Algorithms for S-Unit Equations, Revisited

January 4, 2018

1 de Weger's Approach

Let $S = \{p_1, \ldots, p_s\}$ be a finite set of rational primes, write $N_S = \prod_{p \in S} p$ and denote by $\mathcal{O}^\times$ the group of units of $\mathcal{O} = \mathbb{Z}[1/N_S]$. We are interested in solving the S-unit equation

$$x + y = 1, \quad (x, y) \in \mathcal{O}^\times \times \mathcal{O}^\times. \tag{1}$$

Suppose that (x, y) satisfies (1). Then there exists nonzero $a, b, c \in \mathbb{Z}$ with $\gcd(a, b, c) = 1$ and $\operatorname{rad}(abc) \mid N_S$, such that $x = \frac{a}{c}$, $y = \frac{b}{c}$, and $a + b = c$. Indeed, since $(x, y) \in \mathcal{O}^\times \times \mathcal{O}^\times$, we have $x = \frac{\alpha_1}{\beta_1}, y = \frac{\alpha_2}{\beta_2}$, where $(\alpha_1, \beta_1) = 1$, $(\alpha_2 \beta_2) = 1$, and $\alpha_1, \beta_1, \alpha_2, \beta_2$ are integers composed only of primes of S. Then

$$x + y = \frac{\alpha_1}{\beta_1} + \frac{\alpha_2}{\beta_2} = 1$$

yields

$$\alpha_1 \beta_2 + \alpha_2 \beta_1 = \beta_1 \beta_2$$

and we take $a = \alpha_1 \beta_2$, $b = \alpha_2 \beta_1$ and $c = \beta_1 \beta_2$. Clearly, $\operatorname{rad}(abc) \mid N_S$. Lastly, suppose $\gcd(a, b, c) \neq 1$.