that n passes the test. Note that it suffices to prove that all the conditions of theorem 5.26

---

being $\zeta_1, \cdots, \zeta_{\varphi(n)}$ the n-th primitive (i.e. of order n) roots of unity and $\varphi(\cdot)$ the Euler's φ-function. Since one can show that every n-th root of unity is indeed a power of an n-th primitive root of unity, the following recursive formula for the evaluation of the n-th cyclotomic polynomial holds

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{\substack{d|n \\ d\neq n}} \Phi_d(X)}.$$

hold, since we have verified that n is *not* an integer power in step (1) of our algorithm. Condition (3) is trivial, since it is step (3) of the algorithm; also condition (1) is trivial, by definition of r in step (2) of the algorithm. Lastly let ξ be the order of n modulo r, i. e. $n^{\xi} \equiv 1 \pmod{r}$ (this makes sense since $r \nmid n$); thus $r|(n^{\xi} - 1)$. But in step (2) of the algorithm we have verified that r does not divide the elements $n^i - 1$ for $i = 0, 1, \cdots, \left(\frac{\log(n)}{\log(2)}\right)^2$, hence we can conclude that

$$\xi > \left(\frac{\log(n)}{\log(2)}\right)^2,$$

that is condition (2) of theorem 5.26. Thus the above algorithm works and it is deterministic.

It is natural to ask how we can verify that n is not the power of some integer. Let us suppose $n = m^d$ with $d > 1$ and $m \geq 2$, i. e.

$$n = m^d \geq 2^d \quad \Rightarrow \quad d \leq \frac{\log(n)}{\log(2)}.$$

Hence for $d = 2, 3, \cdots, \frac{\log(n)}{\log(2)}$ we evaluate, with a certain precision, $n^{\frac{1}{d}}$ in $\mathbb{R}$ and we set $m = round(n^{\frac{1}{d}}) \in \mathbb{Z}$; finally we check that $m^d \neq n$. The computational cost is something like $O(\log^4(n))$ that will be negligible.

Now we give an estimate of the running-time of the algorithm. How many values of r must we try in step (2)? Let r be the *smallest* prime such that

$$r \nmid n \cdot \prod_{i=1}^{\left(\frac{\log(n)}{\log(2)}\right)^2} (n^i - 1),$$

thus we can say that the second member is divisible by every prime $\ell < r$, namely

$$\prod_{\substack{\ell < r \\ \ell \text{ prime}}} \ell \mid n \cdot \prod_{i=1}^{\left(\frac{\log(n)}{\log(2)}\right)^2} (n^i - 1).$$

Using the Prime Number Theorem of appendix A we can approximate the first product as e^r, and neglecting the term 1 at second member we can

conclude

$$\begin{aligned}
& e^r \mid n \cdot n^{\sum_{i=1}^{\left(\frac{\log(n)}{\log(2)}\right)^2} i} \\
\Rightarrow \quad & e^r \leq n \cdot n^{\sum_{i=1}^{\left(\frac{\log(n)}{\log(2)}\right)^2} i} \\
\Rightarrow \quad & r \leq \log(n) + \log(n) \sum_{i=1}^{\left(\frac{\log(n)}{\log(2)}\right)^2} i \\
\Rightarrow \quad & \left[\text{recall that } \sum_{i=0}^{s} i = \frac{s(s+1)}{2} \approx \frac{s^2}{2}\right] \\
\Rightarrow \quad & r \leq \log(n) + \frac{1}{2}\frac{\log^4(n)}{\log^2(2)}\log(n) = O(\log^5(n)).
\end{aligned}$$

Since this value is not so large, trying all the values $r = 3, 5, 7, \cdots$ is not too expansive. Finally we need to evaluate $(X + a)^n$ (for $a = 0, 1, \cdots, r-1$) in $\mathbb{Z}[X]/(\Phi(X))$; since an element in that quotient ring has size $O(r\log(n))$, a multiplication (using standard techniques) requires $O(r^2\log^2(n))$ and the evaluation of an n-th power requires $O(\log(n)(r^2\log^2(n)))$. We need to repeat this steps for each $a < r$ hence

$$\text{Running-Time: } \Rightarrow \quad O\left(r^3\log^3(n)\right) = O\left(\log^{18}(n)\right).$$

If we replace standard multiplication techniques by *fast* multiplication techniques, the cost of a multiplication becomes $O\left((r\log(n))^{1+\epsilon}\right)$, which yields a running time $O(\log^{12+\epsilon}(n))$. Further, it is possible that we find the right value of r without trying all $O(\log^5(r))$ values; if this is the case we can estimate the complexity with $O(\log^6(n))$.

It remains to prove the theorem, but we need some technical ingredients. Note that condition (2) of theorem 5.26 implies that there exists a prime $p|n$ such that $p \not\equiv 1 \pmod{r}$; in fact, if this is not the case, i. e. if *all* prime divisors p of n are such that $p \equiv 1 \pmod{r}$, then also $n \equiv 1 \pmod{r}$, that is to say $ord(n \bmod r) = 1$, but this is not allowed by condition (2). Hence let p be a prime such that $p|n$ and consider the ring

$$\mathcal{A} = \mathbb{Z}_p[X]/(\Phi_r(X)) = \left\{a_{r-2}X^{r-2} + \cdots + a_1X + a_0 : \ a_i \in \mathbb{Z}_p\right\}.$$

It is straightforward to note that $\mathcal{A}$ is a quotient of $\mathbb{Z}_n[X]/(\Phi_r(X))$, since

$$\mathbb{Z}_n[X]/(\Phi_r(X)) \xrightarrow{\bmod p} \mathcal{A}$$

Even if this is not necessary to prove theorem 5.26, we speak a little about the structure of $\mathcal{A}$. We need a lemma:

LEMMA 5.27. *The r-th cyclotomic polynomial is the product of distinct irreducible polynomials $\phi(X)$ with the same degree:*

$$\Phi_r(X) = \frac{X^r - 1}{X - 1} = \prod_{\phi \text{ irreducible}} \phi(X).$$

PROOF. First of all we can write every polynomial as a product of (one or more) irreducible polynomials. The fact that the polynomials $\phi(X)$ are all distinct comes from the fact that $\Phi_r(X)$ has not double zeroes. Note that $\Phi_r(X)$ has not double zeroes if its multiples, e. g. $X^r - 1$, has not; since $X^r - 1$ and its derivative rX^{r-1} have not common zeroes, we can conclude that $X^r - 1$ has not double zeroes and, as a consequence $\Phi_r(X)$ has not. Thus the polynomials $\phi(X)$ are all distinct. Now we show that the polynomials $\phi(X)$ have also the same degree. Let α be a zero of $\phi(X)$ and consider the finite extension of $\mathbb{F}_p = \mathbb{Z}_p$ generated by α, namely

$$\mathbb{F}_p(\alpha) = \mathbb{Z}_p[X]/(\phi(X)) \supset \mathbb{Z}_p.$$

Since $\phi(X)$ is irreducible, $\mathbb{F}_p^*(\alpha)$ is a finite field of order

$$\#\mathbb{F}_p^*(\alpha) = p^{deg(\phi)} - 1.$$

But since $\phi(\alpha) = 0$, $\Phi_r(\alpha) = 0$ too, and hence α is a zero of $X^r - 1$, i. e. $\alpha^r \equiv 1$. On the other hand $\alpha \neq 1$ since it is a zero of $\frac{X^r-1}{X-1}$ and we can write

$$\begin{aligned} & ord(\alpha) = r \quad \text{in } \mathbb{F}_p^*(\alpha) \\ \Rightarrow \quad & r | p^{deg(\phi)} - 1 \\ \Rightarrow \quad & p^{deg(\phi)} \equiv 1 \pmod{r}. \end{aligned}$$

But $deg(\phi)$ is minimal, since $\mathbb{F}_p(\alpha)$ is the smallest field generated by α, hence

$$deg(\phi) = ord(p \bmod r),$$

$\forall\ \phi(X)$ irreducible that divide $\Phi_r(X)$. □

The above lemma has an important consequence: using the Chinese Remainder Theorem we can conclude that

$$\begin{aligned} \mathcal{A} = \mathbb{Z}_p[X]/(\Phi_r(X)) &\simeq \prod_{\phi \text{ irreducible}} \mathbb{Z}_p[X]/(\phi(X)) \\ &\simeq \prod_{\phi \text{ irreducible}} \mathbb{F}_{p^d}, \end{aligned}$$

being $d = deg(\phi) = ord(p \bmod r)$.

Now consider the set

$$\Delta = \{\sigma_k : \ k \in \mathbb{Z}/r\mathbb{Z}\}$$

$$\begin{aligned} \sigma_k : \ \mathcal{A} &\to \mathcal{A} \\ X &\mapsto X^k. \end{aligned}$$

We show that the elements of Δ are the automorphisms from $\mathcal{A}$ to $\mathcal{A}$. First of all note that in $\mathcal{A}$ we can write $X^r \equiv 1 \pmod{p}$, since each multiple of $\Phi_r(X)$ is zero in $\mathcal{A}$; as a consequence $(X^r)^k \equiv 1 \pmod{p}$. Hence the action of σ_k on the generic element of $\mathcal{A}$ is

$$\sigma_k\left(\sum_{j=0}^{r-1} b_j X^j\right)^k = \sum_{j=0}^{r-1} b_j (X^j)^k.$$

This is the reason why $k \in \mathbb{Z}/r\mathbb{Z}$: if this is not the case each element would be mapped to 1. We point out that $\sigma_k = \sigma_{k+r}$, since $X^{k+r} = X^k X^r \equiv X^k$ in $\mathcal{A}$; for what concerns the other values of k, σ_k is an automorphism, since it preserves the structure of $\mathcal{A}$. Further Δ is a group: $\sigma_k \circ \sigma_\ell = \sigma_{k\ell} \in \Delta$, σ_1 is the identity element and it is easy to see that the inverse of σ_k is $\sigma_k^{-1} = \sigma_\ell$, with ℓ such that $\ell k \equiv 0 \pmod{r}$. Hence there is a group homomorphism

$$\begin{aligned}(\mathbb{Z}/r\mathbb{Z})^* &\longrightarrow \Delta \\ \overline{\varrho} &\mapsto \sigma_\varrho,\end{aligned}$$

i. e. $\Delta \simeq (\mathbb{Z}/r\mathbb{Z})^*$, which implies

$$\#\Delta = \#(\mathbb{Z}/r\mathbb{Z})^* = r - 1.$$

Denote with

$$\mathcal{G} = \{a \in \mathcal{A}^* : \ \sigma_n(a) = a^n\},$$

being

$$\mathcal{A}^* = \left\{\sum_{j=0}^{r-2} b_j X^j : \ \gcd\left(\sum_{j=0}^{r-2} b_j X^j, \Phi_r(X)\right) = 1\right\}.$$

Note that we can write condition (3) of theorem 5.26 as a function of the elements of Δ. In fact if $(X+a)^n = X^n + a$ in $\mathbb{Z}_n[X]/(\Phi_r(X))$, this relation holds in $\mathcal{A}$ too, since $\mathcal{A}$ is a quotient ring of $\mathbb{Z}_n[X]/(\Phi_r(X))$. That is to say

$$(X+a)^n = \sigma_n(X+a) \quad \Rightarrow \quad (X+a) \in \mathcal{G}.$$

Note that $\mathcal{G}$ is a multiplicative subgroup of $\mathcal{A}^*$, since for each $a, b \in \mathcal{G}$ we can write

$$\sigma_n(ab) = \sigma_n(a)\sigma_n(b) = a^n b^n = (ab)^n \in \mathcal{G},$$

thanks to the automorphism properties of σ_n. On the other hand $\mathcal{G}$ is not an additive subgroup of $\mathcal{A}^*$ since

$$\sigma_n(a+b) = \sigma_n(a) + \sigma_n(b) = a^n + b^n \neq (a+b)^n,$$

when n is not prime. We need a lemma:

Lemma 5.28. *Δ commutes with $\mathcal{G}$-action.*

Proof. Let $a \in \mathcal{G}$ and $\sigma_k \in \Delta$. It suffices to show that $\sigma_k(a) \in \mathcal{G}$ for each $k \in \mathbb{Z}/r\mathbb{Z}$. Note that $\sigma_k(a) \in \mathcal{G}$ if and only if $\sigma_n(\sigma_k(a)) = (\sigma_k(a))^n$. Indeed

$$\begin{aligned}\sigma_n(\sigma_k(a)) &\stackrel{?}{=} (\sigma_k(a))^n \\ &= \sigma_k(a^n) \\ &= \sigma_k(\sigma_n(a)) \\ &= \sigma_n(\sigma_k(a)),\end{aligned}$$

where we used the fact that $\Delta \simeq (\mathbb{Z}/r\mathbb{Z})^*$ is commutative in the last passage. □

There are two special elements of Δ, namely σ_n and σ_p. The former is such that $\sigma_n(a) = a^n$ for each $a \in \mathcal{G}$ (by definition of $\mathcal{G}$). The latter is special because we are in characteristic p; let $g(X) \in \mathcal{G}$, since $\mathcal{G}$ is a subgroup of $\mathcal{A}^*$ we can write

$$\sigma_p(g(X)) = g(X^p) = g^p(X) \quad \forall\, g(X) \in \mathcal{G}.$$

Now denote with Γ the group generated by (σ_n, σ_p); an element of Γ is of the form σ_m, with $m = n^i p^j$ for some positive integers i, j. Let $a \in \mathcal{G}$, hence

$$\sigma_m(a) = a^m,$$

and we know as the element σ_m acts, since we know how the elements of the basis (σ_n, σ_p) behave. It is easy to see that the exponent m of the element $\sigma_m \in \Gamma$ is well-defined only modulo the *exponent*[13] of the group $\mathcal{G}$. One can show that, since $\mathcal{G}$ is abelian, the exponent is the maximum order of the element of the group itself. Hence we have an homomorphism[14]:

$$\begin{aligned}\Gamma &\longrightarrow (\mathbb{Z}/exp(\mathcal{G})\mathbb{Z})^* \\ \sigma_m &\mapsto m.\end{aligned}$$

We have seen that $\mathcal{A}$ is not a field, but we can write it as a product of fields

$$\mathcal{A} \simeq \prod_{\phi \text{ irreducible}} \mathbb{F}_{p^d},$$

[13] We recall the definition:

Definition 5.6 (Exponent of a group $\mathbb{G}$). The *exponent* of a group $\mathcal{G}$ is the minimum positive integer such that it annihilates all the elements of the group, i. e.

$$exp(\mathbb{G}) = \min\left\{h \in \mathbb{Z}_{\geq 0} :\ a^h = e\ \forall\, a \in \mathbb{G}\right\},$$

being e the identity element of $\mathbb{G}$. □

[14] This is clearly an homomorphism since $\sigma_{mm'}$ is mapped on to $m \cdot m'$.

being $\mathbb{F}_{p^d} = \mathcal{K} \simeq \mathbb{Z}_p[X]/(\phi(X))$ and $d = deg(\phi) = ord(p \bmod r)$. Consider the canonical projection $\pi : \mathcal{A} \longrightarrow \mathcal{K}$ and apply it to the group $\mathcal{G}$ too:

$$\begin{array}{ccc} \mathcal{A}^* & \supset & \mathcal{G} \\ \downarrow \pi & & \downarrow \pi \\ \mathcal{K}^* & \supset & \mathcal{H}. \end{array}$$

Note that π maps also $\mathcal{A}^* \longrightarrow \mathcal{K}^*$ since an unity in $\mathcal{A}^*$ is also a unity in $\mathcal{K}^*$ (this is because an unity in $\mathcal{A}^*$ is an element which does not have common factors with $\Phi_r(X)$ and such an element cannot have factors in common with $\phi(X)|\Phi_r(X)$, hence it is a unity in $\mathcal{K}^*$). Moreover, since $\mathcal{K}^*$ and $\mathcal{H}$ are the multiplicative subgroup of a field, they are cyclic[15]; let $s = \#\mathcal{H}$, trivially $s|exp(\mathcal{G})$ since $\mathcal{H}$ is a cyclic quotient of $\mathcal{G}$. Thus we can conclude that the homomorphism $\Gamma \longrightarrow (\mathbb{Z}/exp(\mathcal{G})\mathbb{Z})^*$ induces another homomorphism

$$\Gamma \longrightarrow (\mathbb{Z}/s\mathbb{Z})^*$$
$$\sigma_m \mapsto m \bmod s.$$

It is enlightening to see what happens when n is prime, i. e. when $n = p$. $\mathcal{A} = \mathbb{Z}_p[X]/(\Phi_r(X))$ is still not a field, but

$$\mathcal{A} \simeq \prod_{\phi \text{ irreducible}} \mathbb{F}_{p^d},$$

being $\mathbb{F}_{p^d} = \mathcal{K} \simeq \mathbb{Z}_p[X]/(\phi(X))$, and now $d = deg(\phi) = ord(p \bmod r) = ord(n \bmod r)$. Hence the projection $\pi : \mathcal{A}^* \longrightarrow \mathcal{K}^*$ has a finite field of order $\#\mathcal{K}^* = p^d - 1 = n^d - 1$ elements as destination. Further

$$\mathcal{G} = \left\{ a \in \mathcal{A} : \ \sigma_p(a) = a^p \right\},$$

and $\Gamma \subset \Delta$ is now generated by the only element $\sigma_p = \sigma_n$; hence Γ is cyclic and its order is the order of $\sigma_p = \sigma_n$ in Δ, i. e. $\#\Gamma = ord(\sigma_n)$ in Δ. But $\Delta \simeq (\mathbb{Z}/r\mathbb{Z})^*$ so that we can conclude

$$\#\Gamma = ord(p \bmod r) = ord(n \bmod r) = d.$$

Moreover it is clear that when n is prime $\mathcal{G} = \mathcal{A}^*$ since

$$\sigma_n(a(X)) = \sigma_p(a(X)) = a(x^p) = (a(X))^p = (a(X))^n,$$

and this holds for each $a(X) \in \mathcal{A}^*$. As a consequence also $\mathcal{H} = \mathcal{K}^* \simeq (\mathbb{Z}/s\mathbb{Z})^*$, which yields

$$s = \#\mathcal{H} = \#\mathcal{K}^* = p^d - 1 = p^{\#\Gamma} - 1 = n^{\#\Gamma} - 1.$$

The conclusion is that Γ is very very small (since $r = O(\log^5(n))$), whereas $\mathcal{H}$ is huge.

[15] This is a well-known fact in elementary algebra[**10**].

The point is that, under conditions of theorem 5.26 (but without assuming that n is prime), something similar happens, and this suffices to prove the theorem. In particular we claim that if

$$s > n^{\left[\sqrt{\#\Gamma}\right]}, \tag{5.3}$$

then theorem 5.26 is proven. Let us suppose that $n = p \cdot q$, being q an (eventually not prime) co-factor of n and consider the element $\sigma_q = \sigma_n \sigma_p^{-1} \in \Gamma$ (since Γ is generated by σ_p and σ_n). Take all the elements of the form $\sigma_p^i \sigma_q^j$ with $0 \leq i, j \leq \left[\sqrt{\#\Gamma}\right]$. Since

$$\left(\left[\sqrt{\#\Gamma}\right] + 1\right)^2 > \#\Gamma,$$

we can conclude that the elements $\sigma_p^i \sigma_q^j$ with $0 \leq i, j \leq \left[\sqrt{\#\Gamma}\right]$ are not all distinct, that is to say there exist pairs $(i, j) \neq (i', j')$ such that

$$\sigma_p^i \sigma_q^j = \sigma_p^{i'} \sigma_q^{j'}.$$

Using the map $\Gamma \longrightarrow (\mathbb{Z}/s\mathbb{Z})^*$ we can conclude

$$p^i q^j \equiv p^{i'} q^{j'} \pmod{s}.$$

On the other hand, assuming equation (5.3) we can write

$$p^i q^j \leq p^{\left[\sqrt{\#\Gamma}\right]} q^{\left[\sqrt{\#\Gamma}\right]} = n^{\left[\sqrt{\#\Gamma}\right]} < s$$
$$p^{i'} q^{j'} \leq p^{\left[\sqrt{\#\Gamma}\right]} q^{\left[\sqrt{\#\Gamma}\right]} = n^{\left[\sqrt{\#\Gamma}\right]} < s,$$

so that indeed

$$p^i q^j = p^{i'} q^{j'}$$
$$p^{i-j} n^j = p^{i'-j'} n^{j'}$$
$$n^{j-j'} = p^{i'-i+j-j'},$$

and n is a prime power, since $(i, j) \neq (i', j')$.

Now we prove the claim, i. e. that equation (5.3) holds. First of all we give an estimate of $s = \#\mathcal{H}$ in terms of $\#\mathcal{G}$ and then we show that $\mathcal{G}$ is large. Since $\Gamma \subset \Delta$ is a subgroup of Δ we can consider *cosets* of Δ modulo Γ; that is to say we define an equivalence relation in Δ

$$\delta \varrho \delta' \quad \Leftrightarrow \quad \delta(\delta')^{-1} \in \Gamma.$$

In this way Δ is splitted in equivalence classes[16]:

$$\varrho(\delta) = \{\delta' \in \Delta : \ \delta' \varrho \delta\} = \left\{\delta' \in \Delta : \ \delta'\delta^{-1} = \gamma \in \Gamma\right\} =$$
$$= \{\delta' \in \Delta : \ \delta' = \gamma\delta \text{ for some } \gamma \in \Gamma\} = \delta\Gamma.$$

Let now $C \subset \Delta$ be the set obtained considering only one representant of each coset; clearly for each $\delta \in \Delta$ there exist unique elements $\gamma \in \Gamma$ and $c \in C$

[16]Since Δ is abelian there is no difference between left and right cosets.

such that $\delta = \gamma \cdot c$. Since $\Delta \simeq (\mathbb{Z}/r\mathbb{Z})^*$ we can conclude that $C \simeq \mathcal{D} \subset (\mathbb{Z}/r\mathbb{Z})^*$ and we can write

$$C = \left\{\sigma_j : \ j \in \mathcal{D}\right\},$$

where $\mathcal{D}$ is the set with the indexes representing each coset. Now consider the map:

$$\mathcal{G} \longrightarrow \prod_{j\in\mathcal{D}} \mathcal{K}^* = \underbrace{\mathcal{K} \times \cdots \times \mathcal{K}}_{\#C=\#\mathcal{D} \text{ times}}$$
$$a(X) \mapsto \left(\sigma_j(a(X)) \bmod \phi(X)\right)_{j\in\mathcal{D}},$$

where $\#\mathcal{D} = \frac{\#\Delta}{\#\Gamma} = \frac{r-1}{\#\Gamma}$. We show that this map is injective; first of all this is an isomorphism since σ_j is an isomorphism. It suffices to show that, if $a(X) \in \mathcal{G}$ is mapped onto the identity element $(1, \cdots, 1)$, then $a(X) = 1$. We evaluate

$$\sigma_{jn}(a(X)) = \sigma_j(\sigma_n(a(X))) = \sigma_j(a^n(X)) = (\sigma_j(a(X)))^n = 1$$
$$\sigma_{jp}(a(X)) = \sigma_j(\sigma_p(a(X))) = \sigma_j(a^p(X)) = (\sigma_j(a(X)))^p = 1,$$

so that $\sigma_j(a(X)) = 1$ for each $a(X) \in \Delta$ (or $j \in (\mathbb{Z}/r\mathbb{Z})^*$). Hence

$$\sigma_j(a(X) - 1) = 0 \quad \forall\ j \in (\mathbb{Z}/r\mathbb{Z})^*.$$

Since $a(X) - 1$ is an element of $\mathcal{G}$ we can write $a(X) - 1 = g(X) \bmod \Phi_r(X)$, so that

$$\sigma_j(a(X) - 1) = \sigma_j(g(X)) = g(X^j) \equiv 0 \pmod{\phi(X)} \quad \forall\ \phi(X) | Phi_r(X)$$
$$\Rightarrow \quad \Phi_r(X) | g(X)$$
$$\Rightarrow \quad a(X) - 1 = 0,$$

and the map is injective. This simple observation allows us to write

$$\#\mathcal{G} = \# \prod_{j\in\mathcal{D}} \mathcal{K}^*.$$

Recall that $\sigma_j(a(X)) \in \mathcal{G}$, since, by lemma 5.28 Δ preserves $\mathcal{G}$; thus

$$\#\mathcal{G} \leq \#\mathcal{H}^{\#\mathcal{D}} = s^{\frac{r-1}{\#\Gamma}}$$
$$\Rightarrow \quad s \geq \#\mathcal{G}^{\frac{\#\Gamma}{\#\Delta}}. \tag{5.4}$$

Now we show that $\mathcal{G}$ is large; the main reason is condition (3) of theorem 5.26, namely that $X - a \in \mathcal{G}$ for each $0 \leq a < r$. Since $p \not\equiv 1 \pmod{r}$, all the irreducible factors of $\Phi_r(X)$ have degree $d = ord(p \bmod r) \geq 2$, so that they cannot divide any polynomial of degree 1. As a consequence the elements $X - a$ (with $0 \leq a < r$) are not contained in any maximal ideal[17] of $\mathcal{A}$ (i. e.

[17] Recall that an ideal $\mathcal{I}$ of a ring R, $\mathcal{I} \neq R$, is *maximal* if

$$\forall\ \mathcal{K} \trianglelefteq R : \ \mathcal{I} \subseteq \mathcal{K} \subseteq R \quad \Rightarrow \quad \mathcal{K} = \mathcal{I} \text{ or } \mathcal{K} = R,$$

i. e. there are no intermediate ideals $\mathcal{K}$ between $\mathcal{I}$ and R.

they are units in $\mathcal{A}$). Consider the elements

$$\prod_{a\in\mathcal{J}}(X-a)\subset\mathcal{G}\qquad \mathcal{J}\subseteq\{0,1,\cdots,r-2\};$$

they are elements of $\mathcal{G}$ since condition (3) holds. We show that these elements are all distinct; in fact, since $\Phi_r(X)$ has degree $r-1$ the only elements that could be equal are the elements obtained considering $\mathcal{J}=\emptyset$ and $\mathcal{J}=\{0,1,\cdots,r-2\}$. This is only possible when

$$\prod_{a=0}^{r-2}(X-a)\equiv 1 \quad \text{in } \mathbb{Z}_p[X]/(\Phi_r(X))$$

$$\Leftrightarrow \quad \Phi_r(X)\mid \prod_{a=0}^{r-2}(X-a)-1.$$

Since both polynomials have the same degree we can conclude $\Phi_r(X)=\prod_{a=0}^{r-2}(X-a)-1$ and an inspection of the constant terms yield

$$-1\equiv 1 \pmod p \quad\Rightarrow\quad 2\equiv 0 \pmod p \quad\Rightarrow\quad 2|p,$$

that is impossible since p is odd. As a consequence there are 2^{r-1} possibilities for the subsets $\mathcal{J}$ and we can conclude

$$\#\mathcal{G}\geq 2^{r-1}. \tag{5.5}$$

Equations (5.4) and (5.5) imply

$$s\geq \#\mathcal{G}^{\frac{\#\Gamma}{r-1}}\geq 2^{\#\Gamma}.$$

Further condition (2) of theorem 5.26 tells us that

$$\#\Gamma=ord(n \bmod r)>\left(\frac{\log(n)}{\log(2)}\right)^2.$$

Putting all together:

$$\begin{aligned}\sqrt{\#\Gamma}&>\frac{\log(n)}{\log(2)}\\ \log(2)\sqrt{\#\Gamma}&>\log(n)\\ \log 2^{\sqrt{\#\Gamma}}&>\log(n)\\ 2^{\#\Gamma}&>n^{\sqrt{\#\Gamma}}\\ s>n^{\sqrt{\#\Gamma}}&\geq n^{\lfloor\sqrt{\#\Gamma}\rfloor},\end{aligned}$$

and the claim is proven.

CHAPTER 6

Integer Factoring

Contents

In number theory, integer factorization is the way of breaking down a composite number into smaller non-trivial divisors, which when multiplied together equal the original integer. When the numbers are very large, no efficient integer factorization algorithm is publicly known; this is the reason why some cryptosystems (e. g. RSA[**40**]) are based on the hardness of this problem. A recent effort which factored a 200-digit number (RSA-200) took eighteen months and used over half a century of computer time. In this chapter we introduce the major algorithms known.

Let $p|n$ be the smallest prime divisor of n (the number we want to factor). It is quite obvious that $p \leq \sqrt{n}$. A first simple algorithm is to choose a random value $d < n$ and to hope that $\gcd(d, n) > 1$. Since the probability that the number d we have chosen is divisible by p is $\frac{1}{p}$, and since the gcd's evaluation costs $O(\log^3(p))$ we have a running-time of $O(p \log^3(n))$ and in the worst case:

$$\text{Worst Case: } \Rightarrow \quad O\left(e^{\frac{1}{2}\log(n)} \log^3(n)\right),$$

which is exponential.

Another idea is to look for p simply dividing n by all primes less than or equal to $\sqrt{n}$; this algorithm is called *trial division*. Since we need many divisions as the number of primes less than or equal to p, i. e. by theorem A.1 $\pi(p) \approx \frac{p}{\log(p)}$, we have a complexity of:

$$\text{Running-Time: } \Rightarrow \quad O\left(\frac{p}{\log(p)} \log^2(n)\right),$$

and in the worst case $p \approx \sqrt{n}$ we have:

$$\text{Worst Case: } \Rightarrow \quad O\left(\frac{\sqrt{n}}{\log(\sqrt{n})}\log^2(n)\right) = O\left(e^{\frac{1}{2}\log(n)}\log(n)\right),$$

which is exponential.

6.1. Pollard ρ

The Pollard ρ algorithm is based on the *birthday paradox*. Let $N \in \mathbb{Z}_{>0}$ be a large integer. We ask which is the probability that, chosen k random elements in a set $\mathcal{A}$ (with $\#\mathcal{A} = N$), at least two elements are equal[1]. Let P_0 denote the probability that there are no collisions and suppose $k \ll N$; chosen two elements in $\mathcal{A}$, they are different with probability $1 - \frac{1}{N}$. Chosen a third element this is different from both the previous ones with probability $1 - \frac{2}{N}$ and so on. Hence

$$P_0 = \left(1 - \frac{1}{N}\right)\left(1 - \frac{2}{N}\right)\cdots\left(1 - \frac{k-1}{N}\right).$$

We compute the logarithm and use the approximation $\log(x+1) \approx x$ if $x \ll 1$, which yields:

$$\begin{aligned}
\log(P_0) &= -\frac{1}{N} - \frac{2}{N} - \cdots - \frac{k-1}{N} = -\frac{1}{N}\sum_{m=1}^{k-2} m = -\frac{1}{N}\frac{k(k-1)}{2} \\
&= -\frac{1}{2N}(k(k-1)) \approx -\frac{k^2}{2N} \\
\Rightarrow \quad P_0 &\approx e^{-\frac{k^2}{2N}} \qquad \text{and} \qquad 1 - P_0 = 1 - e^{-\frac{k^2}{2N}}.
\end{aligned}$$

Hence if we want $1 - P_0 \geq \frac{1}{2}$:

$$\begin{aligned}
& 1 - P_0 \geq \frac{1}{2} \\
\Rightarrow \quad & 1 - e^{-\frac{k^2}{2N}} \geq \frac{1}{2} \\
\Rightarrow \quad & e^{-\frac{k^2}{2N}} \leq \frac{1}{2} \\
\Rightarrow \quad & k \geq \sqrt{2\log(2)}\sqrt{N} \approx 1.17\sqrt{N} = O(\sqrt{N}).
\end{aligned}$$

With this in mind, let p be the smallest prime divisor of $n \in \mathbb{Z}_{\geq 0}$. Let us suppose that there are two integer $x, x' \in \mathbb{Z}_n$ such that $x \neq x'$ but $x \equiv x' \pmod{p}$. Thus $p \leq d = \gcd(x - x', n) < n$ is a proper divisor of n, and we have found a factor of n computing one gcd (obviously without knowing p). The

[1]The name of the paradox comes from the fact that when $N = 365$ we are evaluating the probability that in a room with k people, there are at least two with the same day of birth. As we will see $k = 23$ suffices to have a probability grater than $\frac{1}{2}$, that could seem paradoxical.

idea is to choose a random subset $\mathcal{A}' \subseteq \mathbb{Z}_n$, to evaluate $\gcd(x-x', n)$ for every pair $x, x' \in \mathcal{A}'$ (with $x \neq x'$) and to *hope* that the mapping $x \mapsto x \bmod p$ brings at least one collision in $\mathcal{A} = \mathbb{Z}_p$. Using the birthday paradox we can state that this happens with probability grater than $\frac{1}{2}$ when $k = \#\mathcal{A}' = O(\sqrt{p})$. Since p is not known, we need to evaluate at most $\binom{\#\mathcal{A}'}{2} \geq \frac{p}{2}$. Now we try to improve this result.

Let us suppose that the mapping defined by the polynomial $f(X) = X^2+a$ (with $f(X) \in \mathbb{Z}[X]$), namely $x \mapsto f(x)$, is a *random*[2] *mapping*. We fix an element $x_1 \in \mathbb{Z}_n$ and define a *random walk*:

$$x_j = f(x_{j-1}) \bmod n \qquad \forall\ j \geq 2.$$

Let m be an integer and let us suppose that $\mathcal{A}' = \{x_1, \cdots, x_m\}$ is made-up of distinct elements of $\mathbb{Z}_n$. We are looking for a pair of elements such that $\gcd(x_i - x_j, n) > 1$. Let us suppose that we have found such a pair, hence $x_i \equiv x_j \pmod p$ and thus $f(x_i) \equiv f(x_j) \pmod p$. This yields:

$$x_{i+1} = f(x_i) \equiv f(x_j) = x_{j+1} \pmod n \quad \Rightarrow \quad x_{i+1} \equiv x_{j+1} \pmod p.$$

In a similar fashion it is easy to see that:

$$x_i \equiv x_j \quad \Rightarrow \quad x_{i+\delta} \equiv x_{j+\delta} \pmod p \quad \forall\ \delta > 0.$$

In other words, if $\ell = j - i$, then $x_{i'} \equiv x_{j'} \pmod p$ when $j' > i' \geq i$ and $j' - i' \equiv 0 \pmod \ell$. Thus we can draw a graph with vertex in $\mathbb{Z}_p$ and arrows from $x_i \bmod p$ to $x_{i+1} \bmod p$; the graph has a tail:

$$x_1 \bmod p \to x_2 \bmod p \to \cdots \to x_i \bmod p,$$

and a loop of length $\ell = j - i$ that repeat itself ad-libitum (see figure 6.1):

$$x_i \bmod p \to x_{i+1} \bmod p \to \cdots \to x_j \equiv x_i \pmod p.$$

Now let us consider only the collision with $j = 2i$. If $x_i \equiv x_{2i} \pmod p$, also $x_{i'} \equiv x_{2i'} \pmod p$, for each $i \equiv 0 \pmod \ell$ and $i' > i$. We choose two random walks:

$$x_1 \to f(x_1) = x_2 \to f(x_2) = x_3 \cdots$$
$$x_2 \to f(f(x_1)) = x_4 \to f(f(x_4)) = x_6 \cdots,$$

and we check whether $\gcd(x_{2i} - x_i, n) > 1$ is a non-trivial divisor of n or not. Let i be the index of the first element in the loop, thus:

$$x_q \equiv x_{q+s\ell} \pmod p \quad \forall\ q \geq i,\ s \in \mathbb{Z}_{\geq 0},\ \ell = j - i.$$

If we want a collision for $j = 2i$ it must be $q = sl = s(j - i)$; hence:

$$s = \frac{q}{j-i} \geq \frac{i}{j-i},$$

[2]Clearly this is not the case; the mapping is instead pseudo-random, so that we are presenting an heuristic.

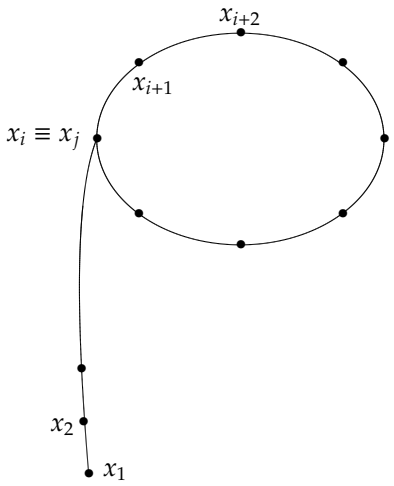


FIGURE 6.1. Pollard's ρ loop.

since $q \geq i$. The smallest integer of that form is $\left[\frac{i}{j-i}\right] + 1$. For such a value:

$$q = s(i-j) = \left(\left[\frac{i}{j-i}\right] + 1\right)(j-i) \leq \left(\frac{i}{j-i} + 1\right)(j-i) = j.$$

Hence in $\approx \sqrt{p}$ steps we find a collision $x_i \equiv x_{2i} \pmod{p}$, so that the complexity is $O\left(\sqrt{p}\log^3(n)\right)$ and in the worst case $p \approx \sqrt{n}$:

$$\text{Worst Case: } \Rightarrow \quad O\left(n^{\frac{1}{4}}\log^3(n)\right) = O\left(e^{\frac{1}{4}\log(n)}\log^3(n)\right),$$

which is exponential, but the factor $\frac{1}{4}$ in the exponent is a good improvement.

6.2. Pollard $p-1$

This is another idea of Pollard. Here we find a situation pretty similar to the case of Pocklington's test and its extension on elliptic curves over finite fields: although the algorithm $p-1$ we will describe now works only if you are very lucky, its elliptic curve version is really efficient.

Denote, as usual, with n the integer to factor; we choose a bound B which is an estimate on the number of step we are disposed to do. We then evaluate:

$$M = \prod_{\substack{p \leq B \\ p \text{ prime} \\ p^{e(p)} \leq B}} p^{e(p)}. \tag{6.1}$$

EXAMPLE 6.1. If $B = 20$, we have $M = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$. □

Using the Prime Number Theorem (see appendix A) we can write $M \approx e^B$. Now we fix a random value $x \in \mathbb{Z}_n^*$ and we compute $y = x^M \bmod n$ and $\gcd(y-1, n) = d$. The *hope* is that $1 < d < n$, so that we have found a non-trivial factor d of n.

EXAMPLE 6.2. Let $n = 10001$ and $B = 10$, so that $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$. For $x = 2 \in \mathbb{Z}_{10001}^*$ we have:

$$y = x^M = 2^{2520} \equiv 3579 \pmod{10001}$$
$$\gcd(3579 - 1, 10001) = 73.$$

Indeed $10001 = 73 \cdot 137$. □

Let p be the minimal prime divisor of n; the algorithm allows us to find p if $p | \gcd(y-1, n)$, i. e. if $p|(y-1)$ since p is a divisor of n. Hence, if this is the case:

$$p|(y-1) \quad \Rightarrow \quad y \equiv 1 \pmod{p} \quad \Rightarrow \quad x^M \equiv 1 \pmod{p}.$$

By Fermat's little theorem, thus, it suffices that M is a multiple of $p-1$, i. e. $p-1$ must divide M. This is possible only if all prime divisors of $p-1$ are smaller then B (by construction of M), i. e. if $p-1$ is *B-smooth*.

DEFINITION 6.1 (Smooth numbers). Let $B \in \mathbb{R}_{>0}$ and $n \in \mathbb{Z}_{>0}$. We say that n is *B-smooth*, if all prime divisors of n are smaller than B. □

EXAMPLE 6.3. For example 100 is 10-smooth, since $100 = 5^2 \cdot 2^2$ and $2, 5 < 10$. □

Hence we can conclude that the Pollard $p-1$ algorithm, works only if $p-1$ is B-smooth. The computational cost is given by the evaluation of $y = x^M \bmod n$ and of the gcd, i. e.

$$\text{Running-Time:} \Rightarrow \quad O\left(\log(M)\log^2(n) + \log^3(n)\right) = O\left(B\log^2(n)\right).$$

In practice, if $B \approx n^{\frac{1}{10}}$, one can see that the probability that n has a prime divisor p such that $p-1$ is B-smooth, is very low; hence the algorithm works only if you are very like. Note that the larger the value of B, the larger the probability that a number is B-smooth; on the other hand the complexity is exponential in $\log(B)$ (or, that is the same, linear in B).

From an algebraic point of view we can consider the reduction modulo p, that is a group homomorphism. The algorithm works if the image of $x^M \in \mathbb{Z}_n^*$ after reduction modulo p is 1 ($x^M \equiv 1 \pmod{p}$), whereas $x^M \bmod q$ is not 1 for all the other prime divisors q of n (see figure 6.2).

6.3. Lenstra and the ECM

Even if Pollard's $p-1$ algorithm is less efficient than Pollard's ρ algorithm, in 1985, Lenstra used Pollard $p-1$ to develop one of the best

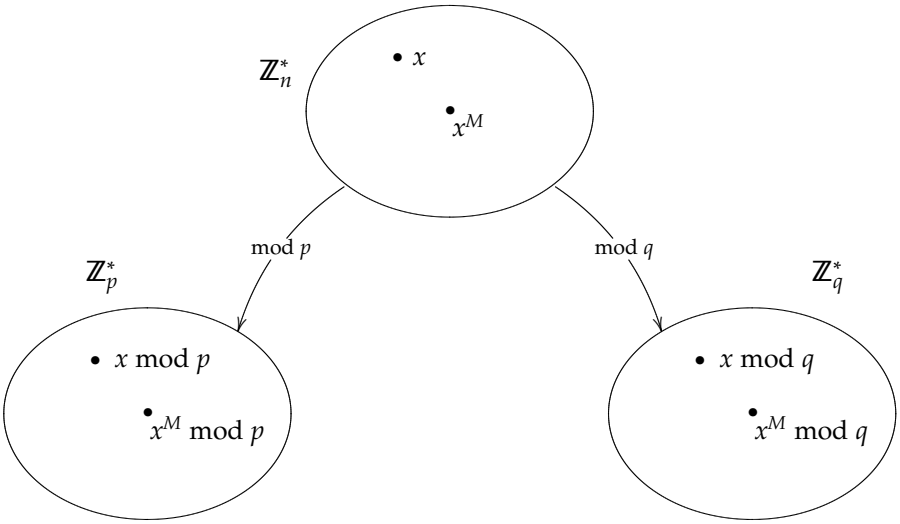


FIGURE 6.2. Pollard's $p-1$ succeeds in finding the prime divisor p of n, only if $x^M \equiv 1 \pmod{p}$ whereas x^M is not 1 modulo q, for each other prime divisor q of n.

factorization algorithms today known: the *Elliptic Curve Method* (ECM). Recall that Pollard $p-1$ works when $p-1$ is B-smooth and $p-1 = \#\mathbb{Z}_p^*$. Lenstra's idea is to replace $\mathbb{Z}_p$ with $E(\mathbb{Z}_p)$, being E a non-singular elliptic curve. Exactly like in Pollard $p-1$, p is not known and all the computations are hence made in $E(\mathbb{Z}_n)$ (in place of $\mathbb{Z}_n^*$).

Consider the elliptic curve with equation:

$$E: \; Y^2 = X^3 + AX + B \qquad \gcd(n,6) = 1 \text{ and } \gcd(\Delta_E, n) = 1,$$

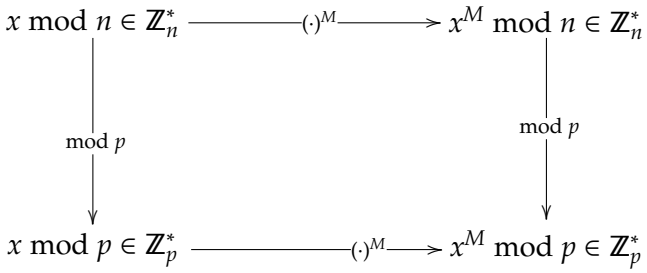
with $\Delta_E = 4A^3 + 27B^2 \neq 0$; in other words the discriminant Δ_E is not divisible by any of the primes divisors of n, that is to say E is a non-singular[3] elliptic curve over $\mathbb{Z}_q$, for each prime divisor q of n. Note that this preliminary test is polynomial (because it suffices to evaluate one gcd); moreover if $\gcd(\Delta_E, n) \neq 1$ we have found a divisor of n. Now consider the

[3]We need to be a little bit careful in the choice of the random curve E. Since the extraction of a square root modulo n (when n is not prime) is equivalent to factor n[**38**], it is better to choose the point P before the curve E. In other words, first one chooses a point $P = (x_0, y_0)$ and a random value A; then

$$B = y_0^2 - x_0^3 - Ax_0.$$

Lastly one can check that $\gcd(\Delta_E, n) = 1$.

ring homomorphism:



We can evaluate the element $x^M \bmod p$ of $\mathbb{Z}_p^*$ following two equivalent roads: either first reducing modulo p and raising to the M-th power, or first raising to the M-th power and then reducing modulo p. This is still true if we replace $\mathbb{Z}_n^*$ and $\mathbb{Z}_p^*$ with $E(\mathbb{Z}_n)$ and $E(\mathbb{Z}_p)$. Further, suppose for a while that $n = pq$ where p and q are distinct primes greater than 3. The Chinese Remainder Theorem implies

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z} \quad \text{(as rings)} \\ (\mathbb{Z}/n\mathbb{Z})^* &\simeq (\mathbb{Z}/p\mathbb{Z})^* \times (\mathbb{Z}/q\mathbb{Z})^* \quad \text{(as groups)} \\ E(\mathbb{Z}_n) &\simeq E(\mathbb{Z}_p) \times E(\mathbb{Z}_q) \quad \text{(as groups)}. \end{aligned}$$

Hence the set $E(\mathbb{Z}_n)$ inherits the structure of an abelian group: most pairs of points in $E(\mathbb{Z}_n)$ can be added using the formulas of equation (2.1). In fact, the formulas fail only if some calculated quantity in $E(\mathbb{Z}_n)$ is zero modulo p and non-zero modulo q or vice versa, in which case n is factored!

Now we are ready to translate the algorithm using elliptic curves. We choose a bound B and we compute the value M of equation (6.1). Thus we choose a random point in $E(\mathbb{Z}_n)$ and we try to evaluate $[M]P$ in $E(\mathbb{Z}_n)$ which is the corresponding of $y = x^M$ in Pollard's $p-1$ algorithm. If at some point the formula to evaluate λ (in equation (2.1)) fails (that is to say when we find a non-invertible value), then we have found a factor of n. This happens only if:

$$\begin{aligned} & [M]P = \infty \text{ in } E(\mathbb{Z}_p) \\ & [M]P \neq \infty \text{ in } E(\mathbb{Z}_q)\ \forall \text{ prime divisor } q \neq p \text{ of } n \\ \Leftrightarrow\ & \#E(\mathbb{Z}_p) | M \quad \text{i. e. } \#E(\mathbb{Z}_p) \text{ is } B\text{-smooth.} \end{aligned}$$

Example 6.4. Consider $n = 35$ and suppose to use $E: Y^2 = X^3 - X - 2$. It is easily verified that $\gcd(\Delta_E, 35) = 1$. Let us choose $M = 3$ (to simplify computation, it is just to render the idea) and we fix a point $P \in E(\mathbb{Z}_n)$, for example $P = (2, 2)$. Now we should evaluate $[M]P$ in $E(\mathbb{Z}_p)$ and hope that $[M]P = \infty$ in $E(\mathbb{Z}_p)$, whereas $[M]P$ is not ∞ in $E(\mathbb{Z}_q)$, for each prime divisor $q \neq p$ of n. Clearly we don't know p, but, if this is the case, it suffices to compute $[M]P = [3]P = P + P + P$ in $E(\mathbb{Z}_n)$ to find a factor of n. We start

evaluating $[2]P$:

$$\lambda = \frac{3x_P^2 + A}{2y_P} = \frac{11}{4} = \frac{11 \cdot 9}{4 \cdot 9} \equiv 99 \equiv -6 \pmod{35};$$

hence

$$x_{2P} = -x_P - x_P + \lambda^2 \equiv -3 \pmod{35}$$
$$y_{2P} = -y_P - \lambda(x_{2P} - x_P) \equiv 3 \pmod{35}.$$

Thus $[2]P = (-3, 3)$. If now we try to compute $[3]P = 2P + P = (-3, 3) + (2, 2)$ we have:

$$\lambda = \frac{3 - 2}{-3 - 2} = -\frac{1}{5},$$

and 5 is non-invertible in $\mathbb{Z}_{35}$. Hence we have found a factor of $n = 5 \cdot 7$. It is easy to check that:

$$[3]P = (2, -2) + (2, 2) = \infty \text{ in } E(\mathbb{Z}_5)$$
$$[3]P = (-3, 3) + (2, 2) \neq \infty \text{ in } E(\mathbb{Z}_7),$$

where $E(\mathbb{Z}_{35}) \simeq E(\mathbb{Z}_7) \times E(\mathbb{Z}_5)$. □

At this point we have just translated the algorithm of the previous section. However here the situation is different since we have one more degree of freedom: if the algorithm fails we can simply try again with another curve, whereas $\mathbb{Z}_p^*$ is unique. In other words, when Pollard $p - 1$ fails (i. e. if $\#\mathbb{Z}_p^*$ is not B-smooth), we could only increase the value of B until $p - 1$ becomes B-smooth. On the other hand, when the ECM fails with a certain curve E, i. e. if $\#E(\mathbb{Z}_p)$ is not B-smooth, we can leave B fixed, try another curve E' and *hope* that now $\#E'(\mathbb{Z}_p)$ is B-smooth. This is the strength of this algorithm.

Now we estimate the computational cost of the ECM. In practice we need to evaluate how many curves one must try before succeeding. We need two ingredients:

(1) The distribution of the number of curves over $\mathbb{Z}_p$ with respect to their number of points. We have already discussed this point in section 5.4 (see theorem (5.25)). The conclusion is that the distribution is almost *uniform*.
(2) B-smooth numbers. How many B-smooth numbers are there?

First of all we try to give an answer to the second question. It is clear that if $B' > B$ all B'-smooth numbers are also B-smooth; in other words, the larger the value of B, the larger the number of B-smooth numbers.

Definition 6.2. We express B in function of another parameter $u \in \mathbb{R}_{>1}$: $B = X^{\frac{1}{u}}$. Moreover we denote the cardinality of the set of B-smooth numbers less than or equal to X with:

$$\Psi(X, X^{\frac{1}{u}}) = \#\{x \leq X : \ x \text{ is } B\text{-smooth}\}.$$

□

The following result is crucial for our analysis:

THEOREM 6.1 (Dickmann and De Bruyn). *With the notation as introduced above we have:*

$$\frac{\Psi(X, X^{\frac{1}{u}})}{X} \approx \frac{1}{u^u}.$$

□

Therefore theorem 6.1 is telling us that the proportion of numbers less than or equal to X that are B-smooth is u^{-u}; if u increases then B decreases and the proportion decreases (and viceversa, as we expected to be). The conclusion is that the probability that a number near to X is $X^{\frac{1}{u}}$-smooth is more or less u^{-u}, i. e. smooth numbers are *rare*.

EXAMPLE 6.5. Let $u = 2$, so that $B = \sqrt{X}$. The probability that a number near to X is $\sqrt{X}$-smooth is more or less $\frac{1}{4}$; in other words about 75% of numbers x have a prime divisor greater than $\sqrt{x}$. For $u = 10$ we have $B = X^{\frac{1}{10}}$, and the probability that $x \approx X$ is $X^{\frac{1}{10}}$-smooth is more or less 10^{-10} (very very small). □

Now we have all the elements to estimate the complexity. The ECM works if $E(\mathbb{Z}_p)$ is B-smooth; if this is not the case you need to try another curve and hope again. Let us write:

$$B = p^{\frac{1}{u}} \quad \Rightarrow \quad u = \frac{\log(p)}{\log(B)}.$$

We need to evaluate the work needed for a single curve and the number of curve one must try. Since the distribution of the number of curves as a function of their number of points is almost uniform, we can conclude that the probability that $E(\mathbb{Z}_p)$ is B-smooth is approximately u^{-u}. In other words we expect to try about u^u curves before $E(\mathbb{Z}_p)$ is B-smooth. For each curve the complexity is dominated by the evaluation of $[M]P$ in $E(\mathbb{Z}_n)$, which requires $O(\log(M)\log^3(n)) = O(B\log^3(n))$. Hence the total cost is:

$$O\left(u^u B \log^3(n)\right) = O\left(u^u B\right) = O\left(u^u p^{\frac{1}{u}}\right).$$

Since we have not yet fixed B, now we want to compute the optimal value of B (hence of u) that *minimizes* the total work:

$$W(u) = W(B) = u^u p^{\frac{1}{u}}.$$

Indeed, as it is depicted in figure 6.3, when $u \to 0$, $W(u) \to \infty$, whereas when $u \to \infty$, $W(u) \to \infty$; hence there is a point u^* for which the work is minimum.

We evaluate the logarithm:

$$\log(W(u)) = u\log(u) + \frac{1}{u}\log(p),$$

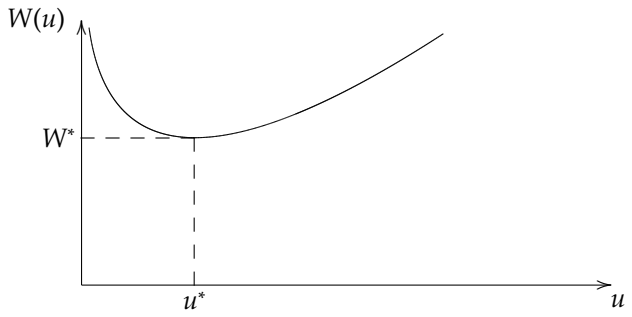


FIGURE 6.3. Total work $W(u)$ as a function of u.

and we look for u^*:

$$\frac{d}{du}\log(W(u)) = 1 + \log(u) - \frac{1}{u^2}\log(p) \stackrel{!}{=} 0$$
$$\Rightarrow \quad \frac{d^2}{du^2}\log(W(u)) > 0 \quad \Rightarrow \quad u^* \text{ is a minimum.}$$

We need a lemma:

LEMMA 6.2. *Let $X, Y \in \mathbb{R}_{\gg 0}$. Then*

$$X\log(X) = Y \quad \Rightarrow \quad X \approx \frac{Y}{\log(Y)}.$$

□

Manipulating:

$$\frac{d}{du}\log(W(u)) = 0 \quad \Rightarrow \quad \log(e) + \log(u^*) - \frac{1}{(u^*)^2}\log(p) = 0$$
$$\log(eu^*) = \frac{\log(p)}{(u^*)^2} \quad \Rightarrow \quad (u^*)^2\log(eu^*) = \log(p)$$
$$2(eu^*)^2\log(eu^*) = 2e^2\log(p) \quad \Rightarrow \quad (eu^*)^2\log(eu^*)^2 = 2e^2\log(p),$$

and using lemma 6.2 yields

$$(eu^*)^2 = \frac{2e^2\log(p)}{\log(2e^2\log(p))}$$
$$\Rightarrow \quad (u^*)^2 = \frac{2\log(p)}{\log\log(p) + \log(2e^2)} \approx \frac{2\log(p)}{\log\log(p)}$$
$$\Rightarrow \quad \log(B^*) = \frac{\log(p)}{u^*} \approx \frac{\log(p)\sqrt{\log\log(p)}}{\sqrt{2\log(p)}}$$
$$\Rightarrow \quad B^* = e^{\frac{\sqrt{2}}{2}\sqrt{\log(p)\log\log(p)}}.$$

That is the optimal value of B with respect to the prime p we are looking for (we know only its order of magnitude). Hence we can evaluate the corresponding value of W^*; first we compute $u^* \log(u^*)$:

$$\begin{aligned} u^* \log(u^*) &= \sqrt{\frac{2\log(p)}{\log\log(p)}}\frac{1}{2}\left(\log(2\log(p)) - \log\log\log(p)\right) \\ &\approx \sqrt{\frac{2\log(p)}{\log\log(p)}}\frac{1}{2}\log\log(p) = \sqrt{\frac{2}{4}\frac{\log(p)(\log\log(p))^2}{\log\log(p)}} \\ &= \sqrt{\frac{1}{2}\log(p)\log\log(p)} = \frac{\sqrt{2}}{2}\sqrt{\log(p)\log\log(p)}, \end{aligned}$$

and then:

$$W^* = B^*(u^*)^{u^*} = B^* e^{u^* \log(u^*)} = e^{\sqrt{2\log(p)\log\log(p)}}.$$

Finally, in the worst case $p \approx \sqrt{n}$, we find:

$$\text{Running-Time: } \Rightarrow \quad O\left(e^{\sqrt{\log(n)\log\log(n)}}\right),$$

which is sub-exponential.

There is a little trick that improves the efficiency of the ECM considerably. The idea is to split the algorithm in two phases; the first is identical to the algorithm discussed above. If phase one fails with a certain curve E, before changing the curve and try again with another one, we go to phase two. In the second phase we choose another smoothness bound $B' > B$ (typically $B' \approx 100B$) and we evaluate:

$$M' = \prod_{\substack{p \le B' \\ p \text{ prime} \\ p^{e(p)} \le B'}} p^{e(p)}.$$

Let $Q = [M]P$ be the last point computed in phase one; since we succeeded in evaluating Q, we have not factorized n, because the order of P is not B-smooth. The idea is to check if:

$$[q_i]Q = [q_i M]P = \infty \quad \forall \text{ primes } q_i \text{ such that } B < q_i < B'.$$

By the Prime Number Theorem we know that primes are quite dense: if $B \approx 10^4$ and $B' \approx 10^6$ we have more or less a probability of $\frac{1}{\log(10^5)} \approx \frac{1}{14}$ that a number in the range (B, B') is prime. Let δ_i be the distance between the primes q_i and q_{i+1}; hence:

$$\begin{aligned} [q_2]Q &= [q_1 + \delta_1]Q = [q_1]Q + [\delta_1]Q \\ [q_3]Q &= [q_2 + \delta_2]Q = [q_2]Q + [\delta_2]Q \\ [q_4]Q &= [q_3 + \delta_3]Q = [q_3]Q + [\delta_1]Q \\ &\cdots \\ &\cdots \end{aligned}$$

Since the points $[\delta_1]Q, [\delta_2]Q, \cdots$ could be pre-calculated, we can evaluate the points $[q_2]Q, [q_3]Q, \cdots$ only at the cost of a summation on the curve E.

6.4. The Quadratic Sieve

The *Quadratic Sieve* (QS) was the best factorization algorithm until the development of the *Number Field Sieve* (NFS) in 1993; the idea is an idea of Carl Pomerance in 1981. This algorithm is quite different from the ECM or Pollard ρ: whereas these algorithms succeed in first finding small factors of n, the quadratic field sieve and the number field sieve usually do not (hence they work well with an RSA number $n = p \cdot q$, with $p \approx q \approx \sqrt{n}$). The key observation was already known by Fermat in 1650: you can hope to factor n if you succeed in writing n as a difference of two squares:

$$n = u^2 - v^2 = (u + v)(u - v).$$

Example 6.6. Take $n = 221$, we can write:

$$n = 221 = 225 - 4 = 15^2 - 2^2 = (15 + 2)(15 - 2) = 13 \cdot 17.$$

□

Example 6.7. Take $n = 2009$, we can write:

$$n = 2009 = 2025 - 16 = 45^2 - 4^2 = (45 + 4)(45 - 4) = 49 \cdot 41.$$

□

Note that it suffices to find elements u and v such that $u^2 - v^2$ is divisible by n, i. e.

$$u^2 - v^2 \equiv 0 \pmod{n}.$$

If $v \in \mathbb{Z}_n^*$ we can write:

$$\begin{aligned} & u^2 - v^2 \equiv 0 \pmod{n} \\ \Leftrightarrow \quad & \left(\frac{u}{v}\right)^2 = t^2 \equiv 1 \pmod{n} \\ \Leftrightarrow \quad & (t + 1)(t - 1) \equiv 1 \pmod{n}, \end{aligned}$$

and hence

$$n = \gcd(n, t - 1) \gcd(n, t + 1).$$

Without loss of generality we can assume that n is odd; note that trivial solutions ($t = \pm 1$) yields trivial factorizations. Hence writing a relation of the kind $u^2 \equiv v^2 \pmod{n}$ is the same as writing $t^2 \equiv 1 \pmod{n}$.

We give an algebraic interpretation of this simple observation. Let R be a ring and denote with $e \in R$ an idempotent element, i. e. e is such that $e^2 = e$ in R. It is easily verified that $1 - e$ is idempotent too, being

$$(1 - e)^2 = 1 + e^2 - 2e = 1 + e - 2e = 1 - e.$$

As a consequence, we can split the ring R in two parts, namely $R/(e)$ and $R/(1-e)$, and the map:

$$R \longrightarrow R/(e) \times R/(1-e)$$
$$x \mapsto (x \bmod e, x \bmod (1-e)),$$

is a ring isomorphism. Here we see the link: $t^2 \equiv 1$ in R implies that the element $e = \frac{1-t}{2}$ is idempotent, since

$$e^2 = \frac{1+t^2-2t}{4} \equiv \frac{1-t}{2} \quad \text{in } R.$$

Also the converse is true, i. e. if e is idempotent then $t^2 \equiv 1$ in R, with $t = 1-2e$; in fact

$$t^2 = (1-2e)^2 = 1 + 4e^2 - 4e \equiv 1 + 4e - 4e \equiv 1 \quad \text{in } R.$$

Hence, finding a relation of the kind $t^2 \equiv 1 \pmod{n}$, is equivalent to find idempotent elements $e \in R = \mathbb{Z}_n$ and an algebraist knows that this is equivalent to factor n.

Now we deal with a more real example.

Example 6.8. Let $n = 2759$, as we have seen the idea is to try the values $u_i \approx \sqrt{n}$ and to hope that $u_i^2 - n$ is a square. Unfortunately this is not always

u_i	$u_i^2 - n$	Factorization
52	-55	$-5 \cdot 11$
53	50	$2 \cdot 5^2$
54	157	prime
55	266	$2 \cdot 7 \cdot 19$
56	377	$13 \cdot 29$
57	490	$2 \cdot 5 \cdot 7^2$
58	605	$5 \cdot 11^2$

Table 6.1. Values $u_i^2 - n$ for different values of u_i.

the case, as we see in table 6.1: we do not succeed in finding a square. The idea is to take the second column modulo n, i. e. $u_i^2 - n \equiv u_i^2 \pmod{n}$, so that for instance

$$53^2 \equiv 2 \cdot 5^2 \pmod{n} \quad 57^2 \equiv 2 \cdot 5 \cdot 7^2 \pmod{n} \quad 58^2 \equiv 5 \cdot 11^2 \pmod{n}.$$

Then we evaluate the product of (some of) these relations, obtaining

$$u^2 = (53 \cdot 57 \cdot 58)^2 \equiv 2^2 \cdot 5^4 \cdot 7^2 \cdot 11^2 = v^2 \pmod{n}.$$

Finally we hope that:

$$n = \gcd(u - v, n) \gcd(u + v, n),$$

is a non-trivial factorization of n. □

Hence now the main idea should be clear. We write the elements

$$Q(u_i) = u_i^2 - n,$$

with $u_i \in [\lfloor \sqrt{n} \rfloor - L, \lfloor \sqrt{n} \rfloor + L]$ and $L \in \mathbb{N}$, try to obtain a complete factorization of the result and look for any convenient combination that (multiplying) yields a relation of the form $u^2 \equiv v^2 \pmod{n}$. This is the *quadratic* part of the algorithm. Note that typically n will be an integer with 50 or 60 digits, hence $\sqrt{n} \approx 10^{25}$ and if $L \approx 10^5, 10^6$ we can conclude that $(\lfloor \sqrt{n} \rfloor + L)^2 - n \approx \sqrt{n}$, so that $Q(u_i) \approx \sqrt{n}$. Thus it is not a good idea to factor these elements; moreover the values $Q(u_i)$ that need to be considered is very high. Here comes the *sieving* part of the algorithm.

We choose a bound B (typically $B \approx 10^4$), and we define a *factor base*:

$$\mathcal{B} = \left\{\text{primes } \ell_j : \ \ell_j < B \text{ and } n \text{ is a quadratic residue modulo } \ell_j\right\}.$$

We know (by quadratic reciprocity theorem[4]) that, fixed u and n, the equivalence $u^2 \equiv n \pmod{\ell}$ (with ℓ prime), admits a solution for exactly half of the values $\ell < B$; in other words n is a quadratic residue modulo ℓ for half of the primes $\ell < B$, so that $\#\mathcal{B} = \frac{\pi(B)}{2}$. Further it is very simple to verify whether a prime $\ell < B$ is an element of $\mathcal{B}$ or not, since it suffices to check when

$$n^{\frac{\ell-1}{2}} \equiv 1 \pmod{\ell}.$$

Hence in the first part of the algorithm we populate an array with the values $Q(u_i)$ for each $u_i \in \mathcal{I} = [u_0 - L, u_0 + L]$ and $u_0 = \lfloor \sqrt{n} \rfloor$. Note that the congruence $X^2 \equiv n \pmod{\ell_j}$ admits a solution for each $\ell_j \in \mathcal{B}$, by construction of the factor base $\mathcal{B}$. We need a lemma:

Lemma 6.4 (Hensel's Lemma). *Let ℓ be a prime, $f(X) \in \mathbb{Z}[X]$ a monic polynomial, $a \in \mathbb{Z}$ an integer such that $f(a) \equiv 0 \pmod{\ell^k}$ (with $k \in \mathbb{N}_{>1}$) and $f'(a) \not\equiv 0 \pmod{\ell}$. Then there exists a unique value $b \in \mathbb{Z}$ such that:*

$$b \equiv a \pmod{\ell^k} \quad \textit{and} \quad f(b) \equiv 0 \pmod{\ell^{k+1}}.$$

---

[4] Also called the *aureum theorema* (golden theorem) by Gauss.

Theorem 6.3 (Quadratic Reciprocity). *If p and q are distinct odd primes, then the congruences*

$$x^2 \equiv p \pmod{q}$$
$$x^2 \equiv q \pmod{p},$$

are both solvable or both unsolvable unless both p and q leave the remainder 3 when divided by 4 (in which case one of the congruences is solvable and the other is not). Written symbolically,

$$\chi_p(q)\chi_q(p) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

where

$$\chi_p(q) = \begin{cases} 1 & \text{if } q \text{ is a quadratic residue modulo } p \\ -1 & \text{if } q \text{ is a quadratic non-residue modulo } p. \end{cases}$$

is the Legrende symbol.

PROOF. Let us suppose that $b \equiv a \pmod{\ell^k}$, i. e. $b = a + h \cdot \ell^k = a + \epsilon$. We ask how to choose b so that $f(b) \equiv 0 \pmod{\ell^{k+1}}$. Note that if $f(X) = \sum_m a_m X^m$ we can write:

$$\begin{aligned}\sum_m a_m (X+\epsilon)^m &\equiv \sum_m a_m (X^m + m X^{m-1}\epsilon) \\ &\equiv \sum_m a_m X^m + \epsilon \sum_m m a_m X^{m-1} \pmod{\epsilon^2} \\ \Rightarrow \quad f(X+\epsilon) &= f(X) + \epsilon f'(X) + O(\epsilon^2).\end{aligned}$$

Hence, since $f(a) \equiv 0 \pmod{\ell^{k+1}}$ and $\ell^k \equiv 0 \pmod{\ell^{k+1}}$, we have

$$f(a + h\ell^k) \equiv f(a) + h\ell^k f'(a) \equiv 0 \pmod{\ell^{k+1}}.$$

Thus there is no choice for h and, since $f'(a) \not\equiv 0 \pmod{\ell}$, we can divide by $f'(a)$ to obtain

$$h\ell^k \equiv -\frac{f(a)}{f'(a)} \pmod{\ell^{k+1}},$$

which yields the unique value of b[5]:

$$b = a - \frac{f(a)}{f'(a)}.$$

□

We are interested in the case $f(X) = X^2 - n$; note that $f'(X) = 2X$ and $2X \equiv 0 \pmod 2$ so that we must deal with the case $\ell = 2$ apart. Hence let us consider a generic element $\ell \in \mathcal{B}$, with $\ell \neq 2$; we solve for $X^2 \equiv n \pmod{\ell}$ using the Cantor-Zassenhaus (or the Tonelli-Shanks) algorithm and denote the solution as $x_0 \in \mathbb{Z}_\ell$. Note that $-x_0$ is a solution as well, and hence also $\pm x_0 + \ell, \pm x_0 + 2\ell, \cdots$ are solutions: we can thus look for the corresponding elements $Q(u_i)$ in our array and divide all of them by ℓ. Now we make an Hensel step, looking for solutions of $X^2 \equiv n \pmod{\ell^2}$; if $\pm x_1 \in \mathbb{Z}_{\ell^2}$ is a solution, also $\pm x_1 + \ell^2, \pm x_1 + 2\ell^2, \cdots$ are solutions and we can look for the corresponding elements $Q(u_i)$ in our array that are all divisible by ℓ^2. Thus we proceed with the case $X^2 \equiv n \pmod{\ell^3}$ and so on, until $\ell^k > L$; repeating this reasoning for each j we have evaluated the maximum power of ℓ_j, denoted with α_{ji}, dividing $Q(u_i)$.

If $\ell = 2$ is an element of $\mathcal{B}$, we cannot use Hensel's lemma directly to evaluate the maximum power of 2 that divides $Q(u_i)$. Since n is odd, if

[5]There is a close analogy with Newton's method in Calculus, where a solution $x \in \mathbb{R}$ of an equation $f(X) = 0$ is found as the limit of a convergent sequence of approximations x_i given by the recurrence relation

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}.$$

$2|(x^2-n)$, then x^2 must be odd too, i. e. $x^2 = 1+2y$, that is to say:

$$x^2 - n = (1+2y)^2 - n = 1 + 4y^2 + 4y - n = 4y(y+1) + 1 - n.$$

It follows that $x^2 - n$ is divisible by 8 only if $1-n$ is divisible by 8; hence if $n \not\equiv 1 \pmod 8$ the maximum number of factors 2 in x^2-n is the same as the number of factors 2 in $n-1$. On the other hand if $n \equiv 1 \pmod 8$ we can write:

$$x^2 - n = 4y^2 + 4y + 1 - n,$$

and we can use Hensel's lemma with $f(Y) = \frac{X^2-n}{4} = Y^2 + Y + \frac{1-n}{4}$ (since $f'(Y) = 2Y + 1 \equiv 1 \pmod 2$) to evaluate the maximum power of 2 which divides $Q(u_i^2)$.

This is the first part of the algorithm; the hope is that, after sieving, some element $Q(u_i)$ is divisible *only* for some (power) of the primes $\ell_j \in \mathcal{B}$, i. e. that some value $Q(u_i)$ is B-smooth. If this is the case, for this value we can write[6]:

$$Q(u_i) = u_i^2 - n = \prod_{j=1}^{\frac{\pi(B)}{2}} \ell_j^{\alpha_{ji}} \equiv u_i^2 \pmod n.$$

Let us suppose we have found M of these relations; in the second part of the algorithm we look for an opportunistic combination which yields a relation of the form $u^2 \equiv v^2 \pmod n$. Let $e_i \in \mathbb{Z}_2$, we evaluate the products:

$$\begin{aligned}\prod_{i=1}^{M} (u_i^2)^{e_i} &\equiv \prod_{i=1}^{M} \prod_{j=1}^{\frac{\pi(B)}{2}} \left(\ell_j^{\alpha_{ji}}\right)^{e_i} \\ &\equiv \prod_{j=1}^{\frac{\pi(B)}{2}} \left(\ell_j^{\sum_{i=1}^{M} \alpha_{ji} e_i}\right) \pmod n.\end{aligned}$$

Note that the first member is a square, whereas, as to make the second member a square as well, it suffices to write

$$\sum_{i=1}^{M} \alpha_{ji} e_i \equiv 0 \pmod 2 \quad \forall\, j = 1, 2, \cdots, \frac{\pi(B)}{2},$$

which yields a linear system:

$$\begin{pmatrix} \alpha_{11} & \cdots & \cdots & \alpha_{1M} \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \alpha_{N1} & \cdots & \cdots & \alpha_{NM} \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ \vdots \\ e_M \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod 2, \tag{6.2}$$

[6] We point out that it is *not* necessary that $Q(u_i)$ is divisible by all the elements in the factor base; in other words some values α_{ji} could be 0.

being $N = \frac{\pi(B)}{2}$. Note that, if $M > N$, i. e. the values $Q(u_i)$ that are $B-smooth$ are more than the elements in the factor base, then the system above admits non-zero solutions; in practice $M = N + 10$ usually suffices. Now, for each solution of the kind $(e_1, \cdots, e_M)$, we can write

$$u^2 = \left(\prod_{i=1}^{M} u_i^{e_i}\right)^2 \equiv \left(\prod_{j=1}^{N} \ell_j^{\frac{1}{2}\sum_{i=1}^{M}\alpha_{ji}e_i}\right)^2 = v^2 \pmod{n},$$

and we can hope to find a non-trivial factorization of n:

$$n = \gcd(u - v, n)\gcd(u + v, n).$$

Now we analyse the running-time of the algorithm. At this aim we need to evaluate the probability that the values $Q(u_i)$ are B-smooth. We have already observed that $Q(u_i) \approx \sqrt{n}$; hence, if $B = \sqrt{n}^{\frac{1}{u}}$, we can use theorem 6.1 to evaluate the probability that $Q(u_i)$ is B-smooth as u^{-u}. Since we need at least $M = \frac{\pi(B)}{2} = \frac{1}{2}\frac{B}{\log(B)} \approx B$ of these values, we must try at least Bu^u values $Q(u_i)$, so that:

$$2L \approx Bu^u = (\sqrt{n})^{\frac{1}{u}}u^u.$$

The next step is the sieving part: for each $\ell_j \in \mathcal{B}$ we must solve for $X^2 \equiv n \pmod{\ell_j}$ (using Cantor-Zassenhaus or Tonelli-Shanks, that run in polynomial time) and apply Hensel's lemma to determine the maximum power of ℓ_j which divide the elements $Q(u_i)$; hence for each ℓ_j we have a work of $\log^3(\ell_j) + \frac{2L}{\ell_j}$. Therefore the total work W_1, needed to build-up the matrix is approximately:

$$W_1 \approx \sum_{\substack{\ell < B \\ \ell \text{ prime}}} \left(\log^3(\ell) + \frac{2L}{\ell}\right) \approx Bu^u \sum_{\substack{\ell < B \\ \ell \text{ prime}}} \frac{1}{\ell},$$

and using Mertens' approximation (see appendix A)

$$\sum_{\substack{\ell < B \\ \ell \text{ prime}}} \frac{1}{\ell} \approx \log\log(B), \tag{6.3}$$

yields the estimate

$$W_1(u) \approx Bu^u \log\log(B) \approx Bu^u = (\sqrt{n})^{\frac{1}{u}}u^u.$$

The total work will be $W = W_1 + W_2$, being W_2 the complexity associated with the solution of the linear system of equation (6.2); since, as we will see, the contribution of W_2 is negligible, we look for the optimal value of u that minimizes $W_1(u)$ (see figure 6.4).

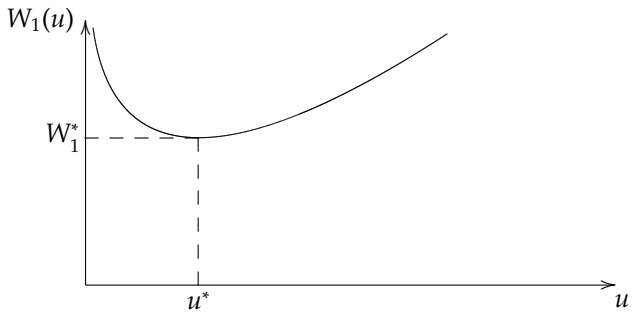


FIGURE 6.4. Partial work $W_1(u)$ as a function of u.

Hence we write

$$\begin{aligned}
&\log(W_1) = \frac{1}{u}\log(\sqrt{n}) + u\log(u)\\
&\frac{d}{du}\log(W_1) = -\frac{\log(\sqrt{n})}{u^2} + 1 + \log(u) \stackrel{!}{=} 0\\
\Rightarrow\quad &\log(u) + 1 = \frac{\log(\sqrt{n})}{u^2}\\
\Rightarrow\quad &u^2\log(ue) = \log(\sqrt{n})\\
\Rightarrow\quad &2e^2u^2\log(ue) = 2e^2\log(\sqrt{n})\\
\Rightarrow\quad &(ue)^2\log(ue)^2 = 2e^2\log(\sqrt{n})\\
\Rightarrow\quad &[\text{using lemma 6.2}]\\
\Rightarrow\quad &(ue)^2 = \frac{2e^2\log(\sqrt{n})}{\log(2e^2\log(\sqrt{n}))}\\
\Rightarrow\quad &u^* = \sqrt{\frac{\log(n)}{\log(e^2)+\log\log(n)}} \approx \sqrt{\frac{\log(n)}{\log\log(n)}}\\
\Rightarrow\quad &B^* = (\sqrt{n})^{\frac{1}{u^*}} = e^{\frac{1}{2}\sqrt{\log(n)\log\log(n)}},
\end{aligned}$$

so that, since now $(u^*)^{u^*} = B^*$, we have found

$$W_1^* = O\left(e^{\sqrt{\log(n)\log\log(n)}}\right) \approx L.$$

On the other hand, the value W_2 depends on the solution of the linear system of equation (6.2); since the matrix's dimension is $\approx B \times B$, Gaussian elimination yields a cost of $O(B^3)$, whereas the minimum cost, using better algorithms, is $O(B^2)$ (since you must at least write the matrix). Thus, using the optimal value B^*, it could seem that $W_2 = W_1$; in practice this is not the case, since the matrix is very sparse and $W_2 \ll W_1$, i. e. $W \approx W_1$.

We close this section presenting a couple of improvements of the algorithm; the first brings a modified version named *Multiple Polynomial Quadratic Sieve* (MPQS). The array we populated with the values $Q(u_i)$ is very long; as a consequence, on the edge of the interval $\mathcal{I}$, the values $Q(u_i)$ are large and the probability that $Q(u_i)$ is B-smooth is indeed very small, as it is depicted in figure 6.5.

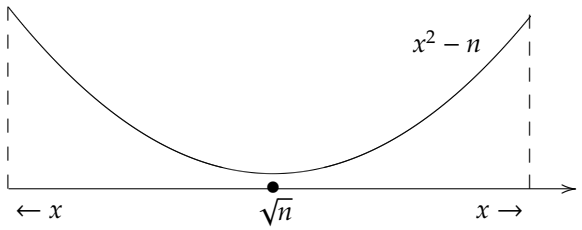


FIGURE 6.5. Values $x^2 - n$ as a function of x.

Hence the idea is to shorten the interval $\mathcal{I}$ and to use a different polynomial; for example we can use a linear shift $(GX + H)^2 - n$, with $G, H \in \mathbb{Z}$ such that $G \mid (H^2 - n)$ and G is a square. If this is the case we can write

$$\begin{aligned}(GX + H)^2 - n = G^2X^2 + 2GHX + H^2 - n = \\ = G\left(GX^2 + 2HX + \frac{H^2 - n}{G}\right),\end{aligned}$$

and since G is a square we can take

$$f(X) = \left(GX^2 + 2HX + \frac{H^2 - n}{G}\right).$$

EXAMPLE 6.9. Let $n = 10090009$; for $H = 4$ we have $H^2 - n = -3 \cdot 17 \cdot 43^2 \cdot 107$ and if we choose $G = 43^2$ we have

$$f(X) = 1849X^2 + 8X - 5457.$$

Hence, if $n \approx 10^{80}$ and $B \approx 10^4$, we have $\#\mathcal{B} \approx 1000$ and if we use $200,300$ polynomials $f(X)$ with $L \approx 5 \cdot 10^4$, each polynomial yields 2 or 3 complete factorizations (among the $\approx 10^4$ we need). □

The second improvement brings the so called *Large Prime Variation*. Let us suppose that, after sieving, we have obtained a partial factorization:

$$Q(u_i) = u_i^2 - n = \prod_j \ell_j^{\alpha_{ji}} \cdot q,$$

being q a prime such that $q < B^2$. Using the birthday paradox, there is a good probability that we find another value:

$$Q(u_m) = u_m^2 - n = \prod_j \ell_j^{\alpha'_{ji}} \cdot q,$$

with $m \neq i$. Hence

$$\frac{Q(u_i)}{Q(u_m)} = \frac{\prod_j \ell_j^{\alpha_{ji}}}{\prod_j \ell_j^{\alpha'_{ji}}} = \prod_j \ell_j^{\alpha''_{ji}},$$

is B-smooth. This trick could improve the efficiency up to a factor of 6.

6.5. The Number Field Sieve

The *Number Field Sieve* (NFS) is the most efficient factorization algorithm known; this algorithm can work with numbers of 200 digits. Table 6.2 shows a comparison between the algorithms presented in previous sections.

Algorithm	Running-Time	Digits
Trial Division	$O\left(e^{\frac{1}{2}\log(n)}\right)$	1-15
Pollard-ρ	$O\left(e^{\frac{1}{4}\log(n)}\right)$	10-30
ECM	$O\left(e^{\sqrt{\log(n)\log\log(n)}}\right)$	10-70
QS	$O\left(e^{\sqrt{\log(n)\log\log(n)}}\right)$	60-120
NFS	$O\left(e^{\log^{\frac{1}{3}}(n)(\log\log(n))^{\frac{2}{3}}}\right)$	120-200

TABLE 6.2. A comparison between different factorization algorithms.

The first 3 algorithms are suitable to look for small factors, whereas the QS and the NFS find large factors first. The running-time of the QS, as we have seen, depends on the probability that the quantities $Q(u_i)$ are B- smooth, and this probability decreases as $Q(u_i)$ increases. The idea of Pollard (1988) was to work with smaller quantities; in 1993 the NFS succeeds is factoring the ninth Fermat number

$$F_9 = 2424833 \cdot (49 \text{ digits}) \cdot (149 \text{ digits}),$$

and the absolute record (2006) is

$$\frac{6^{353}-1}{6-1} = (120 \text{ digits}) \cdot (155 \text{ digits}) \approx (300 \text{ digits}).$$

Indeed there are two versions of the NFS, namely the *Special Number Field Sieve* (SNFS) and the *Generic Number Field Sieve* (GNFS); the former works with numbers of special form, the latter works with general numbers. The original idea brought the SNFS and mathematicians thought that the algorithm was not efficient for number of general form.

Before describing the algorithm we must deal with *number fields*.

DEFINITION 6.3 (Number Field). A *number field* $\mathbb{F}$ is a finite (algebraic) extension of the field of rational numbers $\mathbb{Q}$. In other words $\mathbb{F} = \mathbb{Q}(\alpha)$ is

such that α is a zero of a monic irreducible polynomial $f(X) \in \mathbb{Q}[X]$; α is a formal symbol and we can write

$$\mathbb{Q}(\alpha) = \mathbb{Q}[X]/(f(X)).$$

□

EXAMPLE 6.10. Let $\mathbb{F} = \mathbb{Q}(i)$, where i is a zero of $f(X) = X^2 + 1$. An element $x \in \mathbb{Q}(i)$ is of the form $x = a + bi$; moreover

$$(a + bi)(c + di) = ac + bci + adi + di^2 = ac + bci + adi - d.$$

On the other hand, $\mathbb{R}$ is not a number field, since it is not numerable. □

Hence the elements of $\mathbb{Q}(\alpha)$ are polynomial expressions in α, with $\mathbb{Q}$-coefficients; let $f(X)$ be

$$f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0,$$

with $a_i \in \mathbb{Q}$ ($i = 0, 1, \cdots, d-1$). Since α is a zero of $f(X)$ we can write

$$f(\alpha) = \alpha^d + a_{d-1}\alpha^{d-1} + \cdots + a_1\alpha + a_0 = 0,$$

hence we can always write a d-th power in $\mathbb{Q}(\alpha)$ in terms of powers of degree at most $d-1$. Thus

$$\mathbb{Q}(\alpha) = \left\{ \sum_{j=0}^{d-1} b_j\alpha^j : \ b_j \in \mathbb{Q} \ \forall \ j = 0, 1, \cdots, d-1 \right\}.$$

Now we check that $\mathbb{Q}(\alpha)$ is a *field*: we should be able to compute summations, differences, multiplications and divisions in $\mathbb{Q}(\alpha)$. Summation is trivial:

$$x_1, x_2 \in \mathbb{Q}(\alpha) \quad \Rightarrow \quad x_1 \pm x_2 \in \mathbb{Q}(\alpha).$$

Also products are trivial to deal with, since you can always decrease the degree of the powers greater than d, using the relation $f(\alpha) = 0$. Consider the division in $\mathbb{Q}(\alpha)$. Let $x \in \mathbb{Q}(\alpha)$, hence

$$x = \sum_{j=0}^{d-1} b_j\alpha^j = g(\alpha),$$

being $g(X) = \sum_{j=0}^{d-1} b_jX^j$ and $b_j \in \mathbb{Q}$. Since $f(\alpha) = 0$ and $f(X)$ is irreducible, it is $\gcd(f(X), g(X)) = 1$ and, if $g(X) \neq 0$, we can use Bézout's identity to write:

$$a(X)f(X) + b(X)g(X) = 1,$$

for some $a(X), b(X) \in \mathbb{Q}(X)$. Evaluating in α yields

$$a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = 1 \quad \Rightarrow \quad b(\alpha)g(\alpha) = 1,$$

and $x = g(\alpha)$ is invertible in $\mathbb{Q}(\alpha)$, with inverse $b(\alpha) \in \mathbb{Q}(\alpha)$. Hence $\mathbb{Q}(\alpha)$ is a field.

EXAMPLE 6.11. Let $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt[3]{2})$, where α is a zero of $f(X) = X^3 - 2$. Hence the elements of $\mathbb{Q}(\alpha)$ are polynomials in α with degree at most $d-1 = 2$:

$$\mathbb{Q}(\sqrt[3]{2}) = \left\{ b_0 + b_1 \sqrt[3]{2} + b_2 (\sqrt[3]{2})^2 : \ b_j \in \mathbb{Q} \right\}.$$

Now we evaluate:

$$\begin{aligned}(1 + \sqrt[3]{2})(2 + (\sqrt[3]{2})^2) &= 2 + (\sqrt[3]{2})^2 + 2\sqrt[3]{2} + (\sqrt[3]{2})^3 = \\ &= 2 + (\sqrt[3]{2})^2 + 2\sqrt[3]{2} + 2 \\ &= 4 + 2\sqrt[3]{2} + (\sqrt[3]{2})^2.\end{aligned}$$

Finally let $x = 1 + \sqrt[3]{2}$, we show how to compute x^{-1}; it is $x = g(\alpha)$, being $g(X) = X + 1$ and we have $\gcd(X+1, X^3-2) = 1$, as it is easy to check. Hence there exists $a(X), b(X) \in \mathbb{Q}[X]$ such that

$$a(X)(X^3 - 2) + b(X)(X + 1) = 1,$$

and we can look for $a(X), b(X)$ using the extended euclidean algorithm (see appendix B). We begin with

$$\begin{aligned}1 \cdot (X^3 - 2) + 0 \cdot (X + 1) &= X^3 - 2 \\ 0 \cdot (X^3 - 2) + 1 \cdot (X + 1) &= X + 1,\end{aligned}$$

and we compute

$$\begin{aligned}\frac{X^3 - 2}{X + 1} &= X^2 - X + 1 - \frac{3}{X + 1} \\ \Rightarrow \quad X^3 - 2 - (X^2 - X + 1)(X + 1) &= -3.\end{aligned}$$

Evaluating the result in α yields

$$\begin{aligned}-(\alpha^2 - \alpha + 1)(\alpha + 1) &= -3 \\ \Rightarrow \quad x^{-1} = \frac{1}{\alpha + 1} &= \frac{1}{3}(\alpha^2 - \alpha + 1) = \frac{1}{3}((\sqrt[3]{2})^2 - \sqrt[3]{2} + 1).\end{aligned}$$

□

At this point the reason why $\mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$ should be clear: this is because $\mathbb{Q}(\alpha)$ is a $\mathbb{Q}$-vector space of dimension equal to the *degree* of $\mathbb{F} = \mathbb{Q}(\alpha)$.

DEFINITION 6.4 (Degree of a Number Field). The degree of the number field $\mathbb{F} = \mathbb{Q}(\alpha)$ is $deg(\mathbb{F}) = dim_{\mathbb{Q}}(\mathbb{F}) = d$. □

Now we extend the concept of *norm*, as to be able to speak about distances and inequalities. Let $\mathbb{F} = \mathbb{Q}(\alpha)$ be a number field and take the map:

$$\begin{aligned}\Theta_x : \ \mathbb{F} &\longrightarrow \mathbb{F} \\ y &\mapsto x \cdot y.\end{aligned}$$

The map Θ_x is $\mathbb{Q}$-linear: if $q \in \mathbb{Q}$ then[7] $(qy)x = q(yx)$. Thus there exists a matrix $\mathcal{M}_x$ of dimension $d \times d$, being $d = deg(\mathbb{F})$, with $\mathbb{Q}$-coefficients, that represents the map Θ_x. Obviously the matrix $\mathcal{M}_x$ is not unique, since it depends on the basis you choose to evaluate it, but there are quantities like the characteristic polynomial of $\mathcal{M}_x$, denoted $h_x(X)$, that does not depend on the choice of the basis.

Definition 6.5. With the notation as introduced above we define the *norm* and the *trace* of an element $x \in \mathbb{F} = \mathbb{Q}(\alpha)$ to be (respectively):

$$N(x) = det(\mathcal{M}_x) \in \mathbb{Q}$$
$$Tr(x) = Tr(\mathcal{M}_x) \in \mathbb{Q}.$$

□

Note that the norm is multiplicative, since Binet's rule[8] holds

$$N(x \cdot y) = N(x)N(y) \quad \forall\, x, y, \in \mathbb{F},$$

whereas the trace is additive, being

$$Tr(x + y) = Tr(x) + Tr(y) \quad \forall\, x, y, \in \mathbb{F}.$$

Example 6.12. Let $\mathbb{F} = \mathbb{Q}(i)$, so that $x \in \mathbb{Q}(i)$ is such that $x = a + bi$. Hence the map Θ is given by

$$\Theta_x : \ \mathbb{Q}(i) \longrightarrow \mathbb{Q}(i)$$
$$y \mapsto x \cdot y.$$

We choose a $\mathbb{Q}$-basis, for example the canonical basis $(1, i)$, and we evaluate its image:

$$1 \mapsto a + bi$$
$$i \mapsto ai - b,$$

so that

$$\mathcal{M}_x = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Therefore, $Tr(x) = 2a$ and $N(x) = a^2 + b^2$ (that is the same norm of $\mathbb{C}$). Finally:

$$h_x(X) = X^2 - 2aX + a^2 + b^2 = X^2 - Tr(x)X + N(x).$$

□

Hence we have seen that $\mathbb{Q}(\alpha)$ is an extension of $\mathbb{Q}$: $\mathbb{Q} \subset \mathbb{F} = \mathbb{Q}(\alpha)$. On the other hand $\mathbb{Q} \supset \mathbb{Z}$ and $\mathbb{Z}$ is just a ring; in a similar fashion there is a *ring of integers* in $\mathbb{Q}(\alpha)$.

---

[7] In other words we can first multiplying by q and then evaluate the image of the result or viceversa, but the final result is the same.

[8] Given two squared matrices $\mathcal{M}_1$ and $\mathcal{M}_2$ the following (Binet's rule) holds:

$$det(\mathcal{M}_1 \cdot \mathcal{M}_2) = det(\mathcal{M}_1) \cdot det(\mathcal{M}_2).$$

DEFINITION 6.6. The *ring of integers* of $\mathbb{F} = \mathbb{Q}(\alpha)$ is

$$\mathcal{O}_{\mathbb{F}} = \{x \in \mathbb{F} : \ x \text{ is a zero of the monic polynomial } g(X) \in \mathbb{Z}[X]\}.$$

An equivalent definition is:

$$\mathcal{O}_{\mathbb{F}} = \{x \in \mathbb{F} : \ h_x(X) \in \mathbb{Z}[X]\}.$$

□

One of the basic result from algebra[**10**] is that $\mathcal{O}_{\mathbb{F}}$ is a ring. We already know that α is a zero of $f(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1X + a_0$ with $a_i \in \mathbb{Q}$; if the elements a_i belong to $\mathbb{Z}$, i. e. $a_i \in \mathbb{Z}$, then also $f(X) \in \mathbb{Z}[X]$, and since $f(X)$ is monic and irreducible we can conclude $\alpha \in \mathcal{O}_{\mathbb{F}}$. But $\mathcal{O}_{\mathbb{F}}$ is a ring: all the summations and products of α, namely the elements of $\mathbb{Z}[\alpha] = \left\{\sum_{j=0}^{d-1} b_j\alpha^j : \ b_j \in \mathbb{Z}\right\}$, are contained in $\mathcal{O}_{\mathbb{F}}$ and we can conclude

$$\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{F}}.$$

Thus the general situation is depicted like:

$$\begin{array}{ccccc} \mathbb{Q} & \subset & \mathbb{F} & = & \mathbb{Q}(\alpha) \\ \cup & & \cup & & \cup \\ \mathbb{Z} & \subset & \mathcal{O}_{\mathbb{F}} & \supsetneq & \mathbb{Z}[\alpha]. \end{array}$$

The point is that, sometimes, it could be $\mathcal{O}_{\mathbb{F}} \neq \mathbb{Z}[\alpha]$.

EXAMPLE 6.13. Let $\mathbb{F} = \mathbb{Q}(\sqrt{5})$, so that $f(X) = X^2 - 5 \in \mathbb{Z}[X]$. Hence $\alpha = \sqrt{5} \in O_{\mathbb{F}}$ and $O_{\mathbb{F}} \supsetneq \mathbb{Z}[\sqrt{5}]$. □

EXAMPLE 6.14. As an example we show that $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$ if $\mathbb{F} = \mathbb{Q}(\alpha) = \mathbb{Q}(i)$. Clearly we have $\mathbb{Z}[i] \subset \mathcal{O}_{\mathbb{F}}$, so that it suffices to show that $\mathbb{Z}[i] \supset \mathcal{O}_{\mathbb{F}}$; hence let $x \in \mathcal{O}_{\mathbb{F}}$, we must show that $x \in \mathbb{Z}[i]$. Since $\mathbb{Q}(i) \supset \mathcal{O}_{\mathbb{F}}$ we have $x = a + bi \in \mathbb{Q}(i)$ with $a, b \in \mathbb{Q}$. Thus it suffices to show that $a, b \in \mathbb{Z}$. Consider the characteristic polynomial of the map Θ_x, namely

$$h_x(X) = X^2 - 2aX + (a^2 + b^2).$$

By definition of $\mathcal{O}_{\mathbb{F}}$ we know that $x \in \mathcal{O}_{\mathbb{F}}$ if and only if $h_x(X) \in \mathbb{Z}[X]$ which yields

$$2a \in \mathbb{Z} \qquad a^2 + b^2 \in \mathbb{Z}.$$

Hence there are only two possibilities for a: either $a \in \frac{1}{2}\mathbb{Z}$, i. e. a is of the form $a = \frac{1}{2} + m$ with $m \in \mathbb{Z}$, or $a \in \mathbb{Z}$. If $a \in \mathbb{Z}$, since $a^2 + b^2 \in \mathbb{Z}$ we have $b^2 \in \mathbb{Z}$ too, and by Gauss' lemma $b \in \mathbb{Z}$ and the assertion is proven. On the other hand, let us suppose that $a \in \frac{1}{2}\mathbb{Z}$, we can write

$$\begin{aligned} & a^2 + b^2 = \left(\frac{1}{2} + m\right)^2 + b^2 \in \mathbb{Z} \\ \Rightarrow \quad & (1 + 2m)^2 + (2b)^2 \in 4\mathbb{Z} \\ \Rightarrow \quad & (2b)^2 \in \mathbb{Z}, \end{aligned}$$

and Gauss' lemma yields $2b \in \mathbb{Z}$. Hence if $P = 1 + 2m$ and $Q = 2b$ it should be

$$P^2 + Q^2 \equiv 0 \pmod 4 \quad P, Q \in \mathbb{Z}.$$

Quadratic residues modulo 4 are only 0 or 1, so that $P, Q \equiv 0, 1 \pmod 4$, but P is odd, i. e. $P \equiv 1 \pmod 4$ and it should be

$$1 + Q^2 \equiv 0 \pmod 4 \quad Q \in \mathbb{Z},$$

that is impossible. Hence the only possibility is $a \in \mathbb{Z} \Rightarrow b \in \mathbb{Z} \Rightarrow \mathbb{Z}[i] = \mathscr{O}_{\mathbb{F}}$. □

Now we want to better understand the arithmetic of $\mathbb{Z}[\alpha]$; in $\mathbb{Z}$ there are prime numbers, such that every element of $\mathbb{Z}$ is expressible, in a unique way, as a product of prime numbers. We have an analogous in $\mathbb{Z}[\alpha]$ if we replace prime numbers by *prime ideals* (see definition 4.1). Recall that, if R is a ring, an ideal $\mathcal{I}$ of R is an additive subgroup of R that is stable under multiplication by elements of R:

$$\forall\, \lambda \in R\,,\ x \in \mathcal{I} \quad \Rightarrow \quad \lambda x \in \mathcal{I}.$$

Let $y \in R$, we denote with (y) the ideal[9] generated by y, i. e.

$$(y) = \{\mu y : \mu \in R\}.$$

Now we extend the operations of multiplication and division for ideals. Let $\mathcal{I}, \mathcal{J}$ be two ideals of a ring R. We denote the product $\mathcal{I} \cdot \mathcal{J}$ as

$$\mathcal{K} = \mathcal{I} \cdot \mathcal{J} = \left\{ \sum_i x_i y_i : \ \forall\, x_i \in \mathcal{I}, y_i \in \mathcal{J} \right\}.$$

First of all it is easy to see that $\mathcal{K}$ is an ideal. Further note that it suffices to consider $\mathcal{K}$ to be the ideal generated by all the products between the elements that generate $\mathcal{I}$ and $\mathcal{J}$ (and not by all the elements of the two ideals). Hence this product extends the product of integers, since

$$\mathcal{I} = (x), \mathcal{J} = (y) \quad \Rightarrow \quad \mathcal{K} = (xy).$$

On the other hand we say that the ideal $\mathcal{I}$ divides the ideal $\mathcal{J}$ if and only if $\mathcal{I} \supset \mathcal{J}$. Note that if $x, y \in \mathbb{Z}$ are such that $x|y$, then $y = ux$; hence it is easily verified that $(x)|(y)$ since $(x) = \{\sigma x : \ \sigma \in R\}$ and $(y) = \{\lambda y : \ \lambda \in R\} = \{(\lambda u)x : \ \lambda \in R\} \subset (x)$.

---

[9] It is straightforward to verify that (y) is indeed an ideal. In fact if $y_1, y_2 \in (y)$ we can write

$$y_1 = \mu_1 y \quad y_2 = \mu_2 y \quad y_1 + y_2 = (\mu_1 + \mu_2) y \in (y),$$

since $(\mu_1 + \mu_2) \in R$. Further, $\forall\, \lambda \in R$ and $x \in (y)$ it is

$$\lambda x = \lambda(\mu y) = (\lambda \mu) y \in (y).$$

We know that in $\mathbb{Z}$, we can factor every element n as a product of prime numbers in a unique way:

$$n = \prod_{\text{primes } p<n} p^{e(p)}.$$

The reason is that $\mathbb{Z}$ is a *Unique Factorization Domain* (UFD); this fact is not granted.

EXAMPLE 6.15. Let $\alpha = \sqrt{-5}$, $f(X) = X^2 + 5$ and $R = \mathbb{Z}[\sqrt{-5}]$. We can write

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. □

The situation in the previous example is saved thanks to the concept of *prime ideal*. The following theorem is central in *algebraic number theory*[**21, 30**]:

THEOREM 6.5. *If $\mathbb{F} = \mathbb{Q}(\alpha)$ is a finite extension of $\mathbb{Q}$, then the ring $\mathcal{O}_{\mathbb{F}}$ of the integers of $\mathbb{F}$ admits unique factorization of ideals in prime ideals, i.e. it is a UFD.* □

Hence if $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$, we can conclude that $\mathbb{Z}[\alpha]$ is a UFD replacing the concept of prime numbers with the concept of prime ideals. If this is not the case, i. e. $\mathbb{Z}[\alpha] \neq \mathcal{O}_{\mathbb{F}}$ there are some further difficulties (all solvable[**21, 30**]).

EXAMPLE 6.16. Consider the previous example in $\mathbb{Z}[\sqrt{-5}]$, where:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Let $\mathfrak{p}_1 = (2, 1 + \sqrt{-5})$; it is easy to check that $\mathfrak{p}_1^2 = \mathfrak{p}_1 \cdot \mathfrak{p}_1 = (2)$. In fact on one hand, clearly, $(2) \subset \mathfrak{p}_1^2$ and on the other hand

$$\begin{aligned} \mathfrak{p}_1 \cdot \mathfrak{p}_1 &= (2 \cdot 2, 2(1 + \sqrt{-5}), (1 + \sqrt{-5})^2) = \\ &= (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) \\ \Rightarrow \quad (2) \supset \mathfrak{p}_1^2 \quad &\Rightarrow \quad \mathfrak{p}_1^2 = (2). \end{aligned}$$

Moreover $\mathfrak{p}_1$ is a prime ideal since

$$\begin{aligned} \mathbb{Z}[\sqrt{-5}]/\mathfrak{p}_1 = \mathbb{Z}[\sqrt{-5}]/(2, 1 + X) &\simeq \mathbb{Z}[X]/(X^2 + 5, 2, 1 + X) \\ &\simeq \mathbb{Z}_2[X]/(X^2 + 1, X + 1) \simeq \mathbb{Z}_2, \end{aligned}$$

and $\mathbb{Z}_2$ is a field (and hence an integral domain). In a similar fashion it is easy to check that

$$(3) = \mathfrak{p}_2 \cdot \mathfrak{p}_3 \qquad \text{being } \mathfrak{p}_2 = (3, 1 + \sqrt{-5}) \text{ and } \mathfrak{p}_3 = (3, 1 - \sqrt{-5}),$$

and (3) is a prime ideal. Finally the ideal generated by 6 is expressible as a product of prime ideals in a unique way:

$$(6) = (2) \cdot (3) = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3.$$

□

We will need the following lemma:

Lemma 6.6. *Every prime ideal* $\mathfrak{p}$ *of* $\mathbb{Z}[\alpha]$ *contains at least one prime number* p.

Proof. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[\alpha]$ and let $\gamma \in \mathfrak{p}$ be a non-zero element of $\mathfrak{p}$. We consider the $\mathbb{Z}$-linear map:

$$\begin{aligned} \Theta_\gamma : \ \mathbb{Z}[\alpha] &\longrightarrow \mathbb{Z}[\alpha] \\ x &\mapsto x \cdot \gamma. \end{aligned}$$

Since $\mathbb{Z}[\alpha]$ admits a $\mathbb{Z}$-basis, the matrix $\mathcal{M}_\gamma$ (of dimension $d \times d$)) representing the map Θ_γ with respect to some basis of $\mathbb{Z}[\alpha]$ has integer coefficients. Further it is easy to check that γ is an eigenvalue; hence, denoted with $h_\gamma(X) = X^d + a_{d-1}X^{d-1} + \cdots + a_1 X + a_0$ the characteristic polynomial of $\mathcal{M}_\gamma$ we can write

$$h_\gamma(\gamma) = \gamma^d + a_{d-1}\gamma^{d-1} + \cdots + a_1\gamma + a_0 = 0,$$

so that $h_\gamma(\gamma) \in \mathfrak{p}$. But this is possible if and only if $a_0 = \prod_i p_i \in \mathfrak{p}$ (with p_i primes); thus every prime ideal $\mathfrak{p}$ of $\mathbb{Z}[\alpha]$ divides the ideal (p) for some prime $p \in \mathbb{Z}$ and as a consequence $\mathfrak{p} \supset (p)$ and $p \in \mathfrak{p}$. □

There is a very important class of prime ideals, namely the *prime ideals of degree one*. Let $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$, being $\mathbb{F} = \mathbb{Q}(\alpha)$ with α such that $f(\alpha) = 0$ and $f(X) \in \mathbb{Z}[X]$, monic and irreducible. Let p be a prime and we consider the reduction of $f(X)$ modulo p, i. e. $f(X) \bmod p$, that *could* be not irreducible. Let us suppose that there is a zero $r \in \mathbb{Z}$, such that $f(r) \equiv 0 \pmod{p}$. The ideal $\mathfrak{p} = (p, \alpha - r)$ is a prime ideal of $\mathcal{O}_{\mathbb{F}} = \mathbb{Z}[\alpha]$, being

$$\begin{aligned} \mathbb{Z}[\alpha]/\mathfrak{p} = \mathbb{Z}[\alpha]/(p, \alpha - r) &\simeq \mathbb{Z}[X]/(f(X), p, X - r) \\ &\simeq \mathbb{Z}_p[X]/(f(X), X - r) \simeq \mathbb{Z}_p[X]/(f(r)) \simeq \mathbb{Z}_p, \end{aligned}$$

since $f(r) \equiv 0 \pmod{p}$. The ideal $\mathfrak{p}$ is called prime ideal of degree one because $\mathbb{Z}[\alpha]/\mathfrak{p}$ is isomorphic to $\mathbb{Z}_p$ and $\#\mathbb{Z}_p = p^1$.

Hence, to sum up what we have learned in this introduction, the ring $\mathbb{Z}$ is a UFD and it admits unique factorization in prime numbers; on the other hand we have seen that, if $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{F}}$, $\mathbb{Z}[\alpha]$ admits unique factorization in prime ideals (of degree one and not).

Now we are ready to discuss the NFS. The key idea is the same of the QS, whose efficiency depends on the probability that the quantities $Q(u_i) \approx \sqrt{n}$ are B-smooth. Let n be the integer to factor (we can always consider n odd without loss of generality) and let $\mathbb{F} = \mathbb{Q}(\alpha)$ with $\deg(\mathbb{F}) = d > 0$ (typically d is between 3 and 10). We choose a polynomial $f(X) \in \mathbb{Z}[X]$, monic and irreducible, of degree d, such that

$$f(m) \equiv 0 \pmod{n},$$

being $m \propto \left[n^{\frac{1}{d}}\right]$. Let us show how to build-up such a polynomial; it suffices to write the expansion of n in base m, i. e. $n = [1\ c_{d-1}\ \cdots\ c_1\ c_0]_m$, so that:

$$n = m^d + c_{d-1}m^{d-1} + \cdots c_1 m + c_0,$$

with $0 \leq c_i < m$. If we choose $f(X)$ to be

$$f(X) = X^d + c_{d-1}X^{d-1} + \cdots + c_1 X + c_0,$$

it is straightforward to verify that $f(m) = n \equiv 0 \pmod{n}$. In practice, since $n \gg d$, $f(X)$ is monic; further we can assume that $f(X)$ is irreducible as well, since, if this is not the case, we have found a non-trivial factor of n.

Example 6.17. To factor the ninth Fermat's number $F_9 = 2^{2^9}+1 = 2^{512}+1$, the choices were $d = 5$, $f(X) = X^5 + 8$ and $m = 2^{103}$. In fact

$$f(m) = (2^{103})^5 + 8 = 2^{515} + 8 = 8F_9 \equiv 0 \pmod{F_9}.$$

□

The sieving part of the NFS use two sieves: the first lives in the ring of integers $\mathbb{Z}$ and the second in $\mathbb{Z}[\alpha]$; in the following we suppose that $\mathbb{Z}[\alpha] = \mathscr{O}_{\mathbb{F}}$. The algorithm starts filling an array with the elements $a - bm \in \mathbb{Z}$ and $a - b\alpha \in \mathbb{Z}[\alpha]$, for the values $a, b \in [-L, L]$ varying in an interval of $\mathbb{Z}$ with $2L$ elements. Then we choose a smoothness bound B and a factor base

$$\mathcal{B} = \left\{\text{primes } p_j :\ p_j < B \text{ with } j = 1, 2, \cdots, \pi(B)\right\}.$$

Denote with $p \in \mathcal{B}$ the generic element of $\mathcal{B}$. Let us start dealing with $\mathbb{Z}$; here we look for elements $a - bm$ that are B-smooth. Note that if $p|(a - bm)$ we have $a \equiv bm \pmod{p}$ and, if b is invertible modulo p, $\frac{a}{b} \equiv m \pmod{p}$. Thus, for a fixed value of b, if $p|(a - bm)$, we can conclude that $p|(a' - bm)$, for each a' such that $a' \equiv a \pmod{p}$; hence we can sieve and look for B-smooth numbers among the values $a - bm$ of our array.

Let us now consider $\mathbb{Z}[\alpha]$. The first observation we make is that the ideal generated by the element $a - b\alpha$ is just divisible by prime ideals of degree one.

Lemma 6.7. *The ideal $(a - b\alpha)$ is just divisible by prime ideals $\mathfrak{p}$ of degree one.*

Proof. Let us suppose that the prime ideal $\mathfrak{p}$ divides $(a - b\alpha)$ (hence $a - b\alpha \in \mathfrak{p}$); we show that $\mathfrak{p}$ must be of the form $\mathfrak{p} = (p, \alpha - r)$, i. e. it is a prime ideal of degree one. Since $a - b\alpha \in \mathfrak{p}$ we can write (using also lemma 6.6)

$$\begin{aligned}\mathbb{Z}[\alpha]/\mathfrak{p} &\simeq \mathbb{Z}[X]/(f(X), a - bX, p) \simeq \mathbb{Z}_p[X]/(f(X), a - bX)\\ &\simeq \mathbb{Z}_p/(f(a/b)).\end{aligned}$$

Since $\mathfrak{p}$ is a prime ideal, we can conclude $f\left(\frac{a}{b}\right) \equiv 0 \pmod{p}$ so that $\mathbb{Z}[\alpha]/\mathfrak{p} \simeq \mathbb{Z}_p$; hence

$$f\left(\tfrac{a}{b}\right) \equiv 0 \pmod{p} \Rightarrow f(r) \equiv 0 \pmod{p} \Rightarrow \mathfrak{p} = (p, \alpha - r),$$

being $r \in \mathbb{Z}$ such that $r \equiv \frac{a}{b} \pmod{p}$. □

Note that we have periodicity; if $\mathfrak{p}|(a - b\alpha)$ we know that $(a - b\alpha) \subset \mathfrak{p}$ which implies $a - b\alpha \in \mathfrak{p} = (p, \alpha - r)$, that is to say:

$$\begin{aligned} & (a - b\alpha) \bmod (\alpha - r) \equiv 0 \pmod{p} \\ \Rightarrow \quad & a - br \equiv 0 \pmod{p} \\ \Rightarrow \quad & \mathfrak{p}|(a - b\alpha) \quad \Leftrightarrow \quad p|(a - br). \end{aligned}$$

Fixed $\mathfrak{p} = (p, \alpha - r)$, the values p and r are fixed and we can conclude that $\mathfrak{p}|(a - b\alpha)$ for all the values $a - br \equiv 0 \pmod{p}$. In general the number of prime divisors $\mathfrak{p}$ of degree one for the element $(a - b\alpha)$ is μ, with $0 \leq \mu \leq d$; but one can show that the mean value is 1.

Example 6.18. Consider the number ring $\mathbb{Z}[\alpha] = \mathbb{Z}[i]$; since $(1 + i)^2 = (2)$ in $\mathbb{Z}[i]$, we can write $(1+i) = (1+i, 2)$. One can show that if $p \equiv 3 \pmod{4}$, the ideal (p) is prime in $\mathbb{Z}[i]$, with degree greater than 1; in fact $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_{p^2}$, since $a, b \in \mathbb{Z}_p$. On the other hand, if $p \equiv 1 \pmod{4}$ one can show that $(p) = \mathfrak{p}_1 \cdot \mathfrak{p}_2$. But half the values of $\mathbb{Z}_p$ is congruent to 1 and the other half is congruent to 3 modulo 4, so that, on average, every element $(a + bi)$ generated by $a + bi \in \mathbb{Z}[\alpha]$ is divisible by one prime ideal of degree one. □

As a consequence:

$$\#\{\text{Prime ideals } \mathfrak{p} = (p, r - \alpha) \text{ of degree one} : \ p \leq B\} \approx \#\{p : \ p \leq B\}. \tag{6.4}$$

Hence, for each $p \in \mathcal{B}$, we can sieve for the prime ideal $\mathfrak{p} = (p, \alpha - r)$ in our array with values $(a - b\alpha)$ and look for B-smooth elements. We need to generalize the concept of smoothness for number rings.

Lemma 6.8. *Let $a, b \in \mathbb{Z}$, then*

$$N(a - b\alpha) = b^d f\left(\frac{a}{b}\right) = a^d + c_{d-1}a^{d-1}b + \cdots + c_1 ab^{d-1} + c_0 b^d.$$

Proof. We divide $a - b\alpha$ by b, writing

$$a - b\alpha = b\left(\frac{a}{b} - \alpha\right),$$

and using the multiplicative property of the norm

$$N(a - b\alpha) = N(b) \cdot N\left(\frac{a}{b} - \alpha\right),$$

To evaluate $N(b)$ we consider the map:

$$\begin{aligned} \Theta_b : \ \mathbb{Q}(\alpha) &\longrightarrow \mathbb{Q}(\alpha) \\ x &\mapsto b \cdot x. \end{aligned}$$

It is straightforward to evaluate the matrix $\mathcal{M}_b$ of Θ_b with respect to the canonical basis of $\mathbb{Q}(\alpha)$; it is a $d \times d$ matrix of the form

$$\mathcal{M}_b = \begin{pmatrix} b & 0 & \dots & 0 \\ 0 & b & \ddots & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & b \end{pmatrix},$$

hence $N(b) = b^d$. It remains to show that $N(q-\alpha) = f(q)$ for each element $q \in \mathbb{Q}$. First of all note that $\mathbb{Q}(\alpha) = \mathbb{Q}(q-\alpha)$ and fix the basis

$$\left(1, q-\alpha, (q-\alpha)^2, \cdots, (q-\alpha)^{d-1}\right).$$

We want to evaluate (with respect to the above basis) the matrix $\mathcal{M}_{q-\alpha}$ of the map

$$\begin{aligned} \Theta_{q-\alpha} : \ \mathbb{Q}(\alpha) &\longrightarrow \mathbb{Q}(\alpha) \\ x &\mapsto (q-\alpha) \cdot x. \end{aligned}$$

Since we have

$$\begin{gathered} 1 \mapsto (q-\alpha) \\ q-\alpha \mapsto (q-\alpha)^2 \\ \dots \\ \dots \\ (q-\alpha)^{d-1} \mapsto (q-\alpha)^d, \end{gathered}$$

the matrix $\mathcal{M}_{q-\alpha}$ (of dimension $d \times d$) is of the form

$$\mathcal{M}_{q-\alpha} = \begin{pmatrix} 0 & \dots & \dots & \dots & * \\ 1 & 0 & \dots & \dots & ?? \\ 0 & \ddots & \ddots & \dots & ?? \\ \vdots & 0 & \ddots & \ddots & ?? \\ 0 & 0 & \dots & 1 & ?? \end{pmatrix},$$

where the last column depends on the image $(q-\alpha)^d$ of $(q-\alpha)^{d-1}$. To evaluate the determinant, we just need to evaluate the first element, denoted with $*$, of this column. By definition of $\mathbb{Q}(\alpha)$ we have $f(\alpha) = 0$, hence

$$\begin{aligned} f(\alpha) = f(q-(q-\alpha)) &= \sum_{j=0}^{d} c_j \left(q-(q-\alpha)\right)^j = \\ &= (-1)^d (q-\alpha)^d + \left(\begin{smallmatrix}\text{lower} \\ \text{powers}\end{smallmatrix}\right) + \sum_{j=0}^{d} c_j q^j = \\ &= (-1)^d (q-\alpha)^d + \left(\begin{smallmatrix}\text{lower} \\ \text{powers}\end{smallmatrix}\right) + f(q) \stackrel{!}{=} 0, \end{aligned}$$

and we can conclude

$$(q-\alpha)^d = (-1)^d f(q) + \left(\begin{smallmatrix}\text{lower}\\ \text{powers}\end{smallmatrix}\right).$$

This yields

$$\mathcal{M}_{q-\alpha} = \begin{pmatrix} 0 & \dots & \dots & \dots & (-1)^d f(q) \\ 1 & 0 & \dots & \dots & ?? \\ 0 & \ddots & \ddots & \dots & ?? \\ \vdots & 0 & \ddots & \ddots & ?? \\ 0 & 0 & \dots & 1 & ?? \end{pmatrix},$$

so that $N(q-\alpha) = (-1)^d \cdot (-1)^d f(q) = f(q)$ and the assertion is proven. □

The following result is crucial:

Proposition 6.9. *If (and only if)* $\mathfrak{p} = (p, \alpha - r)$ *divides* $(a - b\alpha)$*, then* $p | N(a - b\alpha)$*.*

Proof. We show only one direction, the other is similar. Let us suppose that $\mathfrak{p} | (a - b\alpha)$, we can write

$$\begin{aligned} & a - b\alpha \equiv 0 \quad \text{in } \mathbb{Z}[\alpha]/(p, \alpha - r) \\ \Rightarrow \quad & \alpha \equiv r \quad \text{in } \mathbb{Z}[\alpha]/(p, \alpha - r) \\ \Rightarrow \quad & a - br \equiv 0 \quad \text{in } \mathbb{Z}[\alpha]/(p, \alpha - r) \\ \Rightarrow \quad & r \equiv \frac{a}{b} \quad \text{in } \mathbb{Z}[\alpha]/(p, \alpha - r). \end{aligned}$$

But, since $\mathfrak{p}$ has degree one, we have $f(r) \equiv 0 \pmod{p}$, so that

$$N(a - b\alpha) = b^d f\left(\frac{a}{b}\right) \equiv b^d f(r) \equiv 0 \pmod{p}.$$

□

Hence divisibility in $\mathbb{Z}[\alpha]$ implies divisibility in $\mathbb{Z}$ (and viceversa). As a consequence, putting equation (6.4) and proposition 6.9 together yields the following important result:

Corollary 6.10. *An element* $a - b\alpha \in \mathbb{Z}[\alpha]$ *is B-smooth if* $N(a - b\alpha)$ *is B-smooth.* □

Consider now the ring homomorphism given by:

$$\begin{aligned} \phi : \ \mathbb{Z}[\alpha] &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ \alpha &\mapsto m. \end{aligned}$$

This is an homomorphism since α is a formal zero of $f(X)$ and we forced $f(m) \equiv 0 \pmod{n}$. We can thus write

$$a - bm = \phi(a - b\alpha) \quad \text{in } \mathbb{Z}/n\mathbb{Z}.$$

After sieving for B-smooth elements we have obtained a certain number, denoted with M, of relations

$$a_i - b_i m = \prod_{j=1}^{N} p_j^{\epsilon_{ji}}$$
$$(a_i - b_i\alpha) = \prod_{j=1}^{N} \mathfrak{p}_j^{\delta_{ji}} = \prod_{j=1}^{N} (p_j, \alpha - r_j)^{\delta_{ji}},$$

with $N = \pi(B)$, $a_i, b_i \in [-L, L]$ $(i = 1, 2, \cdots, M)$ and being ϵ_{ji} (δ_{ji}) the exponent of the prime (prime ideal) p_j $(\mathfrak{p}_j)$ in the *unique* factorization of the integer $a_i - b_i m$ (the ideal $(a_i - b_i\alpha)$). Since $a_i - b_i m \equiv \phi(a_i - b_i\alpha)$ in $\mathbb{Z}/n\mathbb{Z}$ we can look for an opportunistic combination of the above relations, exactly like in the QS algorithm, i. e. vectors $(e_1, \cdots, e_M)$ such that

$$u^2 = \prod_{i=1}^{M} (a_i - b_i m)^{e_i} = \left(\prod_{j=1}^{N} p_j^{\frac{1}{2}\sum_{i=1}^{M} e_i \epsilon_{ji}} \right)^2 =$$
$$= \prod_{i=1}^{M} (a_i - b_i\alpha)^{e_i} = \left(\prod_{j=1}^{N} (p_j, \alpha - r_j)^{\frac{1}{2}\sum_{i=1}^{M} e_i \delta_{ji}} \right)^2 = \mathcal{V}^2,$$

in $\mathbb{Z}/n\mathbb{Z}$. Note that the second member is the square of an ideal; there are some difficulties that we do not explain in details[**49**]:

(1) It could be $\mathbb{Z}[\alpha] \neq \mathcal{O}_{\mathbb{F}}$, so that we do not have unique factorization in prime ideals.
(2) Even if $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{F}}$, the ideal $\mathcal{V}^2$ could not be principal.
(3) Even if $\mathbb{Z}[\alpha] = \mathcal{O}_{\mathbb{F}}$ and $\mathcal{V}^2 = (\gamma)$ is principal, we cannot conclude immediately $v^2 = \gamma$.

We close this section giving an estimate for the running-time of the algorithm. The sieving part of the algorithm terminates when we find approximately $M > B$ B-smooth elements of the form $a - bm$ and $a - b\alpha$, i. e. when the product

$$(a - bm)N(a - b\alpha)$$

is B-smooth (recall that $a - b\alpha$ is B-smooth when its norm is B-smooth). Hence we estimate the order of magnitude of

$$N(a - b\alpha) = a^d + c_{d-1}a^{d-1}b + \cdots + c_1 ab^{d-1} + c_0 b^d,$$

where $|c_i| \approx n^{\frac{1}{d}}$ and $a, b \in [-L, L]$ (hence $|a|, |b| \leq L$). Since the above equation sees $d + 1$ elements of size $\approx n^{\frac{1}{d}}$ and a, b are at most L with exponent less than or equal to d, we have:

$$|N(a - b\alpha)| \leq (d - 1)n^{\frac{1}{d}}L^d.$$

On the other hand the size of $a - bm$ is roughly $Ln^{\frac{1}{d}}$ and we can write

$$|(a - bm)N(a - b\alpha)| \leq Ln^{\frac{1}{d}}(d-1)n^{\frac{1}{d}}L^d \approx L^{d+1}n^{\frac{2}{d}} \approx$$
$$\approx L^d n^{\frac{2}{d}}.$$

Note that the larger the size of the product $(a - bm)N(a - b\alpha)$, the smaller the probability that the product $(a - bm)N(a - b\alpha)$ is B-smooth; hence it makes sense to look for the optimal value of d that minimize the size $L^d n^{\frac{2}{d}}$ (see figure 6.6). With this in mind we evaluate

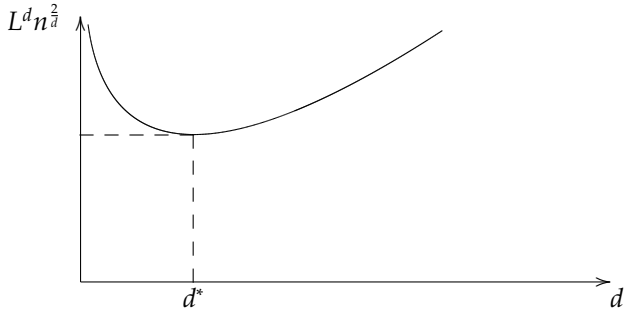


FIGURE 6.6. Size $L^d n^{\frac{2}{d}}$ of the product $(a - bm)N(a - b\alpha)$ as a function of d.

$$\frac{\partial}{\partial d}\left(d\log(L) + \frac{2}{d}\log(n)\right) = 0$$
$$\Rightarrow \quad \log(L) = \frac{2}{d^2}\log(n)$$
$$\Rightarrow \quad d^* = \sqrt{\frac{2\log(n)}{\log(L)}}.$$

For this value the number of digits of the product $(a - bm)N(a - b\alpha)$ is

$$\log\left(L^{d^*}n^{\frac{2}{d^*}}\right) = d^*\log(L) + \frac{2}{d^*}\log(n) = 2\sqrt{2\log(n)\log(L)}.$$

On the other hand, for what concerns the sieving part of the algorithm, the work load is (for each sieve):

$$\sum_{p<B}\frac{1}{p}L^2 = L^2\sum_{p<B}\frac{1}{p} \approx O\left(\log\log(B)L^2\right) = O(L^2),$$

using the approximation of equation (6.3). One can show that here[**49**], unlike in the QS algorithm, the sieving part of the algorithm is faster than the linear algebra part (at least $O(B^2)$), and the optimal choice is hence to set

$$L \approx B.$$

Now it remains to fix B. We need roughly B-smooth elements among the elements of our array, and, as we have seen, the size of these elements is

$$L^{d^*} n^{\frac{2}{d^*}} = e^{\log\left(L^{d^*} n^{\frac{2}{d^*}}\right)} = e^{2\sqrt{2\log(n)\log(L)}}.$$

Hence we set a value $u \in \mathbb{R}_{>1}$ such that

$$B = e^{\frac{2}{u}\sqrt{2\log(n)\log(L)}} = e^{\frac{2}{u}\sqrt{2\log(n)\log(B)}},$$

and, by theorem 6.1, we can estimate the probability that a value in our array is B-smooth with u^{-u}. Since we have L^2 elements and we need roughly B B-smooth values we require $B = \dfrac{L^2}{u^u}$. Manipulating

$$\begin{aligned}
& \log(B) = -u\log(u) + 2\log(L) = -u\log(u) + 2\log(B) \\
\Rightarrow\quad & u\log(u) = \log(B) \\
\Rightarrow\quad & \text{[by lemma 6.2]} \\
\Rightarrow\quad & u \approx \frac{\log(B)}{\log\log(B)}.
\end{aligned}$$

Hence

$$\begin{aligned}
& \log(B) = \frac{2}{u}\sqrt{2\log(n)\log(B)} = \frac{2\log\log(B)}{\log(B)}\sqrt{2\log(n)\log(B)} \\
\Rightarrow\quad & \frac{\log^{\frac{3}{2}}(B)}{\log\log(B)} = 2\sqrt{2\log(n)} \\
\Rightarrow\quad & \frac{\log^{\frac{3}{2}}(B)}{\log(\log^{\frac{3}{2}}(B))} = \frac{2}{3}\cdot 2\sqrt{2\log(n)} \\
\Rightarrow\quad & \log^{\frac{3}{2}}(B) \approx \frac{4}{3}\sqrt{2\log(n)}\log\left(\frac{4}{3}\sqrt{2\log(n)}\right),
\end{aligned}$$

and an approximation of the second member yields

$$\begin{aligned}
\frac{4}{3}\sqrt{2\log(n)}\left(\log\left(\frac{4}{3}\sqrt{2}\right) + \frac{1}{2}\log\log(n)\right) &\approx \frac{4}{3}\sqrt{2\log(n)}\left(\frac{1}{2}\log\log(n)\right) \\
&= \frac{2}{3}\sqrt{2}\sqrt{\log(n)}\log\log(n),
\end{aligned}$$

which implies

$$\log(B) \approx \left(\frac{2\sqrt{2}}{3}\right)^{\frac{2}{3}} \log^{\frac{1}{3}}(n)\left(\log\log(n)\right)^{\frac{2}{3}}.$$

Since the running-time is $O(B^2)$, we can conclude

$$\text{Running-Time:} \Rightarrow \quad O\left(e^{2\left(\frac{8}{9}\right)^{\frac{1}{3}}\log^{\frac{1}{3}}(n)\left(\log\log(n)\right)^{\frac{2}{3}}}\right),$$

which is better than the QS algorithm. Using the optimal value of B, the size of the elements in the array is:

$$2\sqrt{2\log(n)\log(L)} = 2\sqrt{2\log(n)\log(B)} \propto \log^{\frac{2}{3}}(n)\left(\log\log(n)\right)^{\frac{1}{3}}.$$

Note that in the QS algorithm the elements $Q(u_i)$ are of size $\approx \frac{1}{2}\log(n)$, whereas $\log^{\frac{2}{3}}(n) \ll \frac{1}{2}\log(n)$. Finally

$$d \propto \left(\frac{\log(n)}{\log\log(n)}\right)^{\frac{1}{3}},$$

and typically $n \approx 10^{200} \Rightarrow d \approx 5,6$.

CHAPTER 7

Discrete Logarithm

Contents

7.1. Introductory Elements

Let p be a prime number, then $\mathbb{Z}_p^*$ is cyclic (as we will show in theorem 7.3) and we call a *primitive root* (or a *generator*) an element $g \in \mathbb{Z}_p^*$ such that $ord(g \bmod p) = p-1$. As a consequence, for each element $x \in \mathbb{Z}_p^*$ there exists an integer $m \in \mathbb{Z}$ such that $x = g^m$.

Definition 7.1. With the notation as introduced above we say that m is the discrete logarithm of x with respect to the basis g: $m = \log_g(x)$. □

Thanks to Fermat's little theorem, we can always add multiples of $p-1$ at the exponent, i. e.

$$x = g^m \equiv g^{m+k(p-1)} \pmod{p} \qquad k \in \mathbb{Z}.$$

Hence m is an element of $\mathbb{Z}_{p-1}$:

$$m = \log_g(x) \in \mathbb{Z}_{p-1}.$$

The discrete logarithm satisfies the same properties of the natural logarithm; indeed there is a group isomorphism:

$$\mathbb{R}^*_{>0} \underset{e^{(\cdot)}}{\overset{\log(\cdot)}{\rightleftarrows}} \mathbb{R} \qquad \mathbb{Z}_p^* \underset{g^{(\cdot)}}{\overset{\log_g(\cdot)}{\rightleftarrows}} \mathbb{Z}_{p-1}.$$

In particular if $x = g^{m_1}$ and $y = g^{m_2}$, we have $x \cdot y = g^{m_1+m_2}$ and

$$\log_g(x \cdot y) = \log_g(x) + \log_g(y).$$

Further let $h \neq g$ be another primitive root; hence $h = g^a$ and $g = h^b$ for some $a, b \in \mathbb{Z}_{p-1}$ and

$$g = g^1 = h^b = g^{ab} \quad \Rightarrow \quad a \cdot b \equiv 1 \pmod{p-1}.$$

Moreover, if $x = g^m = h^{mb}$, we can conclude

$$\log_h(x) = mb = b\log_g(x) \quad \Rightarrow \quad \frac{\log_h(x)}{\log_g(x)} = b \in \mathbb{Z}_{p-1}^*,$$

that is to say, we can change the basis of the logarithm from g to h just multiplying for a constant b that only depends on g and h. Note that if g is a primitive root of $\mathbb{Z}_p^*$, then $\log_g(-1) = \frac{p-1}{2}$, since g is a quadratic non-residue modulo p.

EXAMPLE 7.1. Let $p = 7$; one can show that $3, 5 \in \mathbb{Z}_7^*$ are primitive roots:

$$\begin{aligned}\mathbb{Z}_7^* &= \left\{\overline{3} = 3^1, \overline{2} = 3^2, \overline{6} = 3^3, \overline{4} = 3^4, \overline{5} = 3^5, \overline{1} = 3^6\right\} \\ &= \left\{\overline{5} = 5^1, \overline{4} = 5^2, \overline{6} = 5^3, \overline{3} = 5^4, \overline{2} = 5^5, \overline{1} = 5^6\right\}.\end{aligned}$$

Hence $\log_3(2) = 2$, $\log_3(3) = 1$ and $\log_3(6) = 2 + 1 = 3$. □

The discrete logarithm is suitable for cryptographic purposes since it seems to be an example of *one-way trapdoor function*[1]: on the one hand is very simple to evaluate powers, but, on the other hand, is very difficult to compute discrete logarithms if p is opportune. The most famous applications are the *Diffie-Hellman Key Exchange*[**17**] and the *ElGamal Cryptosystem*[**18**].

Before dealing with the computation of discrete logarithms, we want to answer the following questions: how to find a primitive root modulo p?, how many primitive roots are there? how can we test whether an element is a primitive root or not? We need a couple of lemmas:

LEMMA 7.1. *If $x \in \mathbb{Z}_p^*$ has order d, then the order of x^a is $\frac{d}{\delta}$, with $\delta = \gcd(a, d)$.*

PROOF. We prove the theorem showing that $ord(x^a)|\frac{d}{\delta}$ and that $\frac{d}{\delta}|ord(x^a)$, so that it must be $ord(x^a) = \frac{d}{\delta}$ in $\mathbb{Z}_p^*$. On the one hand it suffices to note that

$$(x^a)^{\frac{d}{\delta}} = (x^d)^{\frac{a}{\delta}} \equiv 1 \pmod{p},$$

since $d = ord(x)$ in $\mathbb{Z}_p^*$, and $\frac{a}{\delta} \in \mathbb{Z}$ (since $\delta = \gcd(a, d)$). Hence $ord(x^a)|\frac{d}{\delta}$.

On the other hand let us suppose that $ord(x^a) = \epsilon$, so that $(x^a)^\epsilon = 1$ in $\mathbb{Z}_p^*$; since $ord(x) = d$, we have $d|(a\epsilon)$. Thus we can write $d \cdot e = a \cdot \epsilon$ for some e and

[1] These are invertible functions for which the computation of the inverse is hard a priori, but becomes feasible when you know some additional parameter (trapdoor). Another example of a trapdoor one-way function is factorization of a product of two large primes. While selecting and verifying two large primes and multiplying them together is easy, factoring the resulting product is (as we have seen) very difficult. This is the basis for RSA encryption, which is *conjectured* to be trapdoor one-way. The existence of one-way functions is not proven. If true, it would imply $P \neq NP$. Therefore, it would answer the complexity theory *NP*-problem question of whether all apparently *NP*-problems are actually *P*-problems (this is another one million dollars problem by the Clay Mathematics Institute; see also `http://en.wikipedia.org/wiki/Millenium_problems`.). Yet a number of conjectured one-way functions are routinely used in commerce and industry.

applying Bézout's identity yields

$$\gcd(a,d) = \alpha a + \beta d \qquad \text{for some } \alpha, \beta \in \mathbb{Z}.$$

Manipulating

$$\begin{aligned} & (\alpha a + \beta d)\epsilon = \alpha a\epsilon + \beta d\epsilon = \epsilon \gcd(a,d) \\ \Rightarrow \quad & \alpha de + \beta d\epsilon = d(\alpha e + \beta\epsilon) = \epsilon \gcd(a,d) \\ \Rightarrow \quad & \epsilon = \frac{d(\alpha e + \beta\epsilon)}{\gcd(a,d)} \\ \Rightarrow \quad & \frac{d}{\delta} \mid ord(x^a), \end{aligned}$$

and the assertion is proven. □

LEMMA 7.2. *Let p be a prime and $f(X) \in \mathbb{Z}_p[X]$ a monic polynomial of degree d. Then f has at most d zeroes in $\mathbb{Z}_p$.*

PROOF. If f has not zeros in $\mathbb{Z}_p$ there is nothing to prove. Let us suppose that $f(a) = 0$ for some $a \in \mathbb{Z}_p$; dividing the polynomial $f(X)$ by $X - a$ yields a quotient $q(X)$ and a reminder $r \in \mathbb{Z}_p$:

$$f(X) = q(X)(X - a) + r.$$

Hence $f(a) = 0$ implies $r = 0$. Now if b is a zero of $f(X)$ we can write

$$0 = f(b) = q(b)(b - a) \quad \text{in } \mathbb{Z}_p.$$

Since p is prime we can conclude that either p divides $b - a$ or it divides $q(b)$. Thus either $b = a$ in $\mathbb{Z}_p$ or $q(b) = 0$ in $\mathbb{Z}_p$. Now we use induction: the polynomial $q(X)$ has degree $d - 1$ and has at most $d - 1$ zeroes; hence the possibilities for b are $d - 1 + 1 = d$, as required. □

We are now ready to answer to the questions above.

THEOREM 7.3. *$\mathbb{Z}_p^*$ is cyclic since the number of primitive roots of $\mathbb{Z}_p^*$ is $\varphi(p-1) > 0$ (i. e. there exists at least one generator).*

PROOF. For each natural number d we define the set

$$\mathcal{W}_d = \left\{ x \in \mathbb{Z}_p^* : \ ord(x) = d \right\}.$$

We claim that, when $\#\mathcal{W}_d \neq 0$,

$$\#\mathcal{W}_d = \varphi(d).$$

In fact if there exists an element x of order d, then $x^d = 1$, so that

$$\left\{ x^0, x, x^2, \cdots, x^{d-1} \right\} \subset \left\{ \text{zeroes of } X^d - 1 \right\}.$$

Note that the set on the right is the set of the zeroes of the polynomial $X^d - 1$ of degree d; hence by lemma 7.2 this set has at most d elements, whereas the set on the left has exactly d elements. As a consequence the only possibility is

$$\left\{ x^0, x, x^2, \cdots, x^{d-1} \right\} = \left\{ \text{zeroes of } X^d - 1 \right\} = \mathcal{W}_d.$$

Hence the set $\mathcal{W}_d$ consists of powers of x; more precisely, using lemma 7.1, we know that $\mathcal{W}_d$ consists of the elements x^i such that $\gcd(i,d) = 1$, which implies $\#\mathcal{W}_d = \varphi(d)$ as claimed.

Fermat's little theorem tells us that, if $x \in \mathbb{Z}_p^*$, then $ord(x) | \#\mathbb{Z}_p^* = p-1$; as a consequence

$$p - 1 = \sum_{d|(p-1)} \#\mathcal{W}_d,$$

with $\#\mathcal{W}_d$ that is either 0 or $\varphi(d)$. On the other hand, using lemma C.7 of appendix C, we can write $\sum_{d|(p-1)} \varphi(d) = p-1$. Since $0 \leq \#\mathcal{W}_d \leq \varphi(d)$ for each d, we have equality for each d, so that

$$\#\left\{x \in \mathbb{Z}_p^* : \ ord(x) = p-1\right\} = \varphi(p-1) \geq 1,$$

and

$$\mathbb{Z}_p^* = \bigoplus_{d|(p-1)} \left\{x \in \mathbb{Z}_p^* : \ ord(x) = d\right\},$$

is cyclic. □

The above theorem is telling us that the primitive roots of $\mathbb{Z}_p^*$ are $\varphi(p-1)$; one can show that

$$\varphi(n) \geq \frac{n}{c \log\log(n)},$$

for some constant $c \in \mathbb{R}_{>0}$. Since $\log\log(n)$ is almost constant, we can conclude that there is a good proportion of primitive roots; as a consequence we can hope to find a primitive root simply choosing a random element of $\mathbb{Z}_p^*$ and testing if this is a primitive root. This can be done using the following result:

Proposition 7.4. *Let p be a prime number and $g \in \mathbb{Z}_p^*$. g is a primitive root if and only if*

$$g^{\frac{p-1}{q}} \neq 1 \text{ in } \mathbb{Z}_p^* \qquad \forall \text{ prime } q | (p-1).$$

Proof. ($\Rightarrow$). Trivially if $g \in \mathbb{Z}_p^*$ is a primitive root, we have $ord(g) = p$, and as a consequence $g^{\frac{p-1}{q}} \neq 1$, since $\frac{p-1}{q} < p-1 = ord(g)$.

($\Leftarrow$). Let us suppose that g is not a primitive root, i. e. $ord(g) = d$, $d|(p-1)$ but $d \neq p-1$. Hence $\frac{p-1}{d} \in \mathbb{Z}_{>1}$, and there exists a prime q such that $q | \frac{p-1}{d}$, i. e. $p - 1 = q \cdot d \cdot e$ for some $e \in \mathbb{Z}$. Thus

$$g^{\frac{p-1}{q}} = g^{de} = (g^d)^e = 1.$$

□

Example 7.2. We look for one primitive roots of $\mathbb{Z}_{41}^*$. Note that, by theorem 7.3, the total number of primitive roots is $\varphi(40) = 16$. We start with

$g = 2$, and we must check that $2^{\frac{40}{2}}$ and $2^{\frac{40}{5}}$ is not 1. Evaluating

$$\begin{aligned} & 2^7 = 128 \equiv 5 \pmod{41} \\ & 2^{10} = 40 \equiv -1 \pmod{41} \\ \Rightarrow \quad & 2^{20} \equiv 1 \pmod{41}, \end{aligned}$$

we can conclude that 2 is not a primitive root of $\mathbb{Z}_{41}^*$. In a similar fashion it is easy to see that $3^8 \equiv 1 \pmod{41}$, so that 3 is not a primitive root of $\mathbb{Z}_{41}^*$. Note that it is useless to try the powers of an element that is not a primitive root. Repeating the above steps one can find that $g = 6$ is a primitive root of $\mathbb{Z}_{41}^*$. □

The weak point of the above reasoning is that we need all the prime divisors of $p - 1$, and this is not trivial if p is large. A possible solution is to generate a large prime q and try to see if $p = 1 + 2kq$ is prime for some $k = 1, 2, \cdots$. If this is the case we have $p - 1 = 2kq$, and now k is small and we can (usually) factor it. The probability of success is $\approx \frac{1}{\log(q)}$.

In the following sections we deal with the problem of discrete logarithm computation. Let p be a prime and consider a generator g of $\mathbb{Z}_p^*$; given an element $x = g^m \in \mathbb{Z}_p^*$ we look for $m \in \mathbb{Z}_{p-1}$. The simplest solution is the *brute force attack*: we simply evaluate the powers of g, namely $g^2, g^3, \cdots$ looking for m; the complexity is clearly $O(p)$.

7.2. Baby Steps and Giant Steps

The Shanks' algorithm is suitable everytime we have the need to look for some element in a group. We choose a bound $B = \left[\sqrt{p}\right] + 1$ and we write the B-ary expansion of m, namely

$$m = a_0 + Ba_1 \qquad 0 \le a_0, a_1 \le B,$$

since $m < B^2$. Hence we compute the baby-steps $x, xg^{-1}, \cdots, xg^{-B}$ and we put the results in a list; further we evaluate the giant-steps:

$$g^B, (g^B)^2, \cdots, (g^B)^B,$$

and we put the results in a second list. Since $x = g^m = g^{a_0} g^{Ba_1}$ we can look for the element a_0 in the first list and for the element a_1 in the second one; in other words, since

$$xg^{-a_0} = (g^B)^{a_1} \qquad 0 \le a_0, a_1 \le B,$$

we must look for an element that is equal in the two lists. The best way to speed up the baby-step giant-step algorithm is to use an efficient table lookup scheme; the best in this case is a *hash table*. The running time is dominated by the length of the two lists, namely $\sqrt{p}$, i. e.

$$\text{Running-Time: } \Rightarrow \quad O\left(\sqrt{p}\log^2(p)\right) = O\left(e^{\frac{1}{2}\log(p)}\log^2(p)\right),$$

which is exponential (but it is much better than the running-time of the brute force attack).

We close this section presenting an improvement of the algorithm. The idea is trying to factor $p-1$:

$$p-1=\prod_{q|(p-1)} q^{e(q)},$$

and evaluate the elements

$$h=g^{\frac{p-1}{q^{e(q)}}} \qquad y=x^{\frac{p-1}{q^{e(q)}}},$$

for each prime divisor q of $p-1$. Note that the order of h is $q^{e(q)}$ and there is a relation between y and h:

$$x=g^m \quad \Rightarrow \quad y=h^m.$$

Hence we have a new instance of the discrete logarithm problem, in a new group

$$\mathbb{H}=\langle h\rangle=\left\{h^0,h^1,\cdots,h^{e(q)-1}\right\},$$

and we can use the Shanks' algorithm to look for the exponent $m\in\mathbb{Z}_{q^{e(q)}}$. If we repeat the above reasoning for each prime divisor q of $p-1$ we can re-build the original value of $m \bmod p-1 = m \bmod \prod_{q|(p-1)} q^{e(q)}$ by the Chinese Remainder Theorem. The complexity is clearly:

$$\text{Running-Time:} \Rightarrow \quad O\left(\sqrt{q_{max}^{e(q_{max})}}\log^3(p)\right),$$

being q_{max} the largest prime in the factorization of $p-1$[2]. For cryptographic purposes one should avoid primes p such that $p-1$ is smooth with respect to some fixed bound.

7.3. The Index Calculus

The *Index Calculus* is the best algorithm known to solve the discrete logarithm problem. We show the key idea through a couple of examples.

Example 7.3. Let $p=59$, it is easy to see that $g=2$ is a primitive root of $\mathbb{Z}_{59}^*$. We want to evaluate $\log_2(3)\in\mathbb{Z}_{58}$. The idea is to choose random

[2]This result come from the observation that the prime divisors of a given element are just a few. For example let $n=\prod_{i=1}^{d} p_i^{e_i}$, we can write

$$n=\prod_{i=1}^{d} p_i^{e_i}\geq\prod_{i=1}^{d} 2=2^d,$$

so that $d\leq\frac{\log(n)}{\log(2)}$ and the number of prime divisors q of $p-1$ is $\approx\log(p)$.

values around p and trying to factor:

$$\begin{aligned} & 60 = 2^2 \cdot 3 \cdot 5 \equiv 1 \pmod{59} \\ \Rightarrow \quad & 2\log_2(2) + \log_2(3) + \log_2(5) \equiv 0 \pmod{58} \\ \Rightarrow \quad & 2 + \log_2(3) + \log_2(5) \equiv 0 \pmod{58}, \end{aligned}$$

so that we have found a relation between $\log_2(3)$ and $\log_2(5)$. In a similar fashion

$$\begin{aligned} & 64 = 2^6 \equiv 5 \pmod{59} \\ \Rightarrow \quad & 6\log_2(2) \equiv \log_2(5) \pmod{58} \\ \Rightarrow \quad & \log_2(5) \equiv 6 \pmod{58}. \end{aligned}$$

Hence

$$\begin{aligned} & 2 + \log_2(3) + \log_2(5) \equiv \log_2(3) + 2 + 6 \equiv 0 \pmod{58} \\ \Rightarrow \quad & \log_2(3) \equiv -8 \equiv 50 \pmod{58}. \end{aligned}$$

□

Example 7.4. Let $p = 47$, it is easy to see that $g = 5$ is a primitive root of $\mathbb{Z}_{47}^*$. We want to evaluate $\log_5(2) \in \mathbb{Z}_{46}$. We write

$$\begin{aligned} & 50 = 2 \cdot 5^2 \equiv 3 \pmod{47} \\ \Rightarrow \quad & \log_5(2) + 2 \equiv \log_5(3) \pmod{46}, \end{aligned}$$

so that we have found a relation between $\log_5(2)$ and $\log_5(3)$. In a similar fashion

$$\begin{aligned} & 48 = 2^4 \cdot 3 \equiv 1 \pmod{47} \\ \Rightarrow \quad & 4\log_5(2) + \log_5(3) \equiv 0 \pmod{46}. \end{aligned}$$

As a consequence

$$\begin{aligned} & 2 + \log_5(2) \equiv -4\log_5(2) \pmod{46} \\ \Rightarrow \quad & \log_5(2) \equiv -\frac{2}{5} \equiv -\frac{2 \cdot 9}{5 \cdot 9} \equiv 18 \pmod{46}. \end{aligned}$$

□

On the basis of the above examples, we choose a bound and define a factor base:

$$\mathcal{B} = \left\{ \text{primes } \ell_j : \ \ell_j < B \right\}.$$

Typically $B \approx 10^4$. The first part of the algorithm tries to find relations among the discrete logarithms in base g of the primes ℓ_j; the idea is to evaluate the products

$$\prod_{\substack{\ell_j < B \\ \ell_j \text{ primes}}} \ell_j^{e_{ji}} \in \mathbb{Z}, \tag{7.1}$$

and to hope that the element

$$y_i \equiv \prod_{\substack{\ell_j < B \\ \ell_j \text{ primes}}} \ell_j^{e_{ji}} \pmod{p},$$

is B-smooth. Let us suppose that this is the case and denote with

$$y_i = \prod_{\substack{\ell_j < B \\ \ell_j \text{ primes}}} \ell_j^{a_{ji}},$$

the prime factorization of y_i, being a_{ji} the exponent of the element ℓ_j in the factorization of y_i. Note that the above products could not contain *all* the primes of the factor base $\mathcal{B}$; we denote with $\mathcal{S}_i' \subseteq \mathcal{B}$ the set containing the primes ℓ_j in the factorization of y_i and with $\mathcal{S}_i'' \subseteq \mathcal{B}$ the set containing the primes ℓ_j in the product of equation (7.1). We can write

$$\begin{aligned}
&\prod_{\ell_j \in \mathcal{S}_i'} \ell_j^{a_{ji}} \equiv \prod_{\ell_j \in \mathcal{S}_i''} \ell_j^{e_{ji}} \pmod{p} \\
\Rightarrow \quad &\sum_{\ell_j \in \mathcal{S}_i'} a_{ji} \log_g(\ell_j) \equiv \sum_{\ell_j \in \mathcal{S}_i''} e_{ji} \log_g(\ell_j) \pmod{p-1} \\
\Rightarrow \quad &\sum_{\ell_j \in \mathcal{S}_i' \cup \mathcal{S}_i''} (e_{ji} - a_{ji}) \log_g(\ell_j) \equiv 0 \pmod{p-1} \\
\Rightarrow \quad &\sum_{\ell_j \in \mathcal{S}_i} \alpha_{ji} \log_g(\ell_j) \equiv 0 \pmod{p-1},
\end{aligned}$$

where $\alpha_{ji} = e_{ji} - a_{ji}$ and $\mathcal{S}_i = \mathcal{S}_i' \cup \mathcal{S}_i''$. Let us suppose that we have found M of these relations and denote with $N = \#\mathcal{B} = \pi(B)$ the cardinality of the factor base $\mathcal{B}$; we have obtained a linear system of the kind:

$$\begin{pmatrix} \alpha_{11} & \dots & \dots & \alpha_{1N} \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ \alpha_{M1} & \dots & \dots & \alpha_{MN} \end{pmatrix} \begin{pmatrix} \log_g(\ell_1) \\ \log_g(\ell_2) \\ \vdots \\ \log_g(\ell_N) \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{p-1}.$$

When the rank of the matrix above is maximum, there is a unique solution up to multiplication by a constant $\lambda \in \mathbb{Z}_{p-1}$, denoted

$$\lambda \begin{pmatrix} \log_g(\ell_1) \\ \log_g(\ell_2) \\ \vdots \\ \log_g(\ell_N) \end{pmatrix},$$

and it is straightforward to determine λ and normalize[3].

In the last part of the algorithm we evaluate the elements

$$z_k \equiv xg^k \pmod{p} \qquad k = 1, 2, 3, \cdots,$$

being x the element whose discrete logarithm we are looking for; when we met a B-smooth element we can conclude

$$\begin{aligned} z_k \equiv xg^k \equiv & \prod_{\substack{\ell_j < B \\ \ell_j \text{ primes}}} \ell_j^{\xi_k} \pmod{p} \\ \Rightarrow \quad \log_g(x) + k \equiv & \sum_{\substack{\ell_j < B \\ \ell_j \text{ primes}}} \xi_k \log_g(\ell_j) \pmod{p-1}, \end{aligned}$$

and we can compute the desired value $\log_g(x) \in \mathbb{Z}_{p-1}$ since the values $\log_g(\ell_j)$ are now known.

We close this section presenting an estimate of the computational complexity of the algorithm. Note that the running-time depends on the time needed to find elements y_i that are B-smooth, and that the quantities y_i are $\approx p$; hence we can use theorem 6.1 to conclude that the probability that an element $y_i \approx p$ is $B = p^{\frac{1}{u}}$-smooth is approximately u^{-u}. Note that we must factor the values y_i to check whether they are B-smooth or not; if we refer to the Pollard's ρ factorization algorithm, the time needed to find the prime factors $\ell_j < B$ is $O(\sqrt{B}) = O(p^{\frac{1}{2u}})$. As a consequence the time needed to find a single row of the matrix is $O(u^u p^{\frac{1}{2u}})$, and since we need roughly $M \approx N \approx B$ independent rows the total work to build-up the matrix is

$$W_1(u) = u^u p^{\frac{1}{2u}} p^{\frac{1}{u}} = u^u p^{\frac{3}{2u}}.$$

Hence we can minimize (as depicted in figure 7.1) this value with respect to u and determine the optimal value of B.

$$\begin{aligned} & \log(W_1(u)) = u \log(u) + \frac{3}{2u} \log(p) \\ \Rightarrow \quad & \frac{d}{du} \log(W_1(u)) = \log(u) + 1 - \frac{3}{2u^2} \log(p) \stackrel{!}{=} 0 \\ \Rightarrow \quad & \log(ue) - \frac{3}{2u^2} \log(p) = 0. \end{aligned}$$

[3]It suffices to look for an element $\log_g(\ell_i) \in \mathbb{Z}_{p-1}^*$ and choose ℓ_i as primitive root. In fact it is easy to see that

$$e = \log_g(x) \in \mathbb{Z}_{p-1}^* \quad \Leftrightarrow \quad x \text{ is a primitive root.}$$

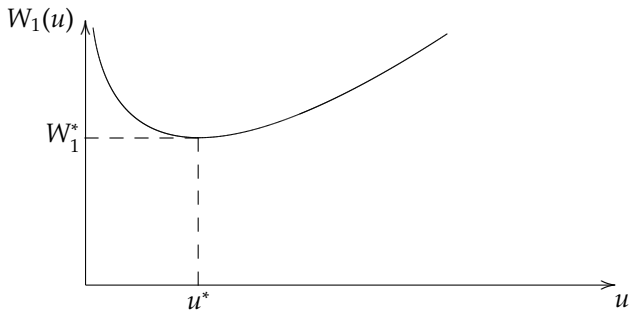


FIGURE 7.1. Work load $W_1(u)$ as a function of u.

Manipulating:

$$\begin{aligned} & \frac{e^2u^2}{2}\log(ue)^2 = \frac{e^2u^2}{2}\frac{3}{u^2}\log(p) \\ \Rightarrow \quad & (ue)^2\log(ue)^2 = 3e^2\log(p), \end{aligned}$$

and using lemma 6.2 we can conclude

$$\begin{aligned} & (ue)^2 = \frac{3e^2\log(p)}{\log(3e^2\log(p))} \\ \Rightarrow \quad & u^2 = \frac{3\log(p)}{\log(3e^2)+\log\log(p)} \approx \frac{3\log(p)}{\log\log(p)} \\ \Rightarrow \quad & u^* \approx \sqrt{\frac{3\log(p)}{\log\log(p)}}. \end{aligned}$$

Thus the optimal value of B is

$$B^* = p^{\frac{1}{u^*}} = e^{\frac{\log(p)}{u^*}} = e^{\sqrt{\frac{1}{3}\log(p)\log\log(p)}},$$

and the minimum work is

$$\begin{aligned} W_1^* &= (u^*)^{u^*}p^{\frac{3}{2u^*}} = e^{u^*\log(u^*)}e^{\log(p)\frac{3}{2u^*}} = \\ &= e^{\sqrt{\frac{3\log(p)}{\log\log(p)}}\frac{1}{2}\log\left(\frac{3\log(p)}{\log\log(p)}\right)} \cdot e^{\frac{3\log(p)}{2}\sqrt{\frac{\log\log(p)}{3\log(p)}}} = \\ &= e^{\frac{1}{2}\sqrt{\frac{3\log(p)}{\log\log(p)}}\left(\log(3)+\log\log(p)-\log\log\log(p)\right)} \cdot e^{\frac{3}{2}\sqrt{\frac{1}{3}\log(p)\log\log(p)}} = \\ &\approx e^{\frac{1}{2}\sqrt{3\log(p)\log\log(p)}}e^{\frac{1}{2}\sqrt{3\log(p)\log\log(p)}} = \\ &= e^{\sqrt{3\log(p)\log\log(p)}}, \end{aligned}$$

which is sub-exponential. This value dominates the complexity $W_2 = O(B^3)$ needed to solve the linear system[4].

Unlike the other algorithms presented in this notes, there is not an elliptic curve version of the index calculus algorithm because of some technical difficulties[**46**].

[4]Note that we need only $M \approx N = \pi(B) \ll B$ relations and indeed:

$$(\pi(B))^3 = \left(\frac{B}{\log(B)}\right)^3 \ll e^{\sqrt{3\log(p)\log\log(p)}}.$$

CHAPTER 8

Pairings on Elliptic Curves

Contents

In this chapter we describe the basic theory of pairings, with particular attention to the *Weil pairing* and the *Tate pairing*. The material covered here follows the description of Maas[**33**], with some minimum changes and some additional concepts. Some examples are taken from Washington[**51**].

8.1. Functions on an Elliptic Curve

Let $\varkappa$ be a field and consider the curve $E: Y^2 = X^3 + AX + B$ defined over $\varkappa$. We define the *coordinate ring* $\varkappa[E]$ of affine curve $E \cap \mathbb{A}^2$ over $\varkappa$ as the integral domain:

$$\varkappa[E] = \varkappa[X, Y]/(Y^2 - X^3 - AX - B).$$

A similar definition holds if we replace $\varkappa$ with $\overline{\varkappa}$. We can write an element $l(X, Y) \in \varkappa[E]$ in *canonical form*

$$l(X, Y) = v(X) + Yw(X) \quad \text{with } v, w \in \varkappa[X],$$

since the exponent of Y is two in the equation defining E.

Example 8.1. Consider the curve $E: Y^2 = X^3 + X + 2$ and the polynomial $l(X, Y) = Y^5 + X - 8 \in \varkappa[X, Y]$. Written in canonical form we have:

$$l(X, Y) = Y \cdot (X^3 + X + 2)^4 + X - 8 \quad \text{in } \varkappa[E],$$

hence $l(X, Y) = v(X) + Yw(X)$, with $v(X) = (X^3 + X + 2)^4$ and $w(X) = X - 8$. □

Definition 8.1 (Rational Function). We define a *function field* $\varkappa(E)$ to be the set:

$$\varkappa(E) = \left\{ f(X, Y) = \frac{g(X, Y)}{h(X, Y)} : \ g, h \in \varkappa[E] \right\}.$$

A similar definition holds if we replace $\varkappa$ with $\overline{\varkappa}$. An element of $\overline{\varkappa}(E)$ is called a *rational function*. □

It can be shown that a rational function $f(X,Y) \in \varkappa(E)$ can always be transformed so as to obtain an expression that is not $\frac{0}{0}$ and hence gives a uniquely determined value in $\overline{\varkappa} \cup \{\infty\}$.

Example 8.2. Consider the curve $E: \ Y^2 = X^3 + X + 2$ over $\varkappa = \mathbb{R}$ and the point $P = (1,2) \in E(\mathbb{R})$. We show that the rational function:

$$f(X,Y) = \frac{X-1}{Y-2} \in \mathbb{R}(E),$$

is not $\frac{0}{0}$ at P. In fact we can manipulate the equation defining E to obtain:

$$(Y-2)(Y+2) = (X-1)^3 + 3(X-1)^2 + 4(X-1),$$

as it is easy to check. Hence

$$f(X,Y) = \frac{Y+2}{(X-1)^2 + 3(X-1) + 4},$$

that is not $\frac{0}{0}$ at $P = (1,2)$. □

Let $O = \infty$ be the point at infinity of $E(\varkappa)$; a non-zero rational function $f \in \overline{\varkappa}^*(E)$ is said to be defined at a point $P \in E(\varkappa) \setminus \{O\}$, if $f = \frac{g}{h}$, for $g, h \in \overline{\varkappa}[E]$, with $h(P) \neq 0$. If this is the case $f(P) = \frac{g(P)}{h(P)}$ is well-defined. The function f is said to have a zero (pole) at P if $f(P) = 0$ ($f(P) = \infty$, i. e. if f is not defined at P).

Now we determine the value of f at the point $P = O$; it seems natural to compare the degrees of the denominator and the enumerator of f. If we want that the relation $Y^2 = X^3 + AX + B$ holds, we assign weights 2 and 3 (respectively) to X and Y, so that if $l(X,Y) \in \overline{\varkappa}[E]$ we have:

$$deg(l) = \max\{2 \cdot deg(v), 3 + 2 \cdot deg(w)\}.$$

Hence, for a rational function $f = \frac{g}{h} \in \overline{\varkappa}(E)$, we say that: $f(O) = \infty$ if $deg(g) > deg(h)$, $f(O) = 0$ if $deg(g) < deg(h)$ and $f(O) = \frac{a}{b}$ if $deg(g) = deg(h)$, being a and b the leading coefficients of g and h (respectively) written in canonical form.

Example 8.3. We take $E: \ Y^2 = X^3 + 3X$ and $\varkappa = \mathbb{Z}_{11}$. The rational function:

$$f(X,Y) = \frac{Y+X+1}{X+8} \in \mathbb{Z}_{11}(E),$$

has $g(X,Y) = Y+X+1$ and $h(X,Y) = h(X) = X+8$, with $deg(g) = 3 > deg(h) = 2$. Thus $f(O) = \infty$ and f has a pole at O. □

Now we deal with *multiplicity* of zeroes and poles. For every point $P \in E(\varkappa)$, there exists a rational function $u_P \in \overline{\varkappa}(E)$ with $u_P(P) = 0$, such that every non-zero rational function $f \in \overline{\varkappa}^*(E)$ can be written as:

$$f(X,Y) = u_P^d(X,Y)s(X,Y),$$

where $s \in \overline{\varkappa}(E)$ with $s(P) \neq 0, \infty$ and $d \in \mathbb{Z}$. The function u_P is called a *uniformizing parameter* for P. The value of d does not depend on the choice of u. The following theorem shows us a way to evaluate a uniformizing parameter:

THEOREM 8.1 (Menezes[**34**]). *Let $P \in E(\varkappa)$ be a point of E. If $u : aX+bY+c = 0$ is any line through P that is not tangent to E at P, then u is a uniformizing parameter for P.* □

It is easy to check[**34**] that if $P = (\alpha, \beta) \notin E[2]$, then $u(X, Y) = X - \alpha$ is a uniformizing parameter for P; if $P = (\alpha, 0) \in E[2]$ then $u(X, Y) = Y$ is a uniformizing parameter for P. Finally if $P = O$, then one can show that $u(X, Y) = \frac{X}{Y}$ is a uniformizing parameter for P.

Now let $u(X, Y)$ be a uniformizing parameter for the non-zero rational function $f \in \overline{\varkappa}^*(E)$.

DEFINITION 8.2 (Order of a Rational Function). We define the *order* of the rational function f at the point P to be:

$$ord_P(f) = d,$$

being $f(X, Y) = u_P^d(X, Y)s(X, Y)$. □

Clearly if P is a zero of f, then $ord_P(f) > 0$ and the zero is said to have multiplicity $ord_P(f)$; on the other hand, if P is a pole of f, then $ord_P(f) < 0$ and the pole is said to have multiplicity $-ord_P(f)$. Remark that if P is neither a zero nor a pole, then $ord_P(f) = 0$.

EXAMPLE 8.4. Consider again the curve $E : Y^2 = X^3 + X + 2$ over $\mathbb{R}$ and the point $P = (1, 2) \in E(\mathbb{R})$. The rational function:

$$f(X, Y) = 4X - Y - 2,$$

has a zero at P. Since $P \notin E[2]$, the line $u_{(1,2)}(X, Y) = X - 1$ is a uniformizing parameter for P; in fact:

$$f(X, Y) = 4(X - 1) - (Y - 2) = (X - 1)\left(4 - \frac{Y - 2}{X - 1}\right) =$$
$$= (X - 1)\left(4 - \frac{(X - 1)^2 + 3(X - 1) + 4}{Y + 2}\right),$$

so that $s(X, Y) = 4 - \frac{(X-1)^2+3(X-1)+4}{Y+2}$ (with $s(P) \neq 0, \infty$) and $d = ord_P(f) = 1$. We say that f has a zero of multiplicity one at $P = (1, 2)$.

Consider now the line tangent to E at P, namely:

$$f(X, Y) = X - Y + 1.$$

We evaluate the multiplicity of the zero $P = (1, 2)$. Manipulating:

$$\begin{aligned} f(X,Y) = (X-1) - (Y-2) &= (X-1)\left(1 - \frac{Y-2}{X-1}\right) = \\ &= (X-1)\left(1 - \frac{(X-1)^2 + 3(X-1) + 4}{Y+2}\right) = \\ &= \frac{X-1}{Y+2}\left((Y-2) - (X-1)^2 - 3(X-1)\right) = \\ &= \frac{(X-1)^2}{Y+2}\left(\frac{(X-1)^2 + 3(X-1) + 4}{Y+2} - (X-1) - 3\right). \end{aligned}$$

The expression in parentheses is finite and does not vanish at P , so $ord_P(f) = 2$, i. e. P is a zero with multiplicity two. In general, the equation of a tangent line will yield a function that vanishes to order *at least* 2 (equal to 2 unless $[3]P = O$ in the group law of E, in which case the order is 3). □

Example 8.5. Recall from example 8.3 that the rational function $f = \frac{Y+X+1}{X+8} \in \mathbb{Z}_{11}(E)$ on the curve $E : \ Y^2 = X^3 + 3X$ has a pole at the point at infinity O. Hence a uniformazing parameter for $P = O$ is $u_O(X, Y) = \frac{X}{Y}$. Thus we can write:

$$f(X,Y) = u_O^d(X,Y)s(X,Y) = \left(\frac{X}{Y}\right)^d \cdot \frac{Y^d(Y+X+1)}{X^d(X+8)}.$$

Then for $d = -1$ we see that $s(X, Y) = \frac{X(Y+X+1)}{Y(X+8)}$ is equal to one at O. Hence $ord_O(f) = -1$ and we say that f has a pole of multiplicity one at O. □

8.2. Divisors Theory

Let E be an elliptic curve defined over a field $\varkappa$. For each point $P \in E(\overline{\varkappa})$, define a formal symbol (P). A *divisor* D on E is a formal sum, i. e. a *finite* linear combination of such symbols with integer coefficients:

$$D = \sum_{P \in E(\overline{\varkappa})} n_P(P), \tag{8.1}$$

where $n_P \in \mathbb{Z}$. The group of divisors of E, namely $Div(E)$, is the free abelian group generated by the points of $E(\overline{\varkappa})$, where addition is given by:

$$D_1 + D_2 = \sum_{P \in E(\overline{\varkappa})} n_P(P) + \sum_{P \in E(\overline{\varkappa})} m_P(P) = \sum_{P \in E(\overline{\varkappa})} (n_P + m_P)(P).$$

We define the *support* and the *degree* of a divisor D, to be (respectively):

$$\mathcal{S} = supp(D) = \{P \in E(\overline{\varkappa}) : \ n_P \neq 0\}$$
$$deg(D) = \sum_{P \in E(\overline{\varkappa})} n_P.$$

It is easy to check that the set of divisors of degree zero, namely $Div^0(E)$, is indeed a sub-group of $Div(E)$.

We can now define the *divisor* of a function f to be:

$$div(f) = \sum_{P \in E(\overline{\varkappa})} ord_P(f)(P).$$

This is a finite sum, hence a divisor, by the following[**22, 26**].

THEOREM 8.2. *Let E be an elliptic curve over $\varkappa$ and let f be a rational function that is not identically zero. Then:*

(1) *f has only finitely many zeroes and poles.*
(2) *$deg(div(f)) = 0$.*
(3) *If f has no zeroes or poles (i. e. if $div(f) = 0$), then f is a constant.*

□

EXAMPLE 8.6. The second statement of theorem 8.2 is telling us that every non-zero rational function $f : E(\varkappa) \to \varkappa$ has the same number of zeroes and poles (counted with multiplicity). Let $E : Y^2 = X^3 + X + 1$ and define f as:

$$\begin{aligned} f : E(\varkappa) &\to \varkappa \\ (x_P, y_P) &\mapsto x_P \in \varkappa \end{aligned}$$

We can easily compute the zeroes of f since $f(P) = 0$ if and only if $P = (0, y_P)$, with $P \in E(\varkappa)$. Hence $P_1 = (0, 1)$ and $P_2 = (0, -1)$ are the zeroes of f. Therefore theorem 8.2 implies that $\mathcal{O}$ is a pole with multiplicity 2, so that:

$$div(f) = (P_1) + (P_2) - 2(\mathcal{O}).$$

□

A divisor $D \in Div(E)$ is called *principal* if $D = div(f)$ for some rational function f. Furthermore, two divisors D_1 and D_2 are said to be (*linearly*) *equivalent*, denoted $D_1 \sim D_2$, if $D_1 - D_2$ is principal, i. e. if $D_1 = D_2 + div(f)$ for some rational function f. The following result[**45**] is central in divisor theory:

THEOREM 8.3. *A divisor $D = \sum_{P \in E} n_P(P)$ is principal if and only if*

$$\sum_{P \in E} n_P = 0 \quad \textit{and} \quad \sum_{P \in E} [n_P]P = \mathcal{O},$$

where the second summation takes place on the curve E. □

Another important result[**32**] is the following theorem:

THEOREM 8.4. *Let $D \in Div(E)$ be a divisor; then there exists a unique point $P \in E$ such that*

$$D \sim (P) + (deg(D) - 1)(\mathcal{O}).$$

□

As a consequence, if $D \in Div^0(E)$, then D is equivalent to $(P) - (\mathcal{O})$ for a uniquely determined point $P \in E$.

The set of all principal divisors is denoted by $Prin(E)$; the quotient group:

$$Pic(E) = Div(E)/Prin(E),$$

whose elements are the divisors that are not principal, is called the *Picard group* or *divisor class group*. Since $div(f_1 f_2) = div(f_1) + div(f_2)$ for all $f_1, f_2 \in \overline{\varkappa}(E)$, $Prin(E)$ is a sub-group of $Div^0(E)$; hence we define the *degree zero part* of the Picard group to be:

$$Pic^0(E) = Div^0(E)/Prin(E).$$

Now we explain how to evaluate a rational function $f \in \overline{\varkappa}(E)$ in a divisor $D = \sum_{P \in E} n_P(P)$ such that $supp(div(f)) \cap supp(D) = \emptyset$. The evaluation of f in D is given by:

$$f(D) = \prod_{P \in supp(D)} f^{n_p}(P).$$

Note that this evaluation is well-defined, since D and $div(f)$ have disjoint support. We have a lemma:

Lemma 8.5. *Let $D \in Div^0 E$ be a degree zero divisor and $f_1 \in \overline{\varkappa}(E)$ a rational function such that $supp(div(f_1)) \cap supp(D) = \emptyset$. Let $c \in \overline{\varkappa}^*$, then the rational function $f_2 = c f_1$ satisfies*

$$f_2(D) = f_1(D).$$

Proof. Let $\mathcal{S} = supp(D)$ be the support of D. Since f_1 and f_2 differ only for a constant, $supp(div(f_1)) = supp(div(f_2))$ and the support of $div(f_2)$ and $\mathcal{S}$ are disjoint. Further we can write $D = \sum_{P \in E} n_P(P) = \sum_{P \in \mathcal{S}} n_P(P)$ and hence:

$$f_2(D) = \prod_{P \in \mathcal{S}} f_2^{n_P}(P) = \prod_{P \in \mathcal{S}} (c f_1(P))^{n_P} = c^{\sum_{P \in \mathcal{S}} n_P} \prod_{P \in \mathcal{S}} f_1^{n_P}(P) =$$
$$= \prod_{P \in \mathcal{S}} f_1^{n_P}(P) = f_1(D),$$

since D has degree zero, i. e. $deg(D) = \sum_{P \in \mathcal{S}} n_P = 0$. □

The following result[**12, 27, 28**] from Weil is an important tool in the study of bilinear maps on elliptic curves:

Theorem 8.6 (Weil's reciprocity law). *Let $f, g \in \overline{\varkappa}(E)$. Then*

$$f(div(g)) = g(div(f)).$$

□

By theorem 8.4 we know that, for any degree zero divisor $D \in Div^0(E)$, there is a unique point $P \in E$ such that $D \sim (P) - (\mathcal{O})$; in other words we can write D in *canonical form*:

$$D = (P) - (\mathcal{O}) + div(f), \tag{8.2}$$

where $f \in \overline{\varkappa}(E)$ is uniquely determined up to a constant multiple. Now we show a procedure to compute the element f and P of equation (8.2) for a given zero degree divisor D. For this purpose, we first find an explicit formula for adding two divisors in canonical form, such that the result is still a divisor in canonical form.

Let $D_1, D_2 \in Div^0(E)$ be written in canonical form:

$$D_1 = (P_1) - (\mathcal{O}) + div(f_1)$$
$$D_2 = (P_2) - (\mathcal{O}) + div(f_2),$$

and let $P_3 = P_1 + P_2$ be the addition (evaluated over the curve E) of the points P_1 and P_2. We indicate the line through P_1 and P_2 with $r: \ Y = \alpha X + \beta$ and the vertical line through P_3 with $r': X = \gamma$; note that if $P_1 = P_2$, r is the line tangent to P_1, furthermore if $P_3 = \mathcal{O}$, we take $r' = 1$. Thus we can write:

$$div(r) = (P_1) + (P_2) + (-P_3) - 3(\mathcal{O})$$
$$div(r') = (P_3) + (-P_3) - 2(\mathcal{O}),$$

and the sum $D_1 + D_2$ is given by:

$$\begin{aligned} D_1 + D_2 &= (P_1) + (P_2) - 2(\mathcal{O}) + div(f_1 f_2) = \\ &= div(r) - div(r') + (P_3) - (\mathcal{O}) + div(f_1 f_2) = \\ &= (P_3) - (\mathcal{O}) + div(f_1 f_2 f_3), \end{aligned} \tag{8.3}$$

where $f_3 = \frac{r}{r'}$. Note that f_3, regarded as an element of $\overline{\varkappa}(X, Y)$, is defined in all points except for P_3 and $-P_3$ (where r' is zero).

Consider now the principal divisor $D = \sum_{i=1}^{n} a_i(P_i) \in Prin(E)$; by theorem 8.3, the divisor D has degree zero and we can write:

$$D = \sum_{i=1}^{n} a_i(P_i) = \sum_{i=1}^{n} a_i((P_i) - (\mathcal{O})).$$

Now let $d_1^{(i)}, d_2^{(i)}, \cdots d_{t_i}^{(i)}$ be an addition chain[1] for a_i. Then for each $i = 1, \cdots, n$ we use the method described above to write the elements $d_j^{(i)}((P_i) - (\mathcal{O}))$ $(j = 1, 2, \cdots, t_i)$ in canonical form. Finally, if $(P_i') - (\mathcal{O}) + div(f_i)$ is the canonical form of the summand $a_i((P_i) - (\mathcal{O}))$, we add the terms $(P_i') - (\mathcal{O}) + div(f_i)$ for $i = 1, 2, \cdots, n$.

Example 8.7. Consider the elliptic curve of the previous example, namely $E: \ Y^2 = X^3 + 3X$ over $\varkappa = \mathbb{Z}_{11}$. Table 8.1 shows the points of $E(\mathbb{Z}_{11})$ with the associated order.

The divisor $D = 6(P_2) - 6(\mathcal{O})$ is clearly principal, because the order of P_2 is 6. An addition chain for 6 is given by $1, 2, 4, 6$. Now we evaluate the rational function f such that $div(f) = D$.

---

[1] Recall that if $a \in \mathbb{N}$, an *addition chain* for a is a sequence $d_1 = 1, d_2, \cdots, d_t = a$, such that each d_j $(2 \le j \le t)$ can be written as $d_j = d_k + d_\ell$, for some $k, \ell < j$.

Point	Order	Point	Order
$P_0 = O$	1	$P_6 = (3,5)$	3
$P_1 = (0,0)$	2	$P_7 = (3,6)$	3
$P_2 = (1,2)$	6	$P_8 = (6,5)$	4
$P_3 = (1,9)$	6	$P_9 = (6,6)$	4
$P_4 = (2,5)$	12	$P_{10} = (7,1)$	12
$P_5 = (2,6)$	12	$P_{11} = (7,10)$	12

TABLE 8.1. $\mathbb{Z}_{11}$-rational points on $E: Y^2 = X^3 + 3X$.

We start noting that, since $div(1) = 0$, we can write:

$$(P_2) - (O) = (P_2) - (O) + div(1).$$

Now we compute:

$$\begin{aligned} 2(P_2) - 2(O) &= ((P_2) - (O)) + ((P_2) - (O)) = \\ &= ((P_2) - (O) + div(1)) + ((P_2) - (O) + div(1)). \end{aligned}$$

It is easy to check that $P_2 + P_2 = P_7$; further $r: Y + 4X + 5 \equiv 0 \pmod{11}$ is the line tangent to P_2 and $r': X + 8 \equiv 0 \pmod{11}$ is the vertical line through P_7 and $-P_7$. Hence equation (8.3) yields:

$$2(P_2) - 2(O) = (P_7) - (O) + div\left(\frac{Y + 4X + 5}{X + 8}\right).$$

In a similar fashion:

$$\begin{aligned} 4(P_2) - 4(O) &= (2(P_2) - 2(O)) + (2(P_2) - 2(O)) = \\ &= (P_6) - (O) + div\left(\frac{(Y + 4X + 5)^2}{(X + 8)^2}\frac{(Y + 3X + 7)}{(X + 8)}\right) \\ 6(P_2) - 6(O) &= (2(P_2) - 2(O)) + (4(P_2) - 4(O)) = \\ &= div\left(\frac{(Y + 4X + 5)^3}{(X + 8)^3}\frac{(Y + 3X + 7)}{(X + 8)}\frac{(X + 8)}{1}\right). \end{aligned}$$

Thus the rational function f such that $div(f) = D$ is:

$$f(X, Y) = \frac{(Y + 4X + 5)^3(Y + 3X + 7)}{(X + 8)^3}.$$

Considered as an element of $\overline{\kappa}[X, Y]$, f is undefined at the points P_6 and P_7; however, regarded as a rational function (i. e. as an element of $\overline{\kappa}(E)$), we

can write:

$$
\begin{aligned}
f(X,Y) &= \frac{(Y+4X+5)^3(Y+3X+7)}{(X+8)^3}\cdot\frac{(Y-4X-5)^3}{(Y-4X-5)^3} = \\
&= \frac{(Y^2+6X^2+4X+8)^3}{(X+8)^3}\cdot\frac{(Y+3X+7)}{(Y-4X-5)^3} = \\
&= \frac{(X^3+6X^2+7X+8)^3}{(X+8)^3}\cdot\frac{(Y+3X+7)}{(Y-4X-5)^3} = \\
&= \frac{(X+8)^3(X+10)^6}{(X+8)^3}\cdot\frac{(Y+3X+7)}{(Y-4X-5)^3} = \\
&= \frac{(X+10)^6(Y+3X+7)}{(Y-4X-5)^3} \\
f(X,Y) &= \frac{(Y+4X+5)^3(Y+3X+7)}{(X+8)^3}\cdot\frac{(Y-3X-7)}{(Y-3X-7)} = \\
&= \frac{(Y+4X+5)^3}{(X+8)^3}\cdot\frac{(X^3+2X^2+5X+6)}{(Y-3X-7)^3} = \\
&= \frac{(Y+4X+5)^3}{(X+8)^3}\cdot\frac{(X+8)^3}{(Y-3X-7)^3} = \\
&= \frac{(Y+4X+5)^3}{(Y-3X-7)},
\end{aligned}
$$

which are both defined (respectively) at P_6 and P_7, as we expected to be. □

8.3. Proof of Associativity

Denote with

$$E(\varkappa) = \left\{(x,y) \in \varkappa \times \varkappa : y^2 = x^3 + A\,x + B\right\} \cup \{O\},$$

the set of points of an elliptic curve defined over a field $\varkappa$. In section 1.2 we stated that $E(\varkappa)$ is an algebraic *group*, $(E(\varkappa), \oplus)$ with the sum operation[2] of definition 1.3.

The *commutativity* is obvious, either having a look at the formulas or observing that the line through P and Q is the same through Q and P. The existence of an identity element (i. e. the point O) is assured by definition; also the inverse of a point P, namely $-P$, exists: it suffices to take the reflection of P across the x-axis. Finally we need to prove associativity, and this is the hardest task. One could check the validity of associativity simply proceeding case by case[**51**] and using definition 1.3, even if it is quite tedious. Here we prefer to use a little bit of *algebraic geometry*[**22**]. Let

[2]To underline the difference of the sum of definition 1.3, only from here to the end of this section, we denote the operation of equation 1.3 with $\oplus$; the formal sum of equation 8.1 is indicated with $+$.

$\varkappa$ be a *perfect* field, with $char(\varkappa) \neq 2, 3$. We recall that a field $\varkappa$ is said to be *perfect* if:

- $char(\varkappa) = 0$ (e. g. $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$), or
- $char(\varkappa) = p$, with p a prime, and every element has a p-th root in the field.

The second condition is equivalent to state that the *Frobenius* map:

$$\begin{aligned} \sigma : \ & \varkappa \to \varkappa \\ & x \mapsto \sigma(x) = x^p \end{aligned}$$

is surjective. We observe explicitly that if $\varkappa$ has $char(\varkappa) = p$ the Frobenius map is an homomorphism since the Newton's binomial is:

$$(x+y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^p = x^p + y^p,$$

thanks to the property $px = 0 \ \forall x \in \varkappa$. The key idea is to show that there exists a bijection between $(E(\varkappa), \oplus)$ and a structure that has an *evident* group structure, like $(Div(E), +)$. Let us start with a definition:

Definition 8.3 ($\varkappa$-Divisors). A $\varkappa$-divisor is a divisor in which the formal sum is taken on points up to conjugate points:

$$Div_\varkappa(E) = \left\{ D \in Div(E) : D = \sum_{\substack{P \in E(\overline{\varkappa}) \\ \text{without} \\ \text{conjugation}}} n_P(P) \right\}$$

□

It is easy to see that $Div_\varkappa(E)$ is a sub-group of $Div(E)$. Recall that the conjugation is a map:

$$\begin{aligned} {}^* : \ & \overline{\varkappa} \to \overline{\varkappa} \\ & x \mapsto x^* \end{aligned}$$

such that it leaves $\varkappa$ fixed and $x \in \varkappa \Leftrightarrow x = x^*$.

Example 8.8. Take $\varkappa = \mathbb{R}$ so that $\overline{\varkappa} = \mathbb{C}$; here we already know the definition of conjugate:

$$\begin{aligned} {}^* : \ & \mathbb{C} \to \mathbb{C} \\ & x \mapsto x^* \end{aligned}$$

which leaves $\mathbb{R}$ fixed and it is such that $x \in \mathbb{R} \Leftrightarrow x = x^*$. □

Hence if P, P' and P'' are conjugate points of $E(\varkappa)$ in the formal sum of definition 8.3 it will appear only one of them. Another subgroup of $Div(E)$ is the set of $\varkappa$-divisors of degree zero:

Definition 8.4 ($\varkappa$-divisors of degree zero). We define the group of $\varkappa$-divisors of degree zero as:

$$Div^0_\varkappa(E) = \{D \in Div_\varkappa(E) : deg(D) = 0\}$$

where $deg(D) = \sum_{P\in E(\overline{\varkappa})} n_P \in \mathbb{Z}$ is the *degree* of D. □

In a similar fashion to the previous section, we denote with

$$Prin_\varkappa(E) = \{D \in Div_\varkappa(E) : \exists\, f \text{ such that } D = div(f)\},$$

the group of principal divisors in $Div_\varkappa(E)$ (it is a subgroup of the group $Div(E)$), and with

$$Pic_\varkappa(E) = Div(E)/Prin_\varkappa(E),$$

the Picard group whose elements are the divisors that are not principal $\varkappa$-divisors.

Let $D \in Div(E)$. We associate to D the set of functions[3]:

$$H^0(D) = \{\text{Rational functions } f :\ div(f) \geq -D\}.$$

Example 8.9. Consider a curve C over $\varkappa$. If $D = (P) + 2(Q)$ (with $P, Q \in C(\varkappa)$), then $H^0(D)$ consists of those algebraic functions having no poles outside P and Q and having at worst a single pole at P and a double pole at Q. Each $H^0(D)$ is a vector space over $\varkappa$, and in fact a finite-dimensional vector space, with dimension $\ell(D)$. □

Now we have all the elements to state one of the most fundamental results in algebraic geometry of curves, i. e. the *Riemann-Roch theorem*:

Theorem 8.7 (Riemann-Roch[**22, 45**]). *Let $D \in Div(E)$ be a divisor and E be an algebraic smooth curve. There is an integer $g \geq 0$ such that*

$$\ell(D) = \#H^0(D) \geq deg(D) + 1 - g.$$

The smallest g with this property is called the genus of the curve. □

One can show that every elliptic curve has genus $g = 1$, hence if E is elliptic $\ell(D) = deg(D)$.

Now we are ready to prove associativity:

Theorem 8.8 (Proof of associativity). *Let ϕ be the map defined by:*

$$\phi :\ E(\varkappa) \longleftrightarrow Div^0_\varkappa(E)/Prin_\varkappa(E)$$
$$P \longmapsto \overline{(P) - (\mathcal{O})}$$

where $\overline{(P) - (\mathcal{O})}$ denotes the equivalence class associated with the divisor $(P) - (\mathcal{O})$ in $Div^0_\varkappa(E)/Prin_\varkappa(E)$. Then:

(1) *ϕ is a bijection,*
(2) *ϕ respects the group law, i. e. $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.*

[3] In general we say that $D \geq 0$ if and only if $n_P \geq 0$, $\forall P \in E(\varkappa)$. Hence $D \geq D'$ if and only if $D - D' \geq 0$.

PROOF. (1). We need to prove that ϕ is injective and surjective; we start with injectivity. Let us suppose that ϕ is not injective, i. e. that there exist P and Q such that $\overline{(P)-(\mathcal{O})} = \overline{(Q)-(\mathcal{O})}$. Hence, by definition of quotient set, the difference $((P)-(\mathcal{O}))-((Q)-(\mathcal{O}))$ is principal, i. e.:

$$((P)-(\mathcal{O}))-((Q)-(\mathcal{O})) = (P)-(Q) = div(f) \in Prin_{\varkappa}(E).$$

Therefore we can state that $div(f) \geq -(Q)$ if and only if $(P) = div(f)+(Q) \geq 0$. Let $f \in H^0((Q))$, using the Riemann-Roch theorem 8.7 we have $\#H^0((Q)) = deg((Q)) = 1$. In general $\varkappa \subseteq H^0((Q))$, but $\#H^0((Q)) = 1$ and then $\varkappa = H^0((Q))$. Hence $f \in H^0((Q))$ is constant and we have:

$$div(f) = 0 = (P)-(Q) \qquad \Rightarrow \qquad (P) = (Q),$$

and ϕ is injective.

To prove surjectivity, let $\overline{D} \in Div^0_{\varkappa}(E)/Prin_{\varkappa}(E)$ the equivalence class associated with the principal divisor D in the quotient set; as D is principal it has degree zero and hence $-D+(\mathcal{O})$ has degree 1. By the Riemann-Roch theorem then:

$$\#H^0(-D+(\mathcal{O})) = deg(-D+(\mathcal{O})) = 1.$$

Therefore $\exists\, f \neq 0$, such that $f \in H^0(-D+(\mathcal{O}))$, i. e.:

$$div(f) \geq -(-D+(\mathcal{O})) = D-(\mathcal{O}) \quad \Rightarrow \quad div(f)-D+(\mathcal{O}) \geq 0.$$

Furthermore:

$$deg(div(f)-D+(\mathcal{O})) = deg(div(f)) - deg(D) + deg((\mathcal{O})) = \\ = 0-0+1 = 1,$$

so that $div(f)-D+(\mathcal{O})$ is indeed of the form $div(f)-D+(\mathcal{O}) = (P)$, i. e. $div(f)-D = (P)-(\mathcal{O})$ and the map ϕ is surjective.

(2). It suffices to show that $((P \oplus Q)-(\mathcal{O})) = ((P)-(\mathcal{O}))+((Q)-(\mathcal{O}))$ in $Div^0_{\varkappa}(E)/Prin_{\varkappa}(E)$, i. e. that

$$((P \oplus Q)-(\mathcal{O}))-((P)-(\mathcal{O})+(Q)-(\mathcal{O})) = (P \oplus Q)-(P)-(Q)+(\mathcal{O})$$

is a principal divisor. For this to hold there must be a function h such that $(P \oplus Q)-(P)-(Q)+(\mathcal{O}) = div(h)$. Write the projective equation of the lines $l_1 :\ \alpha X+\beta Y+\gamma Z = 0$ for P, Q and S and $l_2 :\ X-\delta Z = 0$ for R and S (see figure 1.2). Let $f, g :\ E(\varkappa) \to \mathbb{R}$ the functions $\alpha X+\beta Y+\gamma Z$ and $X-\delta Z$ (respectively), it is quite obvious that the points P, Q and S are the zeroes of $f|_E$ and $R = P \oplus Q$ and S are the zeroes of $g|_E$, so that by lemma 8.2:

$$div(f|_E) = (P)+(Q)+(S)-3(\mathcal{O})$$
$$div(g|_E) = (P \oplus Q)+(S)-2(\mathcal{O}).$$

Hence if we let $h = \frac{g|_E}{f|_E}$ we have proven the theorem, since:

$$div(h) = (P \oplus Q)+(S)-2(\mathcal{O})-(P)-(Q)-(S)+3(\mathcal{O}) = \\ = (P \oplus Q)-(P)-(Q)+(\mathcal{O}),$$

as desired. □

8.4. Weil Pairing

This section is dedicated to the Weil pairing. There are two distinct definition which can be shown to be equivalent; as we will see the second one is more suitable for (efficient) implementation.

We need some further technical ingredients.

Definition 8.5 (Ramification Index). Let $H : E \longrightarrow E$ be a non-constant rational mapping, $P \in E$ and $u(X, Y)$ be a uniformizing parameter for $H(P)$. Then the *ramification index* of H at P is defined by:

$$r_H(P) = ord_P(u \circ H).$$

□

By definition of order for a point, we see that $r_H(P)$ does not depend on the choice of u. It is also clear that, since u is a uniformizing parameter for $H(P)$, $u \circ H$ has a zero at P, so that $r_H(P) \geq 1$. Further one can show[**11**] that, if H is an endomorphism, than $r_H(P)$ is constant for all P, i. e. $r_H(P) = r_H$. In particular, when $H = [n]$, we have $r_H = 1$. We need another definition:

Definition 8.6. Let $H : E \longrightarrow E$ be a non-constant rational mapping. The homomorphism $H^* : Div(E) \longrightarrow Div(E)$ is given by:

$$H^*((Q)) = \sum_{H(P)=Q} r_H(P) \cdot (P).$$

□

One can show[**11**] that $div(t \circ H) = H^*(div(t))$, where t is a non-zero rational function.

Now we are ready to define the Weil pairing. Recall that, by theorem 8.3, a divisor $D = \sum_{P \in E} n_P(P)$ is principal, if and only if $deg(D) = 0$ and $\sum_{P \in E}[n_P]P = \mathcal{O}$. Let $n \geq 2$ be a fixed integer coprime to $char(\varkappa)$ and suppose that T is a point of the n-torsion of E, i. e. $T \in E[n]$. Since T has order n, it easily follows that the divisor $n(T) - n(\mathcal{O})$ is principal, hence there exists $f \in \overline{\varkappa}(E)$ such that

$$n(T) - n(\mathcal{O}) = div(f).$$

Consider the divisor $[n]^*(T) - [n]^*(\mathcal{O})$, by definition 8.5 we can write:

$$[n]^*(T) - [n]^*(\mathcal{O}) = \sum_{[n]P=T} r_{[n]}(P) \cdot (P) - \sum_{[n]P=\mathcal{O}} r_{[n]}(P) \cdot (P).$$

Let $T' \in E$ be such that $[n]T' = T$; note that such a point always exists, since $\overline{\varkappa}$ is an algebraically closed field. Since $r_{[n]} = 1$ we can thus write:

$$[n]^*(T) - [n]^*(\mathcal{O}) = \sum_{R \in E[n]} ((T' + R) - (R)),$$

which clearly has degree zero. Moreover $[n^2]T' = O$ and, by theorem 2.2, $\#E[n] = n^2$; thus

$$\sum_{R \in E[n]} (T' + R - R) = [n^2]T' = O.$$

Hence we can conclude that the divisor $[n]^*(T) - [n]^*(O)$ is principal and then there exists a rational function $g \in \overline{\varkappa}(E)$ such that:

$$[n]^*(T) - [n]^*(O) = div(g).$$

Definition 8.7 (Weil Pairing). Let $\mathcal{U}_n = \{x \in \overline{\varkappa} : \ x^n = 1\}$ be the group of n-th roots of unity in $\overline{\varkappa}$. With the notation as introduced above, the Weil e_n-pairing is a map:

$$e_n : \ E[n] \times E[n] \longrightarrow \mathcal{U}_n,$$

such that

$$e_n(S, T) = \frac{g(S' + S)}{g(S)},$$

where $S' \in E$ is any point such that $g(S' + S), g(S') \neq 0, \infty$. □

The following theorem shows that the Weil pairing is well-defined:

Theorem 8.9. *The Weil pairing e_n is well-defined, i. e. it maps to an n-th root of unity and does not depend on the choice of function g and point S'.*

Proof. Let $S, T \in E[n]$. Recall that $[n]^*$ is build-up in such a way that:

$$\begin{aligned} div(f \circ [n]) = [n]^*(div(f)) = [n]^*(n(T) - n(O)) = \\ = n \cdot div(g) = div(g^n), \end{aligned}$$

i. e. $f \circ [n]$ and g^n are equal, up to a multiplicative constant $c \in \overline{\varkappa}^*$. Hence

$$g^n = c(f \circ [n]). \tag{8.4}$$

Now, for each $S' \in E$ we have:

$$g(S' + S) = cf([n]S' + [n]S) = cf([n]S') = g^n(S'),$$

thus

$$(e_n(S, T))^n = \frac{g^n(S' + S)}{g^n(S')} = 1$$

and $e_n(S, T)$ is indeed an n-th root of unity. Moreover $e_n(S, T)$ does not depend on the choice of g, as g is unique up to a constant multiple.

It remains to show that the pairing does not depend on the choice of S'. Let Ξ_P be the map:

$$\begin{aligned} \Xi_P : \ E &\longrightarrow E \\ Q &\mapsto Q + P, \end{aligned}$$

the Weil pairing is:

$$e_n(S, T) = \frac{(g \circ \Xi_S)(S')}{g(S')}.$$

One can show[**11**] that, for $S, T \in E[n]$, we have $div(g \circ \Xi_S) = div(g)$. Hence $e_n(S, T)$ is a constant and thus it does not depend on the choice of S' (provided that $g(S' + S), g(S') \neq 0, \infty$). □

The following theorem shows some very useful properties of the Weil pairing:

THEOREM 8.10 (Properties of the Weil Pairing). *Let $S_1, S_2, S, T_1, T_2, T \in E[n]$. The Weil pairing satisfies:*

(1) $e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$ *(linearity in the first factor).*
(2) $e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$ *(linearity in the second factor).*
(3) $e_n(S, S) = 1$ *(identity).*
(4) $e_n(S, T) = (e_n(T, S))^{-1}$ *(alternation).*
(5) *If $e_n(S, T) = 1$ for all $S \in E[n]$, then $T = O$ (non-degeneracy).*

PROOF. (1). We use the fact that the value of $e_n(S, T)$ does not depend on the choice of S'; thus we use S' and $S' + S_1$:

$$e_n(S_1, T)e_n(S_2, T) = \frac{g(S' + S_1)}{g(S')}\frac{g(S' + S_1 + S_2)}{g(S' + S_1)} = \\ = \frac{g(S' + S_1 + S_2)}{g(S')} = e_n(S_1 + S_2, T).$$

(2). Let $T_3 = T_1 + T_2$ and let f_i, g_i be the functions used above to define $e_n(S, T_i)$ (with $i = 1, 2, 3$). Since the divisor $(T_3) - (T_1) - (T_2) + (O)$ is principal, by theorem 8.3 there exists $h \in \overline{\varkappa}(E)$ such that:

$$div(h) = (T_3) - (T_1) - (T_2) + (O).$$

Hence

$$div\left(\frac{f_3}{f_1 f_2}\right) = div(f_3) - div(f_1) - div(f_2) = n \cdot div(h) = div(h^n),$$

and $f_3 = c f_1 f_2 h^n$ for some $c \in \overline{\varkappa}^*$. This implies, using equation (8.4) that:

$$g_3 = c^{1/n}(f_3^{1/n} \circ [n]) = c^{1/n}(g_1)(g_2)(h \circ [n])$$

which yields

$$e_n(S, T_1 + T_2) = \frac{g_3(S' + S)}{g_3(S')} = \\ = \frac{g_1(S' + S)}{g_1(S')}\frac{g_2(S' + S)}{g_2(S')}\frac{h([n](S' + S))}{h([n]S')} = \\ = e_n(S, T_1)e_n(S, T_2),$$

since $[n]S = O$, i. e. $h([n](S' + S)) = h([n]S')$.

(3). Consider the function $f \circ \Xi_{[i]T}$, which maps $P \mapsto f(P + [i]T)$. Note that:

$$div\left(\prod_{i=0}^{n-1} f \circ \Xi_{[i]T}\right) = \sum_{i=0}^{n-1} div(f \circ \Xi_{[i]T}) =$$
$$= n \sum_{i=0}^{n-1} ([1-i]T) - ([-i]T) = 0,$$

since the divisor of $f \circ \Xi_{[i]T}$ is $n(T-[i]T)-n([-i]T)$. It follows that $\prod_{i=0}^{n-1} f \circ \Xi_{[i]T}$ is a constant and if we choose some $T' \in E$ such that $[n]T' = T$, then $\prod_{i=0}^{n-1} g \circ \Xi_{[i]T'}$ is also a constant, because its n-th power is the above product of f's:

$$\left(\prod_{i=0}^{n-1} g \circ \Xi_{[i]T'}\right)^n = \prod_{i=0}^{n-1} f \circ [n] \circ \Xi_{[i]T'} =$$
$$= \prod_{i=0}^{n-1} f \circ \Xi_{[i]T} \circ [n].$$

Hence

$$\prod_{i=0}^{n-1} g(S' + T' + [i]T') = \prod_{i=0}^{n-1} g(S' + [i]T'),$$

and cancelling like terms yields $g(S') = g(S' + [n]T') = g(S' + T)$. Finally:

$$e_n(T, T) = \frac{g(S' + T)}{g(S')} = 1.$$

(4). Combining previous properties yields:

$$1 = e_n(S + T, S + T) = e_n(S, S)e_n(S, T)e_n(T, S)e_n(T, T) =$$
$$= e_n(S, T)e_n(T, S)$$
$$\Rightarrow \quad e_n(S, T) = (e_n(T, S))^{-1}.$$

(5). If $e_n(S, T) = 1$ for all $S \in E[n]$ it must be $g(S' + S) = g(S')$ for all $S \in E[n]$. One can show[**45**] that this implies $g = h \circ [n]$ for some function $h \in \overline{\varkappa}(E)$. Hence

$$(h \circ [n])^n = g^n = f \circ [n],$$

so that $f = ch^n$ for some $c \in \overline{\varkappa}^*$. Thus

$$n \cdot div(h) = div(f) = n(T) - n(O)$$
$$\Rightarrow \quad div(h) = (T) - (O),$$

which yields $T = O$. □

Corollary 8.11. *Let n be a prime and S and T be two linearly independent n-torsion points. Then* $e_n(S, T) \neq 1$.

Proof. By the non-degeneracy of the Weil pairing, there exists $T' \in E[n]$, independent from S, such that $e_n(S,T') \neq 1$. Since n is prime, $e_n(S,T')$ is a primitive n-th root of unity in $\overline{\varkappa}$. Moreover $E[n]$ is generated by S and T', since they are independent, i. e. $T = [a]S + [b]T'$, with $0 \leq a, b \leq n-1$. Hence

$$\begin{aligned} e_n(S,T) = e_n(S,[a]S + [b]T') = (e_n(S,S))^a (e_n(S,T'))^b = \\ = (e_n(S,T'))^b \neq 1, \end{aligned}$$

since $e_n(S,T')$ is a primitive n-th root of unity whereas $b \leq n-1$. □

We close this section presenting an alternative definition of the Weil pairing which is more suitable to a practical implementation. Let n be an integer and let $S, T \in E[n]$. Let D_S and D_T be two divisors such that $D_S \sim (S) - (\mathcal{O})$, $D_T \sim (T) - (\mathcal{O})$, and $supp(D_S) \cap supp(D_T) = \emptyset$. Since S, T are n-torsion points, it is easy to see that nD_S and nD_T are principal divisors. Hence there exist $f_S, f_T \in \overline{\varkappa}(E)$ such that:

$$\begin{aligned} div(f_S) &= nD_S \\ div(f_T) &= nD_T. \end{aligned}$$

Definition 8.8 (Alternative Weil Pairing). With the notation as introduced above, the alternative Weil pairing is given by:

$$e'_n : E[n] \times E[n] \longrightarrow \mathcal{U}_n,$$

such that

$$e'_n(S,T) = \frac{f_S(D_T)}{f_T(D_S)}.$$

□

Some authors define the pairing as $\frac{f_T(D_S)}{f_S(D_T)}$, thus obtaining the inverse of our definition. The following theorems show that the alternative Weil pairing is well-defined and bilinear.

Theorem 8.12. *The alternative Weil pairing is well-defined, i. e. it maps to an n-th root of unity and does not depend on the choice of divisors D_S and D_T and functions f_S and f_T.*

Proof. First of all observe that by Weil's reciprocity law we can write:

$$\begin{aligned} \left(\frac{f_S(D_T)}{f_T(D_S)}\right)^n = \frac{(f_S(D_T))^n}{(f_T(D_S))^n} = \frac{f_S(nD_T)}{f_T(nD_S)} = \frac{f_S(div(f_T))}{f_T(nD_S)} = \\ = \frac{f_T(div(f_S))}{f_T(nD_S)} = \frac{f_T(nD_S)}{f_T(nD_S)} = 1, \end{aligned}$$

so that $e'_n(S,T)$ is an n-th root of unity.

Let now $D'_T \neq D_T$ be a divisor such that $supp(D_S) \cap supp(D'_T) = \emptyset$ and $D'_T \sim (T) - (\mathcal{O})$; since nD'_T is a principal divisor, we can write $nD'_T = div(f'_T)$

for some rational function f'_T. Since $D'_T \sim D_T$, we have $D'_T = D_T + div(h)$ and thus $f'_T = f_T h^n$ for some $h \in \overline{\varkappa}(E)$. Hence

$$e'_n(S,T) = \frac{f_S(D'_T)}{f'_T(D_S)} = \frac{f_S(D_T)f_S(div(h))}{f_T(D_S)h^n(D_S)} = \frac{f_S(D_T)f_S(div(h))}{f_T(D_S)h(nD_S)} =$$
$$= \frac{f_S(D_T)}{f_T(D_S)}\frac{f_S(div(h))}{h(div(f_S))} = \frac{f_S(D_T)}{f_T(D_S)}\frac{h(div(f_S))}{h(div(f_S))} = \frac{f_S(D_T)}{f_T(D_S)},$$

where we used Weil's reciprocity law in the last passage. This shows that the pairing does not depend on the choice of D_T; in a similar fashion one can show that $e'_n(S,T)$ does not depend on the choice of D_S too.

Lastly we observe that functions f_S and f_T are unique up to a multiplicative constant. Since both are being evaluated in a degree zero divisor, lemma 8.5 implies that the result does not depend on the choice of these constants. □

THEOREM 8.13. *The alternative Weil pairing is bilinear.*

PROOF. We prove linearity in the first factor, linearity in the second factor goes analogously. Let

$$e'_n(S_1 + S_2, T) = \frac{f_S(D_T)}{f_T(D_S)},$$

where $D_S \sim (S_1 + S_2) - (O)$, $D_T \sim (T) - (O)$, $div(f_S) = nD_S$ and $div(f_T) = nD_T$. We introduce divisors D_{S_1} and D_{S_2} such that

$$D_{S_1} \sim (S_1) - (O) \qquad D_{S_2} \sim (S_2) - (O),$$

and functions f_{S_1} and f_{S_2} such that

$$div(f_{S_1}) = nS_1 \qquad div(f_{S_2}) = nS_2.$$

Note that the divisor $(S_1 + S_2) - (S_1) - (S_2) + (O)$ is principal, so $(S_1) + (S_2) - 2(O) \sim (S_1 + S_2) - (O)$; hence we can take $D_S = D_{S_1} + D_{S_2}$. On the other hand, since

$$div(f_S) = nD_S = nD_{S_1} + nD_{S_2} = div(f_{S_1}) + div(f_{S_2}) = div(f_{S_1}f_{S_2}),$$

we can write $f_S = f_{S_1}f_{S_2}$, and thus

$$e'_n(S_1 + S_2, T) = \frac{f_S(D_T)}{f_T(D_S)} = \frac{(f_{S_1} \cdot f_{S_2})(D_T)}{f_T(D_{S_1} + D_{S_2})} =$$
$$= \frac{f_{S_1}(D_T)}{f_T(D_{S_1})}\frac{f_{S_2}(D_T)}{f_T(D_{S_2})} = e'_n(S_1,T)e'_n(S_2,T).$$

□

Moreover there is a precise relation between definitions 8.7 and 8.8.

THEOREM 8.14. *Let $S, T \in E[n]$. Then:*

$$e_n(S,T) = \frac{1}{e'_n(S,T)}.$$

PROOF. The interested reader is addressed to **[33, 51]**. □

Consequently we can conclude that also the alternative Weil pairing satisfies[4] the properties of theorem 8.10. The fact that $e_n(S,T)$ is not fully equivalent to $e'_n(S,T)$ does not have consequences for the use of the Weil pairing in practice. Since one can exchange the role of points S and T in the definition of the Weil pairing, we can work as well with $e_n(T,S) = \frac{1}{e'_n(T,S)} = e'_n(S,T)$. So without loss of generality we can choose either one of the two definitions; in the following we will work with the Weil pairing using definition 8.8. To ease notation we will denote the pairing by e_n rather than e'_n.

In this section we have defined the Weil pairing as a bilinear map to the n-th group of unity in $\overline{\varkappa}$; let $\varkappa = \mathbb{Z}_p$ be a finite field with p elements. One can show that it is not necessary to consider all the algebraic closure of $\mathbb{Z}_p$, but it suffices to take a subfield $\mathbb{F}_{p^{k_w}}$ of $\overline{\varkappa}$, which is an extension field of $\mathbb{Z}_p$ of degree k_w, being k_w the smallest index such that $E[n] \subseteq E(\mathbb{F}_{p^{k_w}})$. This parameter, called the *Weil embedding degree of the elliptic curve with respect to* n plays an important role in cryptographic applications**[33]**.

8.5. The Tate-Lichtenbaum Pairing

In addition to the Weil pairing there is another bilinear map which is called the Tate pairing**[19, 20]**. Consider the curve E over $\varkappa$, where $\varkappa$ is a finite field. We denote by $nE(\varkappa)$ the set of *distinct* points obtained multiplying the points of $E(\varkappa)$ by n. This set is called a *coset* of $E(\varkappa)$ and it is denoted by C_O since it always contains O. Note that we can obtain other cosets, namely C_R, by adding a point $R \notin C_O$ to every element in the coset. This way we can split the set $E(\varkappa)$ in n distinct cosets. Denote the quotient group of all cosets by $E(\varkappa)/nE(\varkappa)$ and let us suppose that n is prime. If $E[n] \not\subseteq E(\varkappa)$, then every coset contains exactly one n-torsion point, else if $E[n] \subseteq E(\varkappa)$, then there are n points of $E[n]$ in each coset.

EXAMPLE 8.10. Consider the curve of the previous example, $E : Y^2 = X^3 + 3X$ over $\mathbb{Z}_{11}$. The points of $E(\mathbb{Z}_{11})$ are listed in table 8.1 with their order. We choose $n = 3$ and split $E(\mathbb{Z}_{11})$ in cosets. Note that:

$$[3]O = [3]P_6 = [3]P_7 = O \qquad [3]P_1 = [3]P_2 = [3]P_3 = P_1$$
$$[3]P_4 = [3]P_9 = [3]P_{10} = P_8 \qquad [3]P_5 = [3]P_8 = [3]P_{11} = P_9.$$

Hence $nE(\mathbb{Z}_{11}) = C_O = \{O, P_1, P_8, P_9\}$. The cosets C_{P_2} and C_{P_3} are obtained, respectively, adding the points P_2 and P_3 to each point of C_O:

$$C_{P_2} = \{P_2, P_6, P_{10}, P_5\} \qquad C_{P_3} = \{P_3, P_7, P_4, P_{11}\}.$$

[4]The *identity* and *alternation* properties are trivial to prove in the setting of the alternative Weil pairing. Instead, no proof of the *non-degeneracy* that directly uses the alternative definition seems to be known.

Cosets $C_{\mathcal{O}}$, C_{P_2} and C_{P_3} all contain exactly one n-torsion point (since $E[3] \nsubseteq E(\mathbb{Z}_{11})$), namely $\mathcal{O}$, P_6 and P_7 respectively. Finally we have $E(\mathbb{Z}_{11})/3E(\mathbb{Z}_{11}) = \{C_{\mathcal{O}}, C_{P_2}, C_{P_3}\}$. □

Let now n be an integer coprime to p, such that $E(\mathbb{Z}_p)$ contains a point of order n. In cryptographic implementations, n is usually taken to be a large prime such that $n|\#E(\mathbb{Z}_p)$. Define the *Tate embedding degree of the curve with respect to n* to be the smallest integer k_t such that $n|(p^{k_t} - 1)$. Let $P \in E(\mathbb{F}_{p^{k_t}})[n]$, then $n(P) - n(\mathcal{O})$ is a principal divisor. So there is a rational function $g \in \mathbb{F}_{p^{k_t}}(E)$ such that $div(g) = n(P) - n(\mathcal{O})$. Now let Q be a point representing a coset in $E(\mathbb{F}_{p^{k_t}})/nE(\mathbb{F}_{p^{k_t}})$; we build-up a divisor $D \in Div^0(E)$ such that $D \sim (Q) - (\mathcal{O})$ and that $supp(D) \cap supp(div(g)) = \emptyset$. We define the *Tate* pairing as follows:

Definition 8.9 (Tate Pairing). With the notation as introduced above, the *Tate pairing* is a map:

$$\tau_n : E(\mathbb{F}_{p^{k_t}})[n] \times E(\mathbb{F}_{p^{k_t}})/nE(\mathbb{F}_{p^{k_t}}) \longrightarrow \mathbb{F}^*_{p^{k_t}}/(\mathbb{F}^*_{p^{k_t}})^n,$$

such that

$$\tau_n(P, Q) = g(D).$$

□

Note that the outcome of the Tate pairing is not a unique value, but an equivalence class in $\mathbb{F}^*_{p^{k_t}}/(\mathbb{F}^*_{p^{k_t}})^n$; in other words, two elements $a, b \in \mathbb{F}^*_{p^{k_t}}$ are equivalent (denoted by $a \equiv b$) if and only if there is a constant $c \in \mathbb{F}^*_{p^{k_t}}$ such that $a = bc^n$. Often, most of the times for cryptographic purposes, we require the result of the evaluation of the pairing to be unique, so that we need to eliminate n-th powers. This is done by raising the value to the power $\frac{p^{k_t}-1}{n}$, since $a^{p^{k_t}-1} = 1$ for all $a \in \mathbb{F}^*_{p^{k_t}}$; hence, after exponentiation, we obtain a primitive n-th root of unity. This leads to an alternative definition for the Tate pairing:

$$\tau'_n : E(\mathbb{F}_{p^{k_t}})[n] \times E(\mathbb{F}_{p^{k_t}})/nE(\mathbb{F}_{p^{k_t}}) \longrightarrow \mathcal{U}_n,$$

such that

$$\tau'_n(P, Q) = (g(D))^{\frac{p^{k_t}-1}{n}}.$$

The following theorem shows that the Tate pairing is well-defined:

Theorem 8.15. *The result of the Tate pairing does not depend on the choice of the rational function g and divisor D.*

Proof. The function g is determined up to a constant multiple; however, since D is a degree zero divisor, by lemma 8.5 we are sure that this constant has no influence on the evaluation of the function g in D.

Let now g be a rational function such that $div(g) = n(P) - n(\mathcal{O})$ and $D_1 \sim D_2 \sim (Q) - (\mathcal{O})$ be such that the support of both D_1 and D_2 is disjoint

from $supp(div(g))$. Thus there exists a rational function h such that $D_1 = D_2 + div(h)$, with $supp(div(h)) \cap supp(div(g)) = \emptyset$. Hence

$$\begin{aligned}\tau_n(P,Q) = g(D_1) = g(D_2 + div(h)) = g(D_2)g(div(h)) = \\ = g(D_2)h(div(g)) = g(D_2)h(n(P) - n(\mathcal{O})) = \\ = g(D_2)\left(h((P) - (\mathcal{O}))\right)^n \equiv g(D_2) \pmod{(\mathbb{F}_{p^{k_t}}^*)^n}.\end{aligned}$$

□

The Tate pairing satisfies some properties similar to the Weil pairing:

THEOREM 8.16 (Properties of the Tate Pairing). *The Tate pairing satisfies the following properties:*

1. $\tau_n(\mathcal{O}, Q) = 1$ *for all* $Q \in E(\mathbb{F}_{p^{k_t}})$ *and* $\tau_n(P,Q) \in (\mathbb{F}_{p^{k_t}}^*)^n$ *for all* $P \in E(\mathbb{F}_{p^{k_t}})[n]$ *and all* $Q \in nE(\mathbb{F}_{p^{k_t}})$ *(well-defined).*
2. *For each point* $P \in E(\mathbb{F}_{p^{k_t}})[n] \setminus \mathcal{O}$ *there is some point* $Q \in E(\mathbb{F}_{p^{k_t}})$ *such that* $\tau_n(P,Q) \notin (\mathbb{F}_{p^{k_t}}^*)^n$ *(non-degeneracy).*
3. *For all* $P_1, P_2, P \in E(\mathbb{F}_{p^{k_t}})[n]$ *and* $Q_1, Q_2, Q \in E(\mathbb{F}_{p^{k_t}})$ *we have:*

$$\begin{aligned}\tau_n(P_1 + P_2, Q) &\equiv \tau_n(P_1, Q)\tau_n(P_2, Q) \\ \tau_n(P, Q_1 + Q_2) &\equiv \tau_n(P, Q_1)\tau_n(P, Q_2),\end{aligned}$$

i. e. the Tate pairing is bilinear (bilinearity).

PROOF. (1). Let $g \in \mathbb{F}_{p^{k_t}}(E)$ be the constant function that maps everything to 1; then $div(g) = 0$. Thus $\tau_n(\mathcal{O}, Q) = g(Q) = 1$ for all $Q \in E(\mathbb{F}_{p^{k_t}})$.

To prove the second part, let $P \in E(\mathbb{F}_{p^{k_t}})[n]$, $Q \in nE(\mathbb{F}_{p^{k_t}})$ and $g \in \mathbb{F}_{p^{k_t}}(E)$ be such that $div(g) = n(P) - n(\mathcal{O})$. Then there exists a point $Q' \in E(\mathbb{F}_{p^{k_t}})$ such that $[n]Q' = Q$. Let $D \sim (Q) - (\mathcal{O})$ and $D' \sim (Q') - (\mathcal{O})$, with support disjoint from the support of $div(g)$. Then

$$D - nD' \sim (Q) - (\mathcal{O}) - n(Q') + n(\mathcal{O}) = ([n]Q') - n(Q') + (n-1)(\mathcal{O}),$$

which is principal, i. e. $D = nD' + div(h)$ for some rational function h. Hence

$$\begin{aligned}\tau_n(P,Q) = g(D) = g(nD' + div(h)) = (g(D'))^n \cdot g(div(h)) = \\ = g^n(D')h(div(g)) = \left(g(D')h((P) - (\mathcal{O}))\right)^n \in (\mathbb{F}_{p^{k_t}}^*)^n.\end{aligned}$$

(2). For a proof see [**19, 28**].

(3). Let $P_1, P_2, P \in E(\mathbb{F}_{p^{k_t}})[n]$ and $Q_1, Q_2, Q \in E(\mathbb{F}_{p^{k_t}})$. We can write:

$$\tau_n(P_1 + P_2, Q) = g(D),$$

with $D \sim (Q) - (\mathcal{O})$, $div(g) = n(P_1 + P_2) - n(\mathcal{O})$ and $P_1, P_2, P_1 + P_2, \mathcal{O} \notin supp(D)$. Furthermore let g_1, g_2 be functions such that:

$$div(g_1) = n(P_1) - n(\mathcal{O}) \qquad div(g_2) = n(P_2) - n(\mathcal{O}).$$

The divisor $D' = (P_1 + P_2) - (P_1) - (P_2) + (\mathcal{O})$ is principal, i. e. $div(h) = D'$ for some function h. Hence

$$div(g) - div(g_1) - div(g_2) = n(P_1 + P_2) - n(P_1) - n(P_2) + n(\mathcal{O}) = \\ = n \cdot div(h) = div(h^n),$$

so that $g = g_1 g_2 h^n$. Thus

$$\tau_n(P_1 + P_2, Q) = g(D) = g_1(D) g_2(D) h^n(D) \equiv \\ \equiv \tau_n(P_1, Q)\tau_n(P_2, Q) \pmod{(\mathbb{F}^*_{p^{k_t}})^n},$$

and the pairing is linear in the first variable.

Moreover we can write:

$$\tau_n(P, Q_1 + Q_2) = g(D),$$

with $D \sim (Q_1 + Q_2) - (\mathcal{O})$ and $div(g) = n(P) - n(\mathcal{O})$ such that D and $div(g)$ have disjoint support. Choose the divisor D_1 and D_2 to be such that:

$$D_1 \sim (Q_1) - (\mathcal{O}) \qquad D_2 \sim (Q_2) - (\mathcal{O}),$$

with both D_1 and D_2 have disjoint support from $supp(div(g))$. Hence

$$D - D_1 - D_2 \sim (Q_1 + Q_2) - (Q_1) - (Q_2) + (\mathcal{O}),$$

which is principal, so that $D = D_1 + D_2 + div(h)$ for some rational function h. Finally

$$\tau_n(P, Q_1 + Q_2) = g(D) = g(D_1 + D_2 + div(h)) = g(D_1) g(D_2) g(div(h)) = \\ = g(D_1) g(D_2) h(div(g)) = \\ = \tau_n(P, Q_1)\tau_n(P, Q_2) h^n((P) - (\mathcal{O})) \equiv \\ \equiv \tau_n(P, Q_1)\tau_n(P, Q_2) \pmod{(\mathbb{F}^*_{p^{k_t}})^n},$$

and the pairing is linear in the second variable. □

The second part of properties (1) in the above theorem, is telling us that the Tate pairing is irrespective of which element of the particular coset is chosen for the second parameter; namely any element in $nE(\mathbb{F}_{p^{k_t}})$ will be mapped to $(\mathbb{F}^*_{p^{k_t}})^n$, and will therefore vanish in the quotient group $\mathbb{F}^*_{p^{k_t}} / (\mathbb{F}^*_{p^{k_t}})^n$.

Whereas the Weil pairing is such that $e_n(P, P) = 1$ for each $P \in E[n]$, the result of the Tate pairing $\tau_n(P, P)$ is not necessarily the identity in $\mathbb{F}^*_{p^{k_t}} / (\mathbb{F}^*_{p^{k_t}})^n$ (i. e. an n-th power). Often, in cryptographic applications, P is an n-torsion point ($P \in E(\mathbb{Z}_p)[n]$) and n is coprime to p. There is a lemma:

Lemma 8.17 (Galbraith[**23**]). *Let $P \in E(\mathbb{Z}_p)[n]$, with $P \neq \mathcal{O}$ and n coprime to p. Then for $\tau_n(P, P)$ to be non-trivial is necessary that $k_t = 1$.*

Proof. We have $\tau_n(P, P) = g(D)$, with $div(g) = n(P) - n(\mathcal{O})$ and $D \sim (P) - (\mathcal{O})$. Since $P \in E(\mathbb{Z}_p)[n]$, it follows that $g \in \varkappa(E) = \mathbb{Z}_p(E)$ and thus $g(D) \in \mathbb{Z}_p^*$. Now suppose $k_t > 1$, so that $n \nmid (p - 1)$. But n is coprime to p and

hence each element of $\mathbb{Z}_p^*$ is an n-th power, which implies $g(D) \in (\mathbb{F}_{p^{k_t}}^*)^n$. Thus to have $\tau_n(P,P)$ non-trivial a necessary condition is $k_t = 1$. □

Note that $k_t = 1$ is a necessary (and not a sufficient) condition. We derive a corollary:

Corollary 8.18. *Let $P \in E(\mathbb{Z}_p)[n]$, $P \neq \mathcal{O}$ and n be a prime. Let $k_t > 1$ and $Q \in E(\mathbb{F}_{p^{k_t}})[n]$ an n-torsion point independent from P. Then $\tau_n(P,Q)$ is non-trivial.*

Proof. Suppose that the result is trivial, i. e. $\tau_n(P,Q) \equiv 1$. Let $R \in E(\mathbb{F}_{p^{k_t}})$ and take the Tate pairing $\tau_n(P,R)$. As we have seen every coset in $E(\mathbb{F}_{p_t^k})/nE(\mathbb{F}_{p_t^k})$ contains an n-torsion point. Let R' be an n-torsion point that is in the same coset of R, so that $R = R' + [n]R''$ for some $R'' \in E(\mathbb{F}_{p^{k_t}})$. Thus $\tau_n(P,R) \equiv \tau_n(P,R')$. Moreover the group of n-torsion points is generated by P and Q which implies $R' = [a]P + [b]Q$, with $0 \leq a, b \leq n-1$. Hence, by lemma 8.17,

$$\tau_n(P,R) \equiv \tau_n(P,R') = \tau_n(P,[a]P + [b]Q) \equiv (\tau_n(P,P))^a(\tau_n(P,Q))^b \equiv 1.$$

But the Tate pairing is non-degenerate, so that $\tau_n(P,Q)$ must be non-trivial. □

8.6. Computation of the Pairings

In this section we show an algorithm suitable for an efficient computation of the Weil and Tate pairings. In section 8.2 we showed how to express a principal divisor as the divisor of a rational function f. This is all we need to evaluate the Weil and Tate pairings in theory; in practice, for larger examples, a little care is needed to avoid massive calculation.

Let us start with the Weil pairing; the algorithm we are going to describe is known as the Miller algorithm[**36, 34**] for the Weil pairing. Suppose that we want to evaluate $e_n(S,T)$ for the points $S, T \in E[n] \subseteq E(\mathbb{F}_{p^{k_w}})$. Choose points $S', T' \in E(\mathbb{F}_{p^{k_w}})$ such that $S', T', S+S'$ and $T+T'$ are all different. Then we set $D_S = (S+S') - (S')$ and $D_T = (T+T') - (T')$, so that the divisor

$$D_S - (S) + (\mathcal{O}) = (S+S') - (S') - (S) + (\mathcal{O}),$$

is clearly a principal divisor. Thus $D_S \sim (S) - (\mathcal{O})$ as required in the definition of the Weil pairing. In a similar fashion it is straightforward to see that $D_T \sim (T) - (\mathcal{O})$. Now we can use the method described in section 8.2 to compute $f_S, f_T \in \mathbb{F}_{p^{k_w}}(E)$ such that:

$$div(f_S) = n(S+S') - n(S') = nD_S$$
$$div(f_T) = n(T+T') - n(T') = nD_T.$$

Finally we evaluate the Weil pairing as:

$$e_n(S,T) = \frac{f_S(D_T)}{f_T(D_S)} = \frac{f_S((T+T')-(T'))}{f_T((S+S')-(S'))} = \\ = \frac{f_S(T+T')f_T(S')}{f_T(S+S')f_S(T')}.$$

The fact that the points $S+S'$ and S' are distinct from $T+T'$ and T' guarantees that f_S (respectively f_T) is, considered as a rational function, defined at $T+T'$ and T' (respectively $S+S'$ and S'). However, during the algorithm, we consider the functions f_S, f_T as elements of $\mathbb{F}_{p^{k_w}}[X,Y]$ rather than $\mathbb{F}_{p^{k_w}}(E)$. Thus we must choose the points S', T' in such a way that the function f_S (respectively f_T) is, even considered as an element of $\mathbb{F}_{p^{k_w}}[X,Y]$, defined at $T+T'$ and T' (respectively $S+S'$ and S'). Let us suppose that, in the computation of f_S and f_T we used a fixed addition chain $a_1 = 1, a_2, \cdots, a_t = n$ for n. Then, by construction, the function f_S, regarded as an element of $\mathbb{F}_{p^{k_w}}[X,Y]$, is undefined at most at the $4t$ points given by:

$$\pm[a_1](S+S'), \pm[a_2](S+S'), \cdots, \pm[a_t](S+S') \text{ and} \\ \pm[a_1](S'), \pm[a_2](S'), \cdots, \pm[a_t](S'). \tag{8.5}$$

Hence, if $T+T'$ and T' are different from the points listed above, we are sure that f_S is defined at $T+T'$ and T'. In a similar fashion, if $S+S'$ and S' are distinct from the points:

$$\pm[a_1](T+T'), \pm[a_2](T+T'), \cdots, \pm[a_t](T+T') \text{ and} \\ \pm[a_1](T'), \pm[a_2](T'), \cdots, \pm[a_t](T'), \tag{8.6}$$

then f_T, regarded as an element of $\mathbb{F}_{p^{k_w}}[X,Y]$, is defined at $S+S'$ and S'.

We now ask which is the probability of picking a random pair of points S', T' meeting these conditions. For fixed S', both $T+T'$ and T' must be distinct from the $4t$ points listed in (8.5), hence there are at most $8t$ unsuitable values for T'. In a similar fashion there are $8t$ unsuitable values for S'; it follows that the number of unsuitable pairs $(S', T') \in E(\mathbb{F}_{p^{k_w}}) \times E(\mathbb{F}_{p^{k_w}})$ is at most $16t \cdot \#E(\mathbb{F}_{p^{k_w}})$, which yields:

$$\frac{16t \cdot \#E(\mathbb{F}_{p^{k_w}})}{\left(\#E(\mathbb{F}_{p^{k_w}})\right)^2} = \frac{16t}{\#E(\mathbb{F}_{p^{k_w}})} \leq \frac{32 \cdot \log_2(n)}{\#E(\mathbb{F}_{p^{k_w}})},$$

since for every value of n there exists an addition chain of length $t \leq 2\log_2(n)$. Note that $\#E(\mathbb{F}_{p^{k_w}}) \geq n$, so that this probability is less than $\frac{1}{2}$ for $n \geq 1024$.

Example 8.11. We refer to our usual example $E: Y^2 = X^3 + 3X$. We could compute the Weil pairing of two n-torsion points of $E(\mathbb{Z}_{11})$; however it is easy to check that the group structure of $E(\mathbb{Z}_{11})$ is cyclic, i. e. all points are

linearly dependent. Thus, by bilinearity of the pairing and since $e_n(P,P) = 1$ for all $P \in E[n]$, the Weil pairing will map everything to 1. For example:

$$e_6(P_3, P_6) = e_6(P_3, [4]P_3) = (e_6(P_3, P_3))^4 = 1.$$

Consider instead the points of E over $\mathbb{F}_{11^2}$, which is obtained by taking the primitive fourth root of unity i (i. e. $i^2 = -1$). One can easily check that if $(x, y) \in E(\mathbb{F}_{11^2})$, then also $(-x, iy) \in E(\mathbb{F}_{11^2})$. Thus there is an endomorphism:

$$\begin{aligned} \Phi : \ E(\mathbb{F}_{11^2}) &\longrightarrow E(\mathbb{F}_{11^2}) \\ (x, y) &\mapsto (-x, iy). \end{aligned}$$

Clearly the image of a point P, namely $\Phi(P)$, is not a point of $E(\mathbb{Z}_{11})$, i. e. $\Phi(P) \notin E(\mathbb{Z}_{11})$. Moreover if P is an n-torsion point, i. e. $[n]P = \mathcal{O}$, $\Phi(P)$ is an n-torsion point too, since:

$$[n]\Phi(P) = \Phi([n]P) = \Phi(\mathcal{O}) = \mathcal{O}.$$

Thus it makes sense to evaluate $e_n(P, \Phi(P))$ and the result will be non-trivial. Take, for example, the points $S = P_6 = (3, 5)$ and $T = \Phi(P_6) = (8, 5i)$, both with order 3. We choose $S' = (6, 6)$ and $T' = (9, 6i)$ so that $S + S' = (7, 1)$ and $T + T' = (4, 10i)$; note that $S', S + S', T'$ and $T + T'$ are all different. To evaluate $e_3(S, T)$ we need rational functions f_S and f_T such that:

$$div(f_S) = 3(S + S') - 3(S') \quad div(f_T) = 3(T + T') - 3(T').$$

Using the method described in section 8.2 we compute:

$$\begin{aligned} 3(S + S') - 3(\mathcal{O}) &= ((6, 5)) - (\mathcal{O}) + \\ &\quad + div\left(\frac{(Y + 2X + 7)(Y + 5X + 8)}{(X + 10)(X + 5)}\right) \\ 3(S') - 3(\mathcal{O}) &= ((6, 5)) - (\mathcal{O}) + div\left(\frac{(Y + 10X)^2}{X(X + 5)}\right), \end{aligned}$$

which yields:

$$3(S + S') - 3(S') = div\left(\frac{X(Y + 2X + 7)(Y + 5X + 8)}{(X + 10)(Y + 10X)^2}\right).$$

In a similar fashion:

$$\begin{aligned} 3(T + T') - 3(\mathcal{O}) &= ((5, 6i)) - (\mathcal{O}) + \\ &\quad + div\left(\frac{(Y + 2iX + 4i)(Y + 5iX + 3i)}{(X + 1)(X + 6)}\right) \\ 3(T') - 3(\mathcal{O}) &= ((5, 6i)) - (\mathcal{O}) + \\ &\quad + div\left(\frac{(Y + 4iX + 2i)(Y + 8iX + 10i)}{(X + 1)(X + 6)}\right), \end{aligned}$$

which yields:

$$3(T + T') - 3(T') = div\left(\frac{(Y + 2iX + 4i)(Y + 5iX + 3i)}{(Y + 4iX + 2i)(Y + 8iX + 10i)^2}\right).$$

So we have determined:

$$f_S(X,Y) = \frac{X(Y+2X+7)(Y+5X+8)}{(X+10)(Y+10X)^2}$$
$$f_T(X,Y) = \frac{(Y+2iX+4i)(Y+5iX+3i)}{(Y+4iX+2i)(Y+8iX+10i)^2}.$$

Finally:

$$e_3(P_6,\Phi(P_6)) = \frac{f_S(T+T')f_T(S')}{f_S(T')f_T(S+S')} = \\ = \frac{f_S((4,10i))f_T((6,6))}{f_S((9,6i))f_T((7,1))} = 5+8i.$$

Indeed $(5+8i)^3 = 1$ and the result is, as expected, a third root of unity in $\mathbb{F}_{11^2}$. Note that, as we have already observed, we do not need to work over the full algebraic closure of the finite field $\mathbb{Z}_{11}$; in particular, in this case, a field extension $\mathbb{F}_{11^2}$ of order 2 suffices to evaluate the pairing. The endomorphism Φ that maps a point to a linearly independent point of the same order, is called a *distorsion map*. □

Now we deal with the computation of the Tate pairing using Miller's algorithm[**6, 34, 36**]. For each point pair (P,Q) of an elliptic curve $E(\mathbb{F}_{p_t^k})$, we denote with $\Omega_{P,Q} \in \mathbb{F}_{p^{k_t}}(E)$ the rational function given by the line $Y-\alpha X-\beta$ through the points P and Q. In particular, when $P=Q$, $\Omega_{P,Q}$ is the line tangent to the curve in P and if either P or Q is the point at infinity, $\Omega_{P,Q}$ represents the vertical line through the other point. Finally we denote with Ω_P the vertical line $X-\gamma$ through P and $-P$. The key ingredient is given by the following lemma:

Lemma 8.19 (Miller's Formula). *Let $P \in E(\mathbb{F}_{p^{k_t}})$ and f_j be a rational function such that $div(f_j) = j(P) - ([j]P) - (j-1)(\mathcal{O})$, with $j \in \mathbb{Z}$. Then for all $a,b \in \mathbb{Z}$ the following holds:*

$$f_{a+b}(P) = f_a(P)\cdot f_b(P)\cdot \frac{\Omega_{[a]P,[b]P}(P)}{\Omega_{[a+b]P}(P)}.$$

Proof. The divisors of the line functions satisfy:

$$div(\Omega_{[a]P,[b]P}) = ([a]P)+([b]P)+(-[a+b]P)-3(\mathcal{O})$$
$$div(\Omega_{[a+b]P}) = ([a+b]P)+(-[a+b]P)-2(\mathcal{O})$$
$$\Rightarrow \quad div(\Omega_{[a]P,[b]P}) - div(\Omega_{[a+b]P}) = ([a]P)+([b]P)-([a+b]P)-(\mathcal{O}).$$

Hence using the definition of f_j:

$$div(f_{a+b}) = (a+b)(P)-([a+b]P)-(a+b-1)(\mathcal{O}) = \\ = a(P)-([a]P)-(a-1)(\mathcal{O})+b(P)-([b]P)-(b-1)(\mathcal{O})+ \\ +([a]P)+([b]P)-([a+b]P)-(\mathcal{O}) = \\ = div(f_a)+div(f_b)+div(\Omega_{[a]P,[b]P})-div(\Omega_{[a+b]P}),$$

which yields the assertion[5]:

$$f_{a+b}(P) = f_a(P) \cdot f_b(P) \cdot \frac{\Omega_{[a]P,[b]P}(P)}{\Omega_{[a+b]P}(P)}.$$

□

Recall that to evaluate the Tate pairing $\tau_n(P,Q)$, we need a rational function g such that $div(g) = n(P) - n(\mathcal{O})$ for $P \in E(\mathbb{F}_{p^{k_t}})[n]$. Since P is an n-torsion point (i. e. $[n]P = \mathcal{O}$), we can write $g = f_n$, with f_n as in lemma 8.19:

$$div(f_n) = n(P) - ([n]P) - (n-1)(\mathcal{O}) = n(P) - n(\mathcal{O}) = div(g).$$

Since $div(f_1) = 0$ we choose $f_1 = 1$, so that, for $a > 0$ we can write:

$$f_{a+1} = f_a \cdot \frac{\Omega_{[a]P,P}}{\Omega_{[a+1]P}} \tag{8.7}$$

$$f_{2a} = (f_a)^2 \cdot \frac{\Omega_{[a]P,[a]P}}{\Omega_{[2a]P}}. \tag{8.8}$$

Let $(n_s, \cdots, n_1, n_0)_2$ be the binary representation of n, with $n_i \in \{0,1\}$ for $i = 0, \cdots, s-1$ and $n_s = 1$. Starting with $f_{(n_s)_2} = f_1 = 1$ we now successively evaluate $f_{(n_s,\cdots,n_i)_2}$ from $f_{(n_s,\cdots,n_{i+1})_2}$ using first equation (8.8) and then equation (8.7) if $n_i = 1$ (double-and-add) and only equation (8.8) if $n_i = 0$. This is because:

$$(n_s, \cdots, n_{i+1}, n_i)_2 = \begin{cases} 2 \cdot (n_s, \cdots, n_{i+1})_2 + 1 & \text{if } n_i = 1 \\ 2 \cdot (n_s, \cdots, n_{i+1})_2 & \text{if } n_i = 0. \end{cases}$$

The result will be the desired function $g = f_n = f_{(n_s,\cdots,n_0)_2}$ with $div(g) = n(P) - n(\mathcal{O})$.

Now we should evaluate the function g at a divisor $D \sim (Q) - (\mathcal{O})$; take for instance $D = (Q + Q') - (Q')$, being $Q' \in E(\mathbb{F}_{p^{k_t}})$ and hence $\tau_n(P,Q) = g(D) = \frac{g(Q+Q')}{g(Q')}$. Instead of first computing $g = f_n$ and then evaluating $g(D)$,

[5] It is interesting to note that the above formula is a special case of the method for adding two divisors in canonical form we explained in section 8.2. In fact let divisors D_1 and D_2 be given by $D_1 = a(P) - a(\mathcal{O})$ and $D_2 = b(P) - b(\mathcal{O})$ respectively; thus their canonical form is:

$$D_1 = ([a]P) - (\mathcal{O}) + div(f_a)$$
$$D_2 = ([b]P) - (\mathcal{O}) + div(f_b),$$

where f_a and f_b are as in lemma 8.19. Thus we can express their sum $D_1 + D_2 = (a+b)(P) - (a+b)(\mathcal{O})$ in canonical form like:

$$(a+b)(P) - (a+b)(\mathcal{O}) = ([a+b]P) - (\mathcal{O}) + div\left(f_a \cdot f_b \cdot \frac{\Omega_{[a]P,[b]P}}{\Omega_{[a+b]P}}\right),$$

where $\frac{\Omega_{[a]P,[b]P}}{\Omega_{[a+b]P}}$ is denoted by $f_3 = \frac{r}{r'}$ in equation (8.3). Finally, bringing the term $([a+b]P) - (\mathcal{O})$ to the left we can write:

$$div(f_{a+b}) = div(f_a) + div(f_b) + div(\Omega_{[a]P,[b]P}) - div(\Omega_{[a+b]P}),$$

which underlies lemma 8.19.

it is more efficient to do the evaluation along the way. In particular it suffices to use the formulas:

$$f_{a+1}(D) = \frac{f_{a+1}(Q+Q')}{f_{a+1}(Q')} = f_a(D) \cdot \frac{\Omega_{[a]P,P}(Q+Q')\Omega_{[a+1]P}(Q')}{\Omega_{[a]P,P}(Q')\Omega_{[a+1]P}(Q+Q')} \tag{8.9}$$

$$f_{2a}(D) = \frac{f_{2a}(Q+Q')}{f_{2a}(Q')} = (f_a(D))^2 \cdot \frac{\Omega_{[a]P,[a]P}(Q+Q')\Omega_{[2a]P}(Q')}{\Omega_{[a]P,[a]P}(Q')\Omega_{[2a]P}(Q+Q')}. \tag{8.10}$$

Example 8.12. We consider again the curve $E:\ Y^2 = X^3 + 3X$ over $\mathbb{Z}_{11}$. The Tate embedding degree k_t of the curve with respect to 6 is clearly $k_t = 2$ since $6|(11^2-1)$ but $6 \nmid (11-1)$. Then we evaluate $\tau_n(P,Q)$ for $P = (1,9)$, $Q = (\Phi(P)) = (10, 9i)$ and $n = 6$ using Miller's algorithm.

First of all we choose a point $Q' \in E(\mathbb{F}_{11^2})$, for instance $Q' = (6,6)$ and we compute $S = Q + Q' = (8+7i, 10+6i)$. Then we compute $s = \lfloor \log_2(n) \rfloor = 2$ and we write the binary representation of n, namely $n = 6 = (n_2, n_1, n_0)_2 = (1,1,0)_2$.

Now we enter in the loop phase of the algorithm; we start with $f_{(1)_2} = f_1 = 1$ and we evaluate $f_{(11)_2}(D)$ using equations (8.9) and (8.10). Since $n_{s-1} = n_1 = 1$ we are in the double-and-add case, thus we first compute the lines:

$$\Omega_{P,P}:\ Y + 7X + 6 \quad \text{and} \quad \Omega_{[2]P}:\ X + 8$$

Hence we double, using equation (8.10) with $a = 1$,

$$f_2(D) = (1)^2 \cdot \frac{(Y+7X+6)|_S \cdot (X+8)|_{Q'}}{(Y+7X+6)|_{Q'} \cdot (X+8)|_S} = \frac{6 \cdot 3}{(5+7i)\cdot 10} = 8 + 2i,$$

and add, using equation (8.9) with $a = 2$. Thus we first evaluate the lines:

$$\Omega_{[2]P,P}:\ Y + 2X \quad \text{and} \quad \Omega_{[3]P}:\ X,$$

and finally

$$f_{(11)_2} = f_3(D) = f_{2+1}(D) = f_2(D) \cdot \frac{(Y+2X)|_S \cdot (X)|_{Q'}}{(Y+2X)|_{Q'} \cdot (X)|_S} =$$
$$= (8+2i) \cdot \frac{(4+9i)\cdot 6}{(8+7i)\cdot 7} = 5 + 4i.$$

The last step is the computation of $g(D) = f_n(D) = f_{(110)_2}(D) = f_6(D)$ from the knowledge of $f_3(D)$. Since $n_{s-2} = n_0 = 0$ we need only to double using equation (8.10) with $a = 3$. Thus we first compute the lines:

$$\Omega_{[3]P,[3]P} = \Omega_{(0,0),(0,0)}:\ X \quad \text{and} \quad \Omega_{[6]P}:\ 1.$$

Hence we double,

$$\tau_6(P,Q) = g(D) = f_6(D) = f_{3\cdot 2}(D) = (f_3(D))^2 \cdot \frac{(X)|_S \cdot (1)|_{Q'}}{(X)|_{Q'} \cdot (1)|_S} =$$
$$= (5+4i)^2 \cdot \frac{8+7i}{6} = 2 + 7i.$$

The result of the evaluation is $2+7i \in \mathbb{F}^*_{11^2}/(\mathbb{F}^*_{11^2})^6$, that is an equivalence class modulo 6-th powers. If a unique value of the pairing is required, we should raise the result to the power $(p^{k_t}-1)/n = (11^2-1)/6 = 20$ which yields $(2+7i)^{20} = 5+3i$. Indeed $5+3i$ is a 6-th root of unity in $\mathbb{F}^*_{11^2}$, since $(5+3i)^6 = 1$; nevertheless it is possible that the outcome of the Tate pairing is not a *primitive* root of unity, since 6 is not a prime. This is, in fact, the case, being $(5+3i)^3 = 1$ too. □

Since the Weil and Tate pairings are defined over different sets, it could seem that there is not an algebraic relation between the two definitions. However, when we take Q in the n-torsion and regard the outcome of the Weil pairing as an element of $\mathbb{F}^*_{p^{k_t}}/(\mathbb{F}^*_{p^{k_t}})^n$, we find a relation:

THEOREM 8.20. *Let P and Q be n-torsion points; the following holds:*

$$(e_n(P,Q))^{\frac{p^{k_t}-1}{n}} = \left(\frac{\tau_n(P,Q)}{\tau_n(Q,P)}\right)^{\frac{p^{k_t}-1}{n}}.$$

PROOF. The Tate pairing is defined as $\tau_n(P,Q) = g_P(D_Q)$, where $div(g_P) = n(P) - n(\mathcal{O})$ and $D \sim (Q) - (\mathcal{O})$ with $supp(D) \cap supp(div(g_P)) = \emptyset$. Typically one can choose $D = (Q+Q') - (Q')$, for $Q' \in E(\mathbb{F}_{p_t^k})$ such that $Q', Q+Q' \neq P, \mathcal{O}$. Hence:

$$\tau_n(P,Q) = \frac{g_P(Q+Q')}{g_P(Q')}.$$

In a similar fashion:

$$\tau_n(Q,P) = \frac{g_Q(P+P')}{g_Q(P')},$$

where $div(g_Q) = n(Q) - n(\mathcal{O})$ and $P' \in E(\mathbb{F}_{p^{k_t}})$ with $P', P+P' \neq Q, \mathcal{O}$. On the other hand the Weil pairing is:

$$e_n(P,Q) = \frac{f_P(Q+Q')f_Q(P')}{f_P(Q')f_Q(P+P')},$$

where f_P and f_Q are such that $div(f_P) = n(P+P') - n(P')$ and $div(f_Q) = n(Q+Q') - n(Q')$. It is easy to check that $(P+P') - (P') - (P) + (\mathcal{O})$ is a principal divisor, thus we can write

$$div(h_P) = (P+P') - (P') - (P) + (\mathcal{O}),$$

and similarly

$$div(h_Q) = (Q+Q') - (Q') - (Q) + (\mathcal{O}).$$

Thus

$$div(f_P) = n((P+P') - (P')) = ndiv(h_P) + div(g_P) = div(h_P^n g_P)$$
$$div(f_Q) = n((Q+Q') - (Q')) = ndiv(h_Q) + div(g_Q) = div(h_Q^n g_Q)$$
$$\Rightarrow \quad f_P = h_P^n g_P \qquad f_Q = h_Q^n g_Q.$$

Hence the Weil pairing is:

$$e_n(P,Q) = \frac{h_P^n(Q+Q')g_P(Q+Q')}{h_P^n(Q')g_P(Q')}\frac{h_Q^n(P')g_Q(P')}{h_Q^n(P+P')g_Q(P+P')} =$$
$$= \left(\frac{h_P(Q+Q')h_Q(P')}{h_P(Q')h_Q(P+P')}\right)^n \frac{g_P(Q+Q')}{g_P(Q')}\frac{g_Q(P')}{g_Q(P+P')}.$$

Note that the term in parenthesis is an element of $(\mathbb{F}^*_{p^{k_t}})^n$ and therefore vanishes in the quotient group $\mathbb{F}^*_{p^{k_t}}/(\mathbb{F}^*_{p^{k_t}})^n$. Thus, regarded as an element of this quotient group, the Weil pairing can be written as

$$e_n(P,Q) \equiv \frac{g_P(Q+Q')}{g_P(Q')}\frac{g_Q(P')}{g_Q(P+P')} = \frac{\tau_n(P,Q)}{\tau_n(Q,P)} \pmod{(\mathbb{F}^*_{p^{k_t}})^n}.$$

By raising both sides to the power $\frac{p^{k_t}-1}{n}$ we obtain the assertion:

$$(e_n(P,Q))^{\frac{p^{k_t}-1}{n}} = \left(\frac{\tau_n(P,Q)}{\tau_n(Q,P)}\right)^{\frac{p^{k_t}-1}{n}}.$$

□

Example 8.13. In a previous example we have evaluated the Tate pairing $(\tau_6(P,Q))^{20} = 5+3i$ on the curve $E: Y^2 = X^3 + 3X$ and with $P = (1,9)$, $Q = (10, 9i)$. Similarly we can compute the Tate pairing $\tau_6(Q,P)$ which is the equivalence class of $1+2i \in \mathbb{F}^*_{11^2}/(\mathbb{F}^*_{11^2})^6$. Raising to the power 20 we obtain the unique value $(1+2i)^{20} = 5+8i$. Further, using Miller's algorithm, it is easy to check that $e_6(P,Q) = 5+3i$ and

$$\left(\frac{\tau_6(P,Q)}{\tau_6(Q,P)}\right)^{20} = 5+8i = (e_6(P,Q))^{20},$$

as we expected to be. □

This relation suggests that that the computation of the Weil pairing takes roughly twice as long as the computation of the Tate pairing. This can be verified if we look at the algorithms described in this section. To evaluate $e_n(P,Q)$ we need to find functions f_P and f_Q such that $div(f_P) \sim n(P) - n(\mathcal{O})$ and $div(f_Q) \sim n(Q) - n(\mathcal{O})$, hence we have to compute these functions in $D_Q \sim (Q) - (\mathcal{O})$ and $D_P \sim (P) - (\mathcal{O})$ respectively. The Tate pairing, on the other hand, requires only a function g such that $div(g) = n(P) - n(\mathcal{O})$ to be computed at $D \sim (Q) - (\mathcal{O})$. Moreover we can look for the function g efficiently using the double-and-add method described above, in contrast to f_P and f_Q. Hence the computation of the Weil pairing takes at least twice the running-time for the Tate pairing. Lastly, there are a lot of adaptation and ad-hoc choices of parameters for the algorithm which speeds up the computation efficiency of the Tate pairing[**33**].

Pairing-based Cryptography is the use of pairings for cryptographic purposes. While first used for cryptanalysis, pairings have since been used

to construct many cryptographic systems for which no other efficient implementation is known, such as *identity based encryption*. Identity-based cryptosystems are a type of public-key cryptosystems in which the public key of a user is some unique information about the identity of the user (e. g.. a user's email address); this property solve one of the most thorny problem in public-key cryptography, namely the authenticity of public keys. Although the original idea[**41**] of identity-based cryptography has more than 30 years, the implementation of such a cryptosystem was an open problem until 2001, when Boneh and Franklin proposed a solution based on pairings[**8**] and Cocks[**13**] presented a solution based on the quadratic residuosity problem.

APPENDIX A

Prime Number Theorem

The *Prime Number Theorem* is a deep result in number theory which deals with the distribution of prime numbers. Let $\pi(n)$ be the number of prime integers less than or equal to n, i. e.

$$\pi(n) = \#\{\text{primes } p : p \leq n\}.$$

The statement is as follows:

THEOREM A.1 (Prime Number Theorem[**2**]). *We have:*

$$\lim_{n\to+\infty} \frac{\pi(n)\log(n)}{n} = 1$$

□

Consequently, if n is sufficiently large, $\pi(n) \approx \frac{n}{\log(n)}$, i. e. we can estimate the number of primes in a given interval $[1, n]$ with good accuracy. In other words:

$$\frac{\#\{p \leq X : \ p \text{ is prime}\}}{X} \approx \frac{1}{\log(X)},$$

being X an integer. Often one need to know the probability that an integer near X is prime. The following corollary shows that this probability is the same as in equation above:

COROLLARY A.2. *The probability that an integer $\approx X$ is prime is still $\frac{1}{\log(X)}$.*

PROOF. Let us consider a neighbourhood of X, namely

$$\mathcal{I} = [X - \Theta, X + \Theta],$$

with $\Theta \ll X$. We use the Prime Number Theorem to evaluate the number of primes in $\mathcal{I}$:

$$\begin{aligned}
&\#\{\text{primes } p \text{ in } \mathcal{I}\} = \pi(X+\Theta) - \pi(X-\Theta) = \\
&= \frac{X+\Theta}{\log(X+\Theta)} - \frac{X-\Theta}{\log(X-\Theta)} \\
&= X\left(\frac{1}{\log(X+\Theta)} - \frac{1}{\log(X-\Theta)}\right) + \Theta\left(\frac{1}{\log(X+\Theta)} + \frac{1}{\log(X-\Theta)}\right) \\
&= [\log(X+\Theta) + \log(X-\Theta) \approx 2\log(X) \text{ since } \Theta \ll X] \\
&\approx X\left(\frac{1}{\log(X+\Theta)} - \frac{1}{\log(X-\Theta)}\right) + \Theta \cdot \frac{2\log(X)}{\log(X+\Theta)\log(X-\Theta)}
\end{aligned}$$

$$
\begin{aligned}
&= X\left(\frac{\log\left(1-\frac{\Theta}{X}\right)-\log\left(1+\frac{\Theta}{X}\right)}{\log(X+\Theta)\log(X-\Theta)}\right)+\Theta\cdot\frac{2\log(X)}{\log(X+\Theta)\log(X-\Theta)}\\
&= [\log(1+\epsilon)\approx\epsilon \text{ if } \epsilon \text{ is small}]\\
&\approx X\cdot\frac{-2\frac{\Theta}{X}}{\log(X+\Theta)\log(X-\Theta)}+\Theta\cdot\frac{2\log(X)}{\log(X+\Theta)\log(X-\Theta)}\\
&\approx \frac{2\Theta}{\log^2(X)}+\frac{2\Theta}{\log(X)}\approx\frac{2\Theta}{\log(X)}.
\end{aligned}
$$

Note that 2Θ is the number of element in $\mathcal{I}$, so that the probability that an integer $\approx X$ is prime is:

$$\frac{\#\{\text{primes } p \text{ in } \mathcal{I}\}}{2\Theta}\approx\frac{1}{\log(X)}.$$

□

In the following we prove a weak form of the Prime Number Theorem:

THEOREM A.3 (Chebyshev). *$\exists\, c_1, c_2 > 0$ such that:*

$$c_1\frac{n}{\log(n)} < \pi(n) < c_2\frac{n}{\log(n)}$$

with $c_1 = \frac{1}{2}$ e $c_2 = 4$. □

The proof is quite simple, but we need a couple of preliminary remarks. Let $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ be the *binomial coefficient*; the key observation is that:

$$\binom{2m}{m} = \frac{(2m)!}{(m!)^2} = \frac{2m(2m-1)(2m-2)\cdots 2\cdot 1}{m\cdot m(m-1)(m-1)\cdots 2\cdot 2\cdot 1\cdot 1}$$

is divisible by all primes p such that $m < p < 2m$, because the numerator is divisible by all primes $p < 2m$, but the term in the denominator cancels all primes $p \le m$. Recall the expression for the *Newton's binomial*

$$(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k,$$

we can observe that:

$$(1+1)^n = 2^n = \sum_{k=0}^{n}\binom{n}{k}$$

$$\Rightarrow \quad \binom{n}{k}\le 2^n.$$

Hence:

$$\prod_{m<p\le 2m} p \le \binom{2m}{m} \le 2^{2m}. \tag{A.1}$$

Similarly:

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m!(m+1)!}$$
$$\Rightarrow \prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m} \leq 2^{2m}$$

and the last inequality comes from the fact that

$$\binom{2m+1}{m} = \binom{2m+1}{m+1} \quad \text{and} \quad \binom{2m+1}{m} + \binom{2m+1}{m+1} \leq 2^{2m+1}$$
$$\Rightarrow \quad 2\binom{2m+1}{m} \leq 2^{2m+1} \Rightarrow \binom{2m+1}{m} \leq 2^{2m}.$$

We are ready to prove the following lemma:

Lemma A.4. *$\forall n \in \mathbb{Z}_{>0}$ we have:*

$$\prod_{p\leq n} p \leq 4^n$$

Proof. We use induction on n. The basis of induction is right since

$$n = 1 \qquad \Rightarrow \qquad 1 \leq 4.$$

Suppose now that the statement holds for all integers up to $n-1$ (induction hypothesis), we show it holds for n too. If $n = 2m$ is even:

$$\prod_{p\leq n} p = \prod_{p\leq m} p \prod_{m<p\leq 2m} p \leq 4^m \frac{4^{2m}}{4^m} = 4^{2m} = 4^n$$

as desired. If $n = 2m+1$ is odd:

$$\prod_{p\leq n} p = \prod_{p\leq m+1} p \prod_{m+1<p\leq 2m+1} p \leq 4^{m+1} \frac{4^{2m+1}}{4^{m+1}} = 4^{2m+1} = 4^n$$

and the assertion is proven. □

There is a (more recent) stronger version of lemma A.4 in which we have Euler's number e in place of number 4. As we will see the lemma just proven will be crucial in the proof of one of the inequalities in the Chebyshev relation; to prove the other direction we need another couple of observations.

Consider $n!$, it is clear that it is divisible by all primes $p \leq n$, whereas it is not divisible by all primes $p > n$. We ask which is the power of a prime p in the factorization of $n!$. Here the key observation is that between the numbers $1, 2, \ldots, n$ *exactly* $\left\lfloor \frac{n}{p^k} \right\rfloor$ are divisible by p^k, $\forall k \in \mathbb{Z}_{>0}$. For example one can check that for $n = 100$ there are exactly $14 = \left\lfloor \frac{100}{7} \right\rfloor$ numbers in $1, 2, \ldots, n$ divisible by $p = 7$ and $2 = \left\lfloor \frac{100}{7^2} \right\rfloor$ divisible by $p^2 = 49$ (i. e. 49 and 88). As $n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$, we have $14 + 2 = 16$ factors divisible by

$p = 7$ in the factorization of $n!$ and we can conclude that the power of 7 in 100! is 16. We have the following proposition:

PROPOSITION A.5. *The exact power of a prime p in $n!$ is:*

$$\sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

PROOF. Let $v_p(\cdot)$ denote the p-adic valuation[1]; we want to prove

$$v_p(n!) = \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

We write

$$v_p(n!) = \sum_{m \leq n} v_p(m) = \sum_{m \leq n} \sum_{1 \leq k \leq v_p(m)} 1 = \sum_{k=1}^{\infty} \sum_{\substack{m \leq n \\ v_p(m) \leq k}} 1.$$

Since the inner sum equals the number of integers $m \leq n$ which are divisible by p^k, it has value $\left\lfloor \frac{n}{p^k} \right\rfloor$, as desired. □

We point out that the sum is formally an infinite series, but every k such that $p^k > n$ gives zero as contribution. Therefore we can conclude that the power of the prime p in the factorization of $\binom{n}{m} = \frac{n!}{m!(n-m)!}$ is:

$$\sum_{k=1}^{+\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{n-m}{p^k} \right\rfloor \right) =$$

= [We suppose $n = 2m + 1$ is odd, but for even n the proof is similar]

$$= \sum_{k=1}^{+\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor - \left\lfloor \frac{m+1}{p^k} \right\rfloor \right).$$

Note that each terms of the sum is less than 1 and that the number of terms not equal to zero is less than or equal to $\left\lfloor \log_p n \right\rfloor$ that is 1 when $\sqrt{n} < p \leq n$. Now we are ready to prove the following lemma:

LEMMA A.6. *$\forall n \in \mathbb{Z}_{>0}$ we have:*

$$\prod_{p \leq n} p \geq \frac{2^n}{(n+1)n^{\sqrt{n}}}.$$

[1]That is to say v_p is the arithmetic function which associates to each integer n the exponent of p in its canonical factorization.

Proof. On the one hand:

$$\begin{aligned}\binom{n}{m} &\leq \prod_{\sqrt{n}<p\leq n} p \prod_{p\leq\sqrt{n}} p^{\left\lfloor \log_p n\right\rfloor} \\ &\leq \prod_{p\leq n} p\cdot n^{\pi(\sqrt{n})} \leq n^{\sqrt{n}} \prod_{p\leq n} p.\end{aligned}$$

On the other hand:

$$\begin{aligned}(1+1)^n = 2^n = \sum_{m=0}^{n}\binom{n}{m} &\leq (n+1)\binom{n}{m} \\ \Rightarrow \qquad \frac{2^n}{n+1} &\leq \binom{n}{m} \leq \prod_{p\leq n} p\cdot n^{\sqrt{n}} \\ \Rightarrow \qquad \prod_{p\leq n} p &\geq \frac{2^n}{(n+1)n^{\sqrt{n}}}.\end{aligned}$$

□

Finally we are ready to give the proof of theorem A.3:

Proof. Using lemma A.4 we can write:

$$\sum_{p\leq n}\log p \leq n\log 4 \quad \Rightarrow \quad \sum_{\sqrt{n}<p<n}\log p \leq n\log 4.$$

Furthermore:

$$\begin{aligned}\sum_{\sqrt{n}<p<n}\log p &\geq \sum_{\sqrt{n}<p<n}\log(\sqrt{n}) = \log(\sqrt{n})\left(\pi(n)-\pi(\sqrt{n})\right) \\ \Rightarrow \qquad \frac{1}{2}\log n\left(\pi(n)-\pi(\sqrt{n})\right) &\leq \sum_{\sqrt{n}<p<n}\log p \leq n\log 4 \\ \Rightarrow \qquad \pi(n) \leq 2\log 4\frac{n}{\log n} + \pi(\sqrt{n}) &\leq 2\log 4\frac{n}{\log n} + \sqrt{n} < 4\frac{n}{\log n}\end{aligned}$$

and we have proven the right inequality. Using lemma A.6:

$$\begin{aligned}\sum_{p\leq n}\log p &\geq n\log 2 - \log(n+1) - \sqrt{n}\log n > \frac{1}{2}n \\ \Rightarrow \qquad \sum_{p\leq n}\log p &\leq \sum_{p\leq n}\log n \leq \pi(n)\log n \\ \Rightarrow \qquad \pi(n) &\geq \frac{1}{2}\frac{n}{\log n}.\end{aligned}$$

□

We have also the following corollary:

Corollary A.7. *Chebyshev's relation of theorem A.3 implies:*

$$\frac{1}{2} \leq \lim_{n\to+\infty} \frac{\pi(n)\log n}{n} \leq 4.$$

□

Further, assuming the Riemann hypothesis (see appendix D), one can show:

$$\pi(n) = Li(n) + O(\sqrt{n}\log n),$$

where

$$Li(x) = \int_2^x \frac{1}{\log \xi}\, d\xi.$$

Let $X \in \mathbb{R}_{>0}$; we close this section drawing an estimate for $\sum_{p<X} \frac{1}{p}$ (being p a prime). We need a couple of lemmas:

Lemma A.8. *We can write*

$$\sum_{\substack{p<X \\ p \text{ primes}}} \log(p) = O(X) \quad (X \to \infty).$$

Proof. Recall that by equation (A.1) we can write $\prod_{m<p\leq 2m} p \leq 4^m$. Further let $s \in \mathbb{Z}$ be the unique integer such that $2^{s-1} < X \leq 2^s$; hence

$$\prod_{p\leq X} p \leq \prod_{p\leq 2^s} p \leq 4^{2^s+2^{s-1}+\cdots} < 4^{2^{s+1}} \leq 4^{4X}.$$

The assertion follows taking the logarithm of both sides. □

Lemma A.9. *We can write*

$$\sum_{\substack{p<X \\ p \text{ primes}}} \frac{\log(p)}{p} = \log(X) + O(1) \quad (X \to \infty).$$

Proof. Recall that proposition A.5 yields

$$n! = \prod_{\substack{p<n \\ p \text{ primes}}} p^{a_p}, \quad \text{where } a_p = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] < \frac{n}{p-1}.$$

Taking the logarithm of both sides we can write

$$\sum_{p\leq n} \left(\frac{n}{p} - 1\right) \log(p) \leq \log(n!) \leq \sum_{p\leq n} \frac{n}{p-1} \log(p),$$

and hence

$$n \sum_{p\leq n} \frac{\log(p)}{p} - \sum_{p\leq n} \log(p) \leq \log(n!) \leq n \sum_{p\leq n} \frac{\log(p)}{p} + n \sum_{p\leq n} \frac{\log(p)}{p(p-1)}.$$

Using lemma A.8 we have $\sum_{p\leq n}\log(p) = O(n)$. Further, since one can show that the integral $\int_2^\infty \frac{\log(t)\,dt}{t(t-1)}$ converges, we can conclude that $\sum_{p\leq n}\frac{\log(p)}{p(p-1)} = O(1)$. Finally, since

$$\log(n!) = \int_1^n \log(t)\,dt + O(\log(n)) = n\log(n) + O(\log(n)),$$

the assertion follows when we divide all by n. □

The following result is due to Mertens:

THEOREM A.10 (Mertens). *We can write*

$$\sum_{\substack{p<X\\ p \text{ primes}}} \frac{1}{p} = \log\log(X) + O(1) \quad (X\to\infty).$$

PROOF. We have

$$\sum_{p<X}\frac{1}{p} = \sum_{p<X}\frac{\log(p)}{p}\frac{1}{\log(p)} = \sum_{n<X}\left(\sum_{p\leq n}\frac{\log(p)}{p} - \sum_{p\leq n-1}\frac{\log(p)}{p}\right)\frac{1}{\log(n)},$$

where p is prime and n varying on $\mathbb{N}$. Indeed the expression given by $\sum_{p\leq n}\frac{\log(p)}{p} - \sum_{p\leq n-1}\frac{\log(p)}{p}$ is zero unless n is prime; on the other hand if $n = p$ is prime the above expression is exactly $\frac{1}{\log(p)}$.

Hence, using lemma A.9

$$\sum_{p<X}\frac{1}{p} = \sum_{n\leq X}\left(\log(n) - \log(n-1) + \epsilon(n) - \epsilon(n-1)\right)\frac{1}{\log(n)},$$

being ϵ a certain limited function. We cut the summation in two parts; on the one hand

(A.2)

$$\sum_{2\leq n<X}\left(\log(n)-\log(n-1)\right)\frac{1}{\log(n)} = \sum_{2\leq n\leq X}\frac{1}{n\log(n)} + O\left(\sum_{2\leq n\leq X}\frac{1}{n^2\log(n)}\right) = \\ = \log\log(X) + O(1),$$

where the first equality follows from the fact that $\log(n) - \log(n-1) = \frac{1}{n} + O\left(\frac{1}{n^2}\right)$, whereas the second one follows from $\int_2^X \frac{dt}{t\log(t)} = \log\log(X) + O(1)$ and $\int_2^X \frac{dt}{t^2\log(t)} = O\left(\frac{1}{\log(X)}\right)$. On the other hand

(A.3)

$$\sum_{2\leq n<X}\left(\epsilon(n)-\epsilon(n-1)\right)\frac{1}{\log(n)} = \sum_{2\leq n<X}\epsilon(n)\left(\frac{1}{\log(n)} - \frac{1}{\log(n-1)} + O(1)\right) = \\ = O(1),$$

where the second estimate follows from the inequality $\frac{1}{\log(n)} - \frac{1}{\log(n-1)} \leq \frac{1}{n\log(n)\log(n+1)}$; note that $\sum_{n<X} \frac{1}{n\log(n)\log(n+1)}$ converges, since the integral $\int_2^\infty \frac{dt}{t\log(t)\log(t+1)}$ converges. Combining (A.2) and (A.3) yields

$$\sum_{\substack{p<X \\ p \text{ primes}}} \frac{1}{p} = \log\log(X) + O(1),$$

as required. □

APPENDIX B

Euclidean Algorithm

In this appendix we introduce the euclidean algorithm and we give an estimate of its computational complexity. As we will see the key ingredient is Lamé's theorem[1] that links the number of steps in the euclidean algorithm with Fibonacci numbers. Hence in the first part of this appendix we recall some properties of Fibonacci numbers that we will use later as to evaluate the running-time of the euclidean algorithm.

DEFINITION B.1 (Fibonacci numbers). The sequence of natural numbers $\{f_n\}_{n=0}^{+\infty}$, defined by the relations $f_0 = 0$, $f_1 = 1$, $f_{n+2} = f_n + f_{n+1}$ is called the *Fibonacci sequence*. The very first elements are: $0, 1, 1, 2, 3, 5, 8, 13, 21, \cdots$. □

The above sequence takes the name from the Italian mathematician Leonardo Fibonacci (XIII century) and the terms of the sequence are called *Fibonacci numbers*. The Fibonacci sequence was well known in ancient India, where it was applied to the metrical sciences (prosody), long before it was known in Europe. Developments have been attributed to Pingala (200 BC), Virahanka (VI century AD), Gopala (1135 AD), and Hemachandra (1150 AD).

In the West, the sequence was studied by Leonardo of Pisa, known as Fibonacci, in his Liber Abaci (1202). He considers the growth of an idealised (biologically unrealistic) rabbit population, assuming that:

- In the "zero-th"month, there is one pair of rabbits (additional pairs of rabbits = 0).
- In the first month, the first pair begets another pair (additional pairs of rabbits = 1).
- In the second month, both pairs of rabbits have another pair, and the first pair dies (additional pairs of rabbits = 1).
- In the third month, the second pair and the new two pairs have a total of three new pairs, and the older second pair dies (additional pairs of rabbits = 2).

The laws of this are that each pair of rabbits has 2 pairs in its lifetime, and dies. Let the population at month n be f_n. At this time, only rabbits who were alive at month $n-2$ are fertile and produce offspring, so f_{n-2} pairs are added to the current population of f_{n-1}. Thus the total is $f_n = f_{n-1} + f_{n-2}$.

[1] Gabriel Lamé is also famous because he was the first (with Cauchy) that presented a (wrong) complete proof of Fermat's last theorem[**47**].

Fibonacci sequences appear in biological settings, in two consecutive Fibonacci numbers, such as branching in trees, arrangement of leaves on a stem, the fruitlets of a pineapple, the flowering of artichoke, an uncurling fern and the arrangement of a pine cone. In addition, numerous poorly substantiated claims of Fibonacci numbers or golden sections in nature are found in popular sources, e. g. relating to the breeding of rabbits, the spirals of shells, and the curve of waves. The Fibonacci numbers are also found in the family tree of honeybees.

One of the properties we will need is the link between Fibonacci numbers and the *golden ratio*[2] $\Theta = \frac{1+\sqrt{5}}{2}$. We show an interesting property:

LEMMA B.1. *For each natural number $n \in \mathbb{N}$ we have:*

(1) $\Theta^{n+2} = \Theta^{n+1} + \Theta^n$
(2) $(1-\Theta)^{n+2} = (1-\Theta)^{n+1} + (1-\Theta)^n$.

PROOF. It suffices to note that Θ and $(1-\Theta)$ are the solutions of the second degree equation $X^2 = X + 1$; hence $\Theta^2 = \Theta + 1$ and $(1-\Theta)^2 = (1-\Theta) + 1$ and multiplying both members (respectively) by Θ^n and $(1-\Theta)^n$ we find the assertion. □

We note immediately that the relation which defines the n-th Fibonacci number as a function of the previous two elements of the Fibonacci sequence is identical to the expression of the n-th power of Θ. Indeed we have the following (important) theorem:

THEOREM B.2 (Binet's Formula). *For each natural number $n \in \mathbb{N}$ the following holds:*

$$f_n = \frac{1}{\sqrt{5}}\left(\Theta^n - (1-\Theta)^n\right). \tag{B.1}$$

PROOF. We use induction on n. The basis case ($n = 0$ and $n = 1$) is right, since

$$f_0 = \frac{1}{\sqrt{5}}(1-1) = 0$$
$$f_1 = \frac{1}{\sqrt{5}}(\Theta - 1 + \Theta) = 1.$$

[2]In mathematics and the arts, two quantities are in the golden ratio if the ratio between the sum of those quantities and the larger one is the same as the ratio between the larger one and the smaller. The golden ratio is an irrational mathematical constant, approximately 1.6180339887.

Let us suppose that the assertion holds for every integer $k < n$ (induction hypothesis), we show that it is still valid $\forall\, k \geq n$.

$$\begin{aligned} f_n = f_{n-1} + f_{n-2} &= \frac{1}{\sqrt{5}}(\Theta^{n-1} - (1-\Theta)^{n-1} + \Theta^{n-2} - (1-\Theta)^{n-2}) \\ &= \frac{1}{\sqrt{5}}(\underbrace{\Theta^{n-1} + \Theta^{n-2}}_{\Theta^n} - \underbrace{(1-\Theta)^{n-1} + (1-\Theta)^{n-2}}_{(1-\Theta)^n}) \\ &= \frac{1}{\sqrt{5}}(\Theta^n - (1-\Theta)^n). \end{aligned}$$

□

Another interesting fact is that the consecutive powers of Θ are always between two Fibonacci numbers, as stated in the following lemma:

Lemma B.3. *For each natural number $n \in \mathbb{N}_{\geq 1}$, we have $f_{n+1} < \Theta^n < f_{n+2}$.*

Proof. We use induction on n. The basis case ($n = 1$) is right since

$$f_1 = 1 < \Theta < f_2 = 2.$$

Let us suppose that the assertion holds $\forall\, k < n$, we can write:

$$\begin{aligned} f_{n-1} < \Theta^{n-2} < f_n \\ f_n < \Theta^{n-1} < f_{n+1}, \end{aligned}$$

so that

$$f_{n-1} + f_n = f_{n+1} < \Theta^{n-2} + \Theta^{n-1} = \Theta^n < f_n + f_{n+1} = f_{n+2}.$$

□

Now we have all the elements to introduce the *euclidean algorithm*; this algorithm defines an automatic procedure to compute the greatest common divisor between two numbers (or two polynomials), namely $\gcd(a, b)$, with $a, b \in \mathbb{Z}$. In what follows we will suppose that $a \geq b > 0$, that $\gcd(a, b) = \gcd(b, a) = \gcd(a, -b)$ and $\gcd(a, 0) = a$. The heart of the algorithm depends on the following lemma.

Lemma B.4. *Let a and b be two integers, such that $a \geq b > 0$. Then* $\gcd(a, b) = \gcd(b, a \bmod b)$.

Proof. It suffices to show that common divisors of a and b are common divisors of b and $a \bmod b$. Recall that we can always write $a = qb + a \bmod b$, with $q = \lfloor \frac{a}{b} \rfloor$. Now a common divisor of a and b divides also $a - qb = a \bmod b$; hence a common divisor of a and b divides also b and $a \bmod b$. On the other hand, a common divisor of b and $a \bmod b$ is a divisor of $a = qb + a \bmod b$ too; thus a common divisor of b and $a \bmod b$ divides also a and b. □

The euclidean algorithm exploits the above lemma in an iterative fashion; first of all if $b = 0$ we have immediately $\gcd(a, 0) = a$. On the other hand, when $b \neq 0$ we can apply lemma B.4 and state that $\gcd(a, b) = \gcd(b, a \bmod b)$ (with $b > a \bmod b \geq 0$), since $a \bmod b$ is the remainder of the division between a and b. Hence, if we apply lemma B.4 iteratively, the second argument of the gcd decreases step by step, until it reaches zero; at that point $\gcd(a, b) = \cdots = \gcd(h, 0) = h$, being h the greatest common divisor between a and b.

It is useful to have an estimate of the running-time of the algorithm. The following theorem is crucial:

THEOREM B.5 (G. Lamé). *Let $a \geq b > 0$ and denote with $E(a, b)$ the number of steps in the euclidean algorithm. Then, for every natural number n, we have $E(a, b) < n$ whenever $b < f_{n+1}$, or $a < f_{n+2}$.*

PROOF. First of all note that it suffices to prove the contrapositive statement, namely that if $E(a, b) \geq n$ then $b \geq f_{n+1}$ and $a \geq f_{n+2}$. We use induction on n. The basis case ($n = 0$) implies

$$E(a, b) \geq 0 \Rightarrow b \geq f_{0+1} = 1 \text{ e } a \geq f_{0+2} = 2,$$

and this holds, since we have supposed $a \geq b > 0$.

Let now us suppose that $E(a, b) \geq k$ implies $b \geq f_{k+1}$ and $a \geq f_{k+2}$, $\forall\, k \leq n$; we show that the assertion holds $\forall\, k \geq n + 1$. Namely we wish to show that if $E(a, b) \geq n + 1$, then $a \geq f_{n+3}$ and $b \geq f_{n+2}$. Let $E(a, b) \geq n + 1$; using lemma B.4 we can write $\gcd(a, b) = \gcd(b, a \bmod b)$ and the computation of $\gcd(b, a \bmod b)$ requires exactly $E(a, b) - 1$ steps. Since $E(b, a \bmod b) = E(a, b) - 1 \geq n$, we can use the induction hypothesis to conclude that $b \geq f_{n+2}$ and $a \bmod b \geq f_{n+1}$. Thus it remains to show that $a \geq f_{n+3}$; but $a = qb + a \bmod b \geq b + a \bmod b$, and as a consequence $a \geq b + a \bmod b \geq f_{n+2} + f_{n+1} = f_{n+3}$. □

Lamé's theorem can be used to show that the computational complexity of the euclidean algorithm is polynomial.

COROLLARY B.6. *For each integer $b_0 > 0$, the number of steps required by the euclidean algorithm to evaluate $\gcd(a, b_0)$ is $O(\log a)$.*

PROOF. Let us denote with $E(a, b_0) = N$ the required number of steps; Lamé's theorem tells us that $a \geq f_{N+2}$. Moreover, by lemma B.3, we know that $f_{N+2} > \Theta^N$, hence $a > \Theta^N$, and taking $\log_\Theta$ of both sides yields:

$$\log_\Theta a > N \quad \Rightarrow \quad N < \log a.$$

□

COROLLARY B.7. *For each integer $b_0 > 0$, the number of steps required to evaluate $\gcd(a, b_0)$ is $E(a, b_0) = N < 5d_a$, being d_a the number of decimal digits in a.*

Proof. As in the proof of the previous corollary we have $a > \Theta^N$. Since $\log_{10}\Theta < \frac{1}{5}$ we can write:

$$\log_{10} a > \log_{10}\Theta^N > \frac{N}{5} \quad \Rightarrow \quad N < 5\log_{10} a.$$

The number of decimal digits in a is $d_a = \lfloor \log_{10} a \rfloor + 1$, whereas $\log_{10} a = \lfloor \log_{10} a \rfloor + \epsilon_a$, with $0 \leq \epsilon_a < 1$; as a consequence $d_a > \log_{10} a$ which implies the assertion

$$N < 5\log_{10} a < 5d_a.$$

□

Corollary B.8 (Computational Cost of the Euclidean Algorithm). *The running-time of the euclidean algorithm is $O(\log^3(n))$, being $n = \max(a, b)$.*

Proof. Corollary B.6 tells us that the number of steps the algorithm needs is $O(\log(n))$; on the other hand, in each step, we evaluate a division with remainder, whose complexity is $O(\log^2(n))$. Hence

$$\text{Running-Time: } \Rightarrow \quad O(\log^3(n)).$$

□

We close this chapter presenting an extended version of the algorithm, that can be used to solve diofantine equation of the form $aX+bY \equiv \gcd(a, b)$[3]. The crucial result is the following:

Theorem B.9. *Define the quantities:*

$$\begin{aligned} x_{k+1} &= q_k x_k + x_{k-1} \qquad x_0 = 1,\ x_1 = 0 \\ y_{k+1} &= q_k x_k + y_{k-1} \qquad y_0 = 0,\ y_1 = 1. \end{aligned}$$

being q_k the k-th quotient of the euclidean algorithm applied to the integers $a \geq b > 0$ (with $k = 0, 1, \cdots, N$). Hence we can write:

$$r_k = (-1)^k x_k a + (-1)^{k+1} y_k b \qquad k = 0, 1, \cdots, N,$$

being r_k the k-th remainder in the euclidean algorithm, given by $r_{k-2} = r_{k-1}q_{k-1} + r_k$, $k = 2, 3, \cdots, N$ ($r_0 = a$, $r_1 = b$ and $r_N = h = \gcd(a, b)$).

Proof. We use induction on k. The basis case ($k = 0$ e $k = 1$) is OK, since

$$\begin{aligned} k = 0 &\Rightarrow r_0 = (-1)^0 x_0 a + (-1)^1 y_0 b = a \\ k = 1 &\Rightarrow r_1 = (-1)^1 x_1 a + (-1)^2 y_1 b = b. \end{aligned}$$

[3]Such an equation is met when you need to evaluate the inverse of an element in $\mathbb{Z}_n$. For example let $a \in \mathbb{Z}_n$ an element such that $\gcd(a, n) = 1$. The modular (multiplicative) inverse of a is the element $x \in \mathbb{Z}_n$ such that $a \cdot x \equiv 1 \pmod{n}$. As a consequence

$$a \cdot x = 1 + y \cdot n \quad \Rightarrow \quad a \cdot x - n \cdot y = 1.$$

Hence it suffices to solve for $aX - nY = 1$.

Let us now suppose that the assertion holds for all the integers strictly less than k; we show that the theorem is still valid for the integers greater or equal to k. Using the induction hypothesis we can write:

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_{k-1} \\ &= (-1)^{k-2}x_{k-2}a + (-1)^{k-1}y_{k-2}b - q_{k-1}\left[(-1)^{k-1}x_{k-1}a + (-1)^k y_{k-1}b\right] \\ &= (-1)^k a(x_{k-2} + q_{k-1}x_{k-1}) + (-1)^{k+1}b(y_{k-2} + q_{k-1}y_{k-1}) \\ &= (-1)^k x_k a + (-1)^{k+1}y_k b. \end{aligned}$$

□

Corollary B.10. *With the notation as introduced above, the solution of the diofantine equation*

$$aX + bY = \gcd(a, b)$$

are $X = (-1)^N x_N$ *and* $Y = (-1)^{N+1}y_N$.

Proof. Using theorem B.9 we can write,

$$r_N = \gcd(a, b) = (-1)^N x_N a + (-1)^{N+1}y_N b,$$

hence the assertion. □

APPENDIX C

Euler's φ-Function

In this appendix we derive some properties relative to Euler's φ-function. Let n be a natural number, and consider the ring of integers modulo n, namely $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. We write $\overline{a}$ for the congruence class of a modulo n, so that

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\}.$$

Let $\mathbb{Z}_n^*$ be the subset of $\mathbb{Z}_n$ that contains all invertible elements modulo n, that is to say

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n : \ \gcd(a, n) = 1\}.$$

We define the *Euler totient function* (or Euler's φ-function), to be

$$\varphi(n) = \#\{a \in \mathbb{Z} : \ 0 < a \leq n \text{ and } \gcd(a, n) = 1\}.$$

We want to derive a general formula to evaluate $\varphi(n)$. Note that it is very easy to evaluate $\varphi(p)$ when p is prime; indeed when p is prime we have $\gcd(a, p) \neq 1$ if and only if $p|a$, i. e. $a \equiv 0 \pmod{p}$. In other words the set $\mathbb{Z}_p^*$ is $\mathbb{Z}_p$ deprived of $\overline{0}$; as a consequence $\varphi(p) = p - 1$. The above reasoning can be extended to prove:

Proposition C.1. *Let p be a prime number and $m \in \mathbb{N}$. Then*

$$\varphi(p^m) = p^m \left(1 - \frac{1}{p}\right).$$

Proof. A number $a \in \mathbb{Z}$ is such that $\gcd(a, p^m) = 1$ if and only if $p \nmid a$; hence an element $\overline{a} \in \mathbb{Z}_{p^m}$ is invertible if and only if p does not divide a. Since exactly one out of p elements of

$$\mathbb{Z}_{p^m} = \left\{\overline{0}, \overline{1}, \cdots, \overline{p}, \cdots, \overline{2p}, \cdots, \overline{3p}, \cdots, \overline{p^m - 1}\right\},$$

is divisible by p, we can conclude that exactly $\frac{1}{p}p^m$ elements of $\mathbb{Z}_{p^m}$ are not invertible. Thus the number of invertible elements is $p^m - \frac{1}{p}p^m$, as required. □

The next step is proving that $\varphi(n \cdots m) = \varphi(n) \cdot \varphi(m)$, for all natural numbers n, m. In order to show this properties we need some preliminary observations.

Lemma C.2. *Let $n, m \in \mathbb{Z}$ be two integers such that $\gcd(n, m) = 1$. The for each $a \in \mathbb{Z}$ we have that n and m divide a if and only if the product $n \cdot m$ divides a.*

PROOF. ($\Rightarrow$). Let us suppose that n and m divide a, so that $a = rn$ and $a = sm$. Since $\gcd(n, m) = 1$, we can use Bézout's identity to write $xn + ym = 1$. Hence

$$a = a(xn + ym) = ms(xn) + nr(ym) = (sx + yr)nm,$$

as desired.

($\Leftarrow$). On the other hand, if nm divides a, it is clear that both n and m divide a. □

PROPOSITION C.3. *Let $m, n \in \mathbb{Z}$ be two integers such that $\gcd(n, m) = 1$. Then the map given by:*

$$\begin{aligned} f : \mathbb{Z}_{nm} &\longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m \\ x \bmod mn &\mapsto (x \bmod n, x \bmod m), \end{aligned}$$

is a bijection.

PROOF. Since $\#\mathbb{Z}_{nm} = \#(\mathbb{Z}_n \times \mathbb{Z}_m) = nm$, it suffices to prove that f is injective. Hence let $x \bmod nm$ and $y \bmod nm$ be two elements of $\mathbb{Z}_{nm}$, and let us suppose that $f(x) = f(y)$. As a consequence $(x \bmod n, x \bmod m) = (y \bmod n, y \bmod m)$, that is to say

$$x \equiv y \pmod{n} \quad \text{and} \quad x \equiv y \pmod{m}.$$

In other words both n and m divide $x - y$. But $gcd(n, m) = 1$, so that lemma C.2 implies that nm divides $x-y$, i. e. $xy \equiv 0 \pmod{nm}$ and f is injective. □

Now we consider the restriction of f on the subset $\mathbb{Z}_n^*$ of $\mathbb{Z}_n$. Note that if the class $x \bmod nm$ is an element of $\mathbb{Z}_{nm}^*$, then $\gcd(x, nm) = 1$; as a consequence $\gcd(x, n) = \gcd(x, m) = 1$. Hence for each element $x \in \mathbb{Z}_{nm}^*$ we have that x is also an element of $\mathbb{Z}_n^*$ and $\mathbb{Z}_m^*$; in other words the image of $f|_{\mathbb{Z}_{nm}^*}$ is contained in the subset $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ of $\mathbb{Z}_n \times \mathbb{Z}_m$.

PROPOSITION C.4. *Let $m, n \in \mathbb{Z}$ be two integers such that $\gcd(n, m) = 1$. Then the map given by:*

$$\begin{aligned} f : \mathbb{Z}_{nm}^* &\longrightarrow \mathbb{Z}_n^* \times \mathbb{Z}_m^* \\ x \bmod mn &\mapsto (x \bmod n, x \bmod m), \end{aligned}$$

is a bijection.

PROOF. Proposition C.3 implies that f is injective, hence it suffices to prove that it is surjective. Consider an element of $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$, proposition C.3 tells us that it is of the form $(x \bmod n, x \bmod m)$, for some $x \bmod nm$ in $\mathbb{Z}_{nm}$. If we show that $x \in \mathbb{Z}_{nm}^*$ we are done. But $\gcd(x, n) = \gcd(x, m) = 1$, so that $\gcd(x, nm) = 1$ and $x \in \mathbb{Z}_{nm}^*$ as required. □

COROLLARY C.5. *Let $m, n \in \mathbb{Z}$ be two integers such that $\gcd(n, m) = 1$. Then*

$$\varphi(nm) = \varphi(n) \cdot \varphi(m).$$

PROOF. Since the map f of proposition C.4 is a bijection, $\mathbb{Z}_{nm}^*$ and $\mathbb{Z}_n^* \times \mathbb{Z}_m^*$ have the same number of elements. Hence

$$\varphi(nm) = \#\mathbb{Z}_{nm}^* = \#(\mathbb{Z}_n^* \times \mathbb{Z}_m^*) = \#\mathbb{Z}_n^* \cdot \#\mathbb{Z}_m^* = \varphi(n) \cdot \varphi(m).$$

□

We are ready to give the main result of this appendix

THEOREM C.6. *Let n be a natural number. Then*

$$\varphi(n) = n \prod_{\substack{p|n \\ p \text{ primes}}} \left(1 - \frac{1}{p}\right).$$

PROOF. Let

$$n = \prod_{\substack{p|n \\ p \text{ primes}}} p^{a(p)},$$

be the prime factorization of n. Hence $p^{a(p)}$ divides n, whereas $p^{a(p)+1}$ does not. Hence, corollary C.5 implies

$$\varphi(n) = \prod_{p|n} \varphi(p^{a(p)}) = \prod_{p|n} p^{a(p)} \left(1 - \frac{1}{p}\right),$$

where we have used proposition C.1 in the last equality. Thus

$$\varphi(n) = \prod_{p|n} p^{a(p)} \left(1 - \frac{1}{p}\right) = \prod_{p|n} p^{a(p)} \prod_{p|n} \left(1 - \frac{1}{p}\right) =$$
$$= n \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

□

EXAMPLE C.1. Take $n = 7020 = 2^2 \cdot 3^3 \cdot 5 \cdot 13$. Hence

$$\varphi(7020) = 7020 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{13}\right) = 1728.$$

□

We close this appendix presenting a very useful properties of $\varphi(\cdot)$.

LEMMA C.7. *Let $n \in \mathbb{Z}_{>1}$ be an integer; we can write*

$$\sum_{d|n} \varphi(d) = n.$$

PROOF. Let $\mathcal{S} = \{1, 2, \cdots, n\}$ and for each divisor d of n let $\mathcal{S}_d = \{a \in \mathcal{S} : \gcd(a, n) = \frac{n}{d}\}$. These sets $\mathcal{S}_d$ partition $\mathcal{S}$ into disjoint subsets, since if $a \in \mathcal{S}$, then $\gcd(a, n) = \frac{n}{d}$ for some unique divisor d of n. Hence

$$\sum_{d|n} \#\mathcal{S}_d = \#\mathcal{S} = n,$$

and it suffices to show that $\#\mathcal{S}_d = \varphi(d)$ for each d divisor of n. Note that

$$a \in \mathcal{S}_d \quad \Leftrightarrow \quad a \in \mathbb{Z} \text{ with } 1 \le a \le n \text{ and } \gcd(a,n) = \frac{n}{d}.$$

If we define $a = a' \frac{n}{d}$ for each integer a, then a' is an integer since $\frac{n}{d} = \gcd(a,n)$ divides a. Dividing the above condition by $\frac{n}{d}$ yields

$$a \in \mathcal{S}_d \quad \Leftrightarrow \quad a = a' \frac{n}{d} \text{ where } a' \in \mathbb{Z} \text{ with } 1 \le a' \le d \text{ and } \gcd(a',d) = 1.$$

Thus $\#\mathcal{S}_d$ is the number of integers a' between 1 and d, which are coprime to d, namely $\varphi(d)$, and the assertion is proven. □

EXAMPLE C.2. Let $n = 12$, so that $d = 1, 2, 3, 4, 6, 12$ and $\varphi(d) = 1, 1, 2, 2, 2, 4$. Hence

$$\sum_{d|n} \varphi(d) = 1 + 1 + 2 + 2 + 2 + 4 = 12 = n.$$

□

APPENDIX D

The Link between Hasse's bound and the Riemann Hypothesis

In this appendix we will show that Hasse's theorem implies the Riemann hypothesis for an elliptic curve defined over $\mathbb{Z}_p$. The harmonic series

$$\sum_{n=1}^{+\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots$$

is one of the series of major interest for number theorists, since it involves integer numbers. It is easy to check that this series diverge: the sum of the first n terms is $\log(n)$ which tends to infinity when $n \to +\infty$. We can obtain convergence if we write $\frac{1}{n^s}$ $(s > 1)$ in place of $\frac{1}{n}$:

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots, \tag{D.1}$$

which is the *Riemann-zeta function*.

Although the series of equation (D.1) was attributed to Riemann after he published an article with the study of its properties (1859), the series was known since the time of Euler, who showed:

THEOREM D.1 (Eulero). *We have:*

$$\zeta(s) = \prod_{\text{primes } p} \frac{1}{1 - p^{-s}} = \prod_{\text{primes } p} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{D.2}$$

PROOF. Dividing each member of equation (D.1) by 2^s we obtain:

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \cdots,$$

and subtracting from equation (D.1) we have:

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \cdots, \tag{D.3}$$

which does not contain the multiples of $\frac{1}{2}$.

Now we divide equation (D.3) by 3^s, obtaining:

$$\frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \cdots,$$

and subtracting from equation (D.3) we have:

$$\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s) = 1+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{11^s}+\frac{1}{13^s}+\cdots,$$

which does not contain the multiples of $\frac{1}{3}$ and $\frac{1}{2}$. Iterating this argument we obtain:

$$\cdots\left(1-\frac{1}{11^s}\right)\left(1-\frac{1}{7^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{2^s}\right)\zeta(s) = 1$$

which brings:

$$\zeta(s) = \prod_{\text{primes } p}\frac{1}{1-p^{-s}}.$$

Note that $1-\frac{1}{p^s} = \frac{p^s-1}{p^s}\cdot\frac{p^{-s}}{p^{-s}} = 1-p^{-s}$ and hence:

$$\zeta(s) = \prod_{\text{primes } p}\left(1-\frac{1}{p^s}\right)^{-1}.$$

□

For what concerns convergence, one can show that $\zeta(s)$ converges if $\Re(s) > 1$. The famous Riemann hypothesis[1] states:

Conjecture D.2 (Riemann Hypothesis). *Let $\zeta(s)$ be the meromorphic extension of the series defined in* (D.1)*. The non-trivial zeroes of $\zeta(s)$ are such that $\Re(s) = \frac{1}{2}$.*

Riemann showed that if we extend $\zeta(s)$ to $\mathbb{C}$, we obtain a meromorphic function with a single pole at $s = 1$. It is easy to check that $\zeta(s)$ is zero for all even negative integers, hence the non-trivial zeroes are those with $\Re(s) > 0$, as showed in figure D.1.

Now we show the link with Hasse's theorem. Let $C(\mathbb{Z}_p)$ be a smooth, projective curve over $\mathbb{Z}_p$. It is possible to define a zeta function associated with the curve, of the kind:

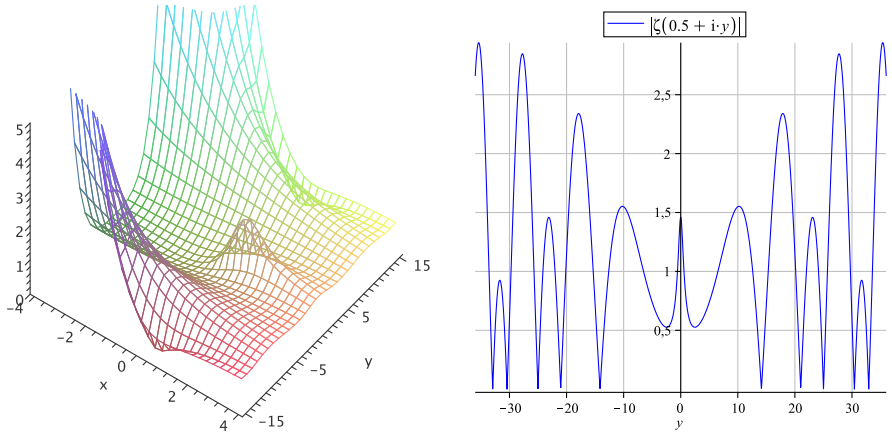
$$\zeta_C(s) = \prod_{\substack{Q\in C(\overline{\mathbb{Z}}_p)\\ \text{without}\\ \text{conjugation}}}\left(1-\frac{1}{\mathcal{N}(Q^s)}\right)^{-1}, \tag{D.4}$$

where $\mathcal{N}(Q)$ is the *norm*[2] of the point $Q = (x, y) \in C(\overline{\mathbb{Z}}_p)$.

We explicitly note the similarity between equation (D.4) and (D.2); actually the result is quite deeper, and one can show that the points Q of

[1] The Riemann hypothesis implies a large body of other important results. Most mathematicians believe the Riemann hypothesis to be true. A one million dollars prize has been offered by the Clay Mathematics Institute for the first correct proof. See also `http://en.wikipedia.org/wiki/Riemann_hypothesis`.

[2] Since $Q = (x, y) \in C(\overline{\mathbb{Z}}_p)$, $\exists\, h, g \in \mathbb{Z}_p[X]$ (of minimum degree) such that $h(x) = 0$ and $g(y) = 0$; let $\lambda = lcm\,(deg(h), deg(g))$, the norm of the point Q is $\mathcal{N}(Q) = p^\lambda$.



(A) $|\zeta(x+iy)|$ (B) $|\zeta(0.5+iy)|$

FIGURE D.1. Plot of the absolute value of the Riemann zeta function: (A) as a function of both $x = \Re(s)$ and $y = \Im(s)$, (B) on the critical line as a function of $y = \Im(s)$.

equation (D.4) are indeed prime ideals of the ring $\mathbb{Z}_p[X,Y]/(f(X,Y))$, where $C(\mathbb{Z}_p)$ is the set of solutions of $f(X,Y) \in \mathbb{Z}_p[X,Y]$: the points Q play the same role of the primes p in equation (D.2). Recall that conjugation in $\overline{\mathbb{Z}}_p$ is a map:

$$\begin{aligned} {}^* : \overline{\mathbb{Z}}_p &\to \overline{\mathbb{Z}}_p \\ x &\mapsto x^* = x^p \end{aligned}$$

which leaves $\mathbb{Z}_p$ fixed and it is such that $x \in \mathbb{R} \Leftrightarrow x \equiv x^p \pmod{p}$ (as we have shown in proposition 2.9). Hence points Q without conjugation means that only one between $Q = (x,y)$, $Q' = (x^p, y^p)$ and $Q'' = (x^{2p}, y^{2p})$ will appear in the product of equation (D.4). It is possible to show the following equality:

$$\zeta_C(s) = \prod_{\substack{Q \in C(\overline{\mathbb{Z}}_p) \\ \text{without} \\ \text{conjugation}}} \left(1 - \frac{1}{\mathcal{N}(Q^s)}\right)^{-1} = \sum_{\substack{D \geq 0 \\ \mathbb{Z}_p\text{-divisors}}} p^{-deg(D)s}.$$

Now we show that the Riemann hypothesis is true[3] for $\zeta_C(s)$.

THEOREM D.3 (Weil, Artin). *Let* $0 < \Re(s) < 1$. *Then* $\zeta_C(s) = 0$ *if and only if* $\Re(s) = \frac{1}{2}$.

[3]Deligne showed that this result holds also when we replace the algebraic curve C with an arbitrary algebraic variety.

Let us introduce the function:

$$Z_C(T) = \sum_{\substack{D\geq 0 \\ \mathbb{Z}_p\text{-divisors}}} T^{deg(D)} \in \mathbb{Z}[|T|],$$

where $\mathbb{Z}[|T|] \supset \mathbb{Z}[T]$ is the ring of formal power series of the kind $1 + T + T^2 + \cdots$. In $\mathbb{Z}[|T|]$ we can compute the inverse of $T - 1$ and $pT - 1$, at least if we can sum an infinite number of terms:

$$\frac{1}{T-1} = 1 + T + T^2 + T^3 + \cdots$$
$$\frac{1}{pT-1} = 1 + pT + p^2T^2 + p^3T^3 + \cdots$$

by the formula for the geometric series. We need a lemma, proved by Schmidt:

Lemma D.4 (Schmidt 1939). *It is:*

$$Z_C(T) = \frac{1 + a_1T + a_2T^2 + \cdots + a_2p^{g-2}T^{2g-2} + a_1p^{g-1}T^{2g-1} + p^gT^{2g}}{(1-T)(1-pT)} =$$
$$= \frac{P_C(T)}{(1-T)(1-pT)},$$

where g is the genus of the curve C. □

Now we are ready to give the proof of theorem D.3 at least when C is an elliptic curve (and hence it has genus $g = 1$).

Proof. First of all it is quite obvious that:

$$\zeta_C(s) = 0 \quad \Leftrightarrow \quad Z_C(p^{-s}) = 0 \quad \Leftrightarrow \quad P_C(p^{-s}) = 0,$$

since the zeroes of $1-T$ and $1-pT$ have (respectively) $\Re(s) = 0$ and $\Re(s) = 1$, whereas we require that $0 < \Re(s) < 1$. Furthermore:

$$\zeta_C(s) = 0 \text{ with } \Re(s) = \frac{1}{2} \quad \Leftrightarrow \quad |p^{-s}| = \sqrt{p}.$$

Let C be an elliptic curve, then $C \equiv E$ has genus $g = 1$ and thus, by lemma D.4:

$$Z_E(T) = \frac{1 + aT + pT^2}{(1-T)(1-pT)} =$$
$$= (1 + aT + pT^2)(1 + T + T^2 + \cdots)(1 + pT + p^2T^2 + \cdots) =$$
$$= 1 + T(p + 1 + a) + O(T^2).$$

On the other hand $D = 0$ is the only divisor of degree zero, whereas $D = \sum n_Q Q$ is a divisor of degree one if and only if $\sum n_Q = 1$, but since D must

be $D \geq 0$ we have $n_Q \in \mathbb{N}$ and then D is only a point $D = Q$. Hence:

$$\begin{aligned} Z_E(T) = & \sum_{\substack{D \geq 0 \\ \mathbb{Z}_p\text{-divisors}}} T^{deg(D)} = \\ & = T^0 + T(\#E(\mathbb{Z}_p)) + O(T^2) = \\ & = 1 + T(p + 1 - t) + O(T^2), \end{aligned}$$

where we used that $\#E(\mathbb{Z}_p) = p + 1 - t$; as a consequence we can write $a = -t$.

Hence,

$$\begin{aligned} Z_E(T) = & \frac{1 - tT + pT^2}{(1 - T)(1 - pT)} = \\ & = \frac{P_E(T)}{(1 - T)(1 - pT)} \end{aligned}$$

with $|t| < 2\sqrt{p}$ by Hasse's bound. Thus the discriminant of $P_E(T)$, namely $\Delta_{P_E(T)} = t^2 - 4p$, is less than or equal to 0 (since $4p > t^2$ by Hasse's bound), i. e. $P_E(T)$ has two conjugate roots:

$$P_E(T) = (1 - \alpha T)(1 - \alpha^* T) = 1 + \alpha\alpha^* T^2 - \alpha T - \alpha^* T \qquad \alpha, \alpha^* \in \mathbb{C}.$$

Hence we have $\alpha\alpha^* = p$ and $|\alpha| = |\alpha^*|$, since α and α^* are conjugate, and we can conclude:

$$|\alpha| = |\alpha^*| = \sqrt{p} \quad \Rightarrow \quad \Re(\alpha) = \frac{1}{2}.$$

Finally:

$$\zeta_E(s) = 0 \quad \Leftrightarrow \quad P_E(p^{-s}) = 0 \quad \Leftrightarrow \quad p^{-s} = \alpha, \alpha^* \quad \Leftrightarrow \quad \Re(s) = \frac{1}{2}.$$

Now we show that Riemann $\Rightarrow$ Hasse. We have already shown that $P_E(T) = 1 - tT + pT^2$; let us suppose that $\zeta_E(s) = 0$ with $\Re(s) = \frac{1}{2}$ and let α and β be the zeroes of $P_E(T)$, so that it must be $|\alpha| = |\beta| = \sqrt{p}$. Thus there are 4 possibilities for α and β:

- $\alpha = \sqrt{p} = \beta$, or
- $\alpha = \sqrt{p} = -\beta$, or
- $\alpha = -\sqrt{p} = \beta$, or
- $\alpha, \beta \in \mathbb{C}$ are conjugate.

Anyway $P_E(T) = (T - \alpha)(T - \beta) = T^2 - (\alpha + \beta)T + \alpha\beta$, and thus $t = \alpha + \beta$. Now if $\alpha = \beta = \pm\sqrt{p}$, we have $t \notin \mathbb{Z}$ that is not possible; if $\alpha = -\beta$, we have $t = 0$ and $P_E(T) = 1 + pT^2$ would not have real roots. Thus it is $\alpha = \beta^*$, i. e. $\Delta_{P_E(T)} < 0$, and then:

$$t^2 < 4p \quad \Rightarrow \quad |t| < 2\sqrt{p},$$

which is Hasse's bound. □

Bibliography

[1] M. Agrawal, N. Kayal and N. Saxena: *Primes is in P*, Annals of Math. 160 (2004), 781–793.

[2] T. M. Apostol: *Introduction To Analytical Number Theory*, Undergraduate Texts in Mathematics, Springer-Verlang ('76).

[3] E. Artin and J. Tate: *Class Field Theory*, AMS Chelsea Publishing - Providence Rhode Island('00).

[4] M. M. Artjuhov: *Certain Criteria for Primality of Numbers Connected with the Little Fermat Theorem*, Acta Arith. 12 (1966/1967), 355–364.

[5] A. O. L. Atkin and F. Morain: *Elliptic Curves and Primality Proving*, Math. Comp. 61:203 (1993), 29–68.

[6] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott: *Efficient Algorithms for Pairing-Based Cryptosystems*, Advance in Cryptology - Crypto 2002, LNCS 2442, Springer-Verlang (2002), 354–368.

[7] D. J. Bernstein: *Fast Multiplication and its Applications*, pp. 325–384 in *Surveys in Algorithmic Number Theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. 44, Cambridge University Press, New York, 2008.

[8] D. Boneh, M. K. Franklin: *Identity-Based Encryption from the Weil Pairing*, Advances in Cryptology: Proceedings of CRYPTO 2001 (2001).

[9] J. Buchmann: *Introduction to Cryptography*, Undergraduate Texts in Mathematics. Springer-Verlang, Second Edition ('01).

[10] D. S. Dummit, R. M. Foote: *Abstract Algebra*, John Wiley & Sons, Inc. ('04).

[11] L. S. Charlap and D. P. Robbins: *An Elementary Introduction to Elliptic Curves*, CRD Expository Report No. 31('88).

[12] L. S. Charlap and R. Coley: *An Elementary Introduction to Elliptic Curves II*, CCR Expository Report No. 34('90).

[13] A. Shamir: *An Identity Based Encryption Scheme Based on Quadratic Residues*, Proceedings of the 8th IMA International Conference on Cryptography and Coding, 2001.

[14] H. Cohen: *A Course in Computational Algebraic Number Theory*, Springer-Verlang ('93).

[15] G. Cornacchia: *Su di un Metodo per la Risoluzione in Numeri Interi dell' Equazione* $\sum_{h=0}^{n} C_h x^{n-h} = P$, Giornale di Matematiche di Battaglini 46 (1908), 33–90.

[16] J. Derbyshire: *Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics*, Pinguin Books, First Edition ('04).

[17] W. Diffie, M. Hellman: *New Directions in Cryptography*, IEEE Transactions on Information Theory, vol. IT-22, No. 6, Nov. 1976, pp. 644-654.

[18] T. ElGamal: *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985, pp. 469–472 or CRYPTO 84, pp. 10–18, Springer-Verlag.

[19] G. Frey, M. Muller and H. G. Ruck: *A Remark Concerning the m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves*, Mathematics of Computation 62 No. 206 (1994), 865–874.

[20] G. Frey, H. G. Ruck: *The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems*, IEEE Transactions on Information Theory 45(5) (1999), 1717–1719.

[21] A. Frölich, M. Taylor: *Algebraic Number Theory*, Cambridge University Press, Cambridge 1991.
[22] W. Fulton: *Algebraic Curves: An Introduction to Algebraic Geometry*, Addison-Wesley Publishing Company Advanced Book Program, Redwood City, CA, 1989. Notes written with the collaboration of R. Weiss, reprint of 1969 original.
[23] S. D. Galbraith: *Supersingular Curves in Cryptography*, Advances in Cryptology - Asiacrypt 2001, LNCS 2248, Springer-Verlang (2001), 495–513.
[24] S. Goldwasser and J. Kilian: *Almost All Primes Can be Quickly Certified*, pp. 316–329 in Proceedings of the eighteenth annual ACM Symposium on the theory of computing, ACM, New York, 1986.
[25] F. Q. Gouvea: *p-adic Numbers: An Introduction*, Universitext. Springer-Verlang, Third printing('08).
[26] R. Hartshorne: *Algebraic Geometry*, Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.
[27] F. Hess: *A Note on the Tate Pairing of Curves over Finite Fields*, to appear in Arch. Math.(02').
[28] F. Hess: *Some Remarks on the Weil and Tate Pairings of Curves over Finite Fields*, unpublished manuscript.
[29] G. A. Jones, J. A. Jones: *Elementary Number Theory*, Undergraduate Texts in Mathematics. Springer-Verlang ('99).
[30] S. Lang: *Algebraic Number Theory*, Addison-Wesley, New York 1970.
[31] S. Lang: *Elliptic Functions*, Addison-Wesley ('76).
[32] B. Lynn: *Elliptic Curves*, Lecture Notes, `http://rooster.stanford.edu/~ben/notes`.
[33] M. Maas: *Pairing-Based Cryptography*, Master's Thesis, Technische Universiteit Eindhoven, Department of Mathematics and Computing Science (04').
[34] A. J. Menezes: *Elliptic Curve Public-Key Cryptosystems*, Kluwer Academic Publishers ('93).
[35] G. L. Miller: *Riemann's Hypothesis and Tests for Primality*, J. Comput. System Sci. 13:3 (1976), 300–317.
[36] V. Miller: *Short Programs for Functions on Curves*, unpublished manuscript ('86).
[37] F. Morain: *Implementing the Asymptotically Fast Version of the Elliptic Curve Primality Proving Algorithm*, Math. Comp. 76:257 (2007), 493–505.
[38] M. O. Rabin: *Digitalized Signatures and Public-Key Functions as Intractable as Factorization*, MIT Laboratory for Computer Science, January 1979.
[39] M. O. Rabin: *Probabilistic Algorithms for Testing Primality*, J. Number Theory 12:1 (1980), 128–138.
[40] R. Rivest, A. Shamir,L. Adleman: *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Communications of the ACM 21 (2): pp.120–126, available via `http://theory.lcs.mit.edu/~rivest/rsapaper.pdf`.
[41] A. Shamir: *Identity-Based Cryptosystems and Signature Schemes*, Advances in Cryptology: Proceedings of CRYPTO 84, Lecture Notes in Computer Science, 7:47–53, 1984.
[42] R. Schoof: *Counting Points on Elliptic Curves over Finite Fields*, Journal de Théorie des Nombres de Bordeaux 7 ('95), 219–254.
[43] R. Schoof: *Four Primality Testing Algorithms*, pp. 101–126 in *Surveys in Algorithmic Number Theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. 44, Cambridge University Press, New York, 2008.
[44] D. Shanks: *Class Numbers, a Theory of Factorization and Genera*, 1969 Number Theory Institute, Proc. of Symp. in Pure Math. 20, AMS, Providence RI, 1971.
[45] J. H. Silverman: *Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics. Springer-Verlang ('86).
[46] J. H. Silverman and J. Suzuki: *Elliptic Curve Discrete Logarithms and the Index Calculus*, Advances in Cryptology - Eurocrypt 1998, LNCS 1514, Springer-Verlang (1998), 110–125.

[47] S. Singh: *Fermat's Last Theorem: The Story of a Riddle that Confounded the World's Greatest Minds*, Fourth Estate, London ('97).

[48] D. Stinson: *Cryptography: Theory and Practice*, Discrete Mathematics and its Applications. Chapman & all, Fourth Edition('96).

[49] P. Stevenhagen: *The Number Field Sieve*, pp. 83–100 in *Surveys in Algorithmic Number Theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. 44, Cambridge University Press, New York, 2008.

[50] F. C. Titchmarsh, D. R. Heath-Brown: *The Theory of the Riemann Zeta-function*, Oxford University Press, Second Edition('99).

[51] L. C. Washington: *Elliptic Curves: Number Theory and Cryptography*, Discrete Mathematics and its Applications. Chapman & all, Second Edition('08).

ECCC ISSN 1433-8092

http://eccc.hpi-web.de