Electronic Colloquium on Computational Complexity, Comment 2 on Report No. 009 (1998)

Eq. 3, p. 4 of Parallel Complexity of Integer Coprimality

B. Litow [§]

May 17, 1998

Eq. 3, p. 4 is correct as it stands (up to a constant factor.) Eq. 3, p.4 is based on multiplying the two partial fraction expansions of

$$\frac{1}{z^a - 1/\rho^a}$$

and

$$\frac{1}{z^{-b} - 1/\rho^b}$$

In general if Q is a polynomial in w with simple zeros, then

$$\frac{1}{Q} = \sum_{\beta} \frac{1}{Q'(\beta) \cdot (w - \beta)}$$

where the sum is over the zeros β of Q, and Q' is the derivative of Q w.r.t. w.

In the case of $\frac{1}{z^a - 1/\rho^a}$, we have $Q = z^a - 1/\rho^a$, i.e., z plays the role of w, and in case of $\frac{1}{z^{-b} - 1/\rho^b}$, $Q = (1/z)^b - 1/\rho^b$, and $1/z$ plays the role of w.

In the first case Q can be written as

$$\prod_{j=0}^{a-1} (z - \omega^j/\rho)$$

where ω is a primitive a-th root of unity. In the second case Q can be written as

$$\prod_{k=0}^{b-1} (1/z - \nu^k/\rho)$$

where ν is a primitive b-th root of unity.

In the first case $Q' = az^{a-1}$, so $Q'(\omega^j/\rho) = a\omega^{-j}/\rho^{a-1}$. In the second case $Q' = b(1/z)^{b-1}$ (remember that the variable is $1/z$), so $Q'(\nu^k/\rho) = b\nu^{-k}/\rho^{b-1}$. This yields

$$\frac{1}{z^a - 1/\rho^a} = \sum_{j=0}^{a-1} \frac{\omega^j}{z - \omega^j/\rho}$$

[§] Dept. of Computer Science, James Cook University, Townsville, Qld. 4811, Australia bruce@cs.jcu.edu.au

ISSN 1433-8092

and

$$\frac{1}{z^{-b} - 1/\rho^b} = \sum_{k=0}^{b-1} \frac{\nu^k}{1/z - \nu^k/\rho}$$

In turn, Eq. 3, p.4 arises from

$$\frac{1}{z^a - 1/\rho^a} = \sum_{j=0}^{a-1} \frac{\omega^j}{\omega^j \cdot (z\omega^{-j} - 1/\rho}$$

and

$$\frac{1}{z^{-b} - 1/\rho^b} = \sum_{k=0}^{b-1} \frac{\nu^k}{\nu^k \cdot (\nu^{-k}/z - 1/\rho}$$

Note that the root of unity factors cancel in the numerator and denominator of each term.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'