Prof. C. P. Schnorr Wintersemester 2014/15

Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 4 19.11.2014, Abgabe 3..12.2014

Aufgabe 1. Sei $N = pq \in \mathbb{N}$, p, q prim. Sei $2^{4n-1} < q < p < 2^{4n}$ (somit $2^{8n-2} < N < 2^{8n}$) und $p = a + 2^n c + 2^{3n} e$ mit $a, e \in [0, 2^n[, c \in [0, 2^{2n}[$.
Zeige, man kann N zu gegebenen a, e in Zeit $n^{O(1)}$ zerlegen.

Hinweis: Wende Thm 7 (May) an auf $f_p(x) = a + 2^n(x + 2^{2n-1}) + 2^{3n} e$ (ist nicht monisch). f_p hat Nullstelle $x_0 = c - 2^{2n-1}$ modulo p, $|x_0| \leq 2^{2n-1} < 1/\sqrt{2}\, N^{1/4}$. Es werden Thm 11 und Thm 12 von May kombiniert.

Aufgabe 2. Seien $N = pq$, p, q prim und $2^{6n-1} < q^3 < p < 2^{6n}$ (somit $2^{8n-4/3} < N < 2^{8n}$) und $p = a + 2^n c + 2^{5n} e$ mit $a, e \in [0, 2^n[, c \in [0, 2^{4n}[$.
$f_p(x_1, x_2) = x_1 + 2^n c + 2^{5n} x_2$ hat modulo p die Nullstelle $(x_1, x_2) = (a, e)$.
Zeige: Zu gegebenem c findet man in Zeit $n^{O(1)}$ ein $f(x_1, x_2) \in \mathbb{Z}[x_1, x_2] \neq \mathbf{0}$ so dass $f(r_1, r_2) = 0$ für alle $(r_1, r_2) \in \mathbb{Z}^2$ mit $f_p(r_1, r_2) = 0 \mod p$ und $|r_1|, |r_2| \leq 2^{n-1} < 2^{-5/6} N^{1/8}$.
Benutze Coppersmith's Methode im multivariaten Fall.

Aufgabe 3. Zeige, dass man das N von Aufgabe 2 nach erraten von $1, 5n+1$ führenden Bits von p bzw. q in Zeit $n^{O(1)}$ zerlegen kann, gemäß Thm 7 (May). Begründe mit Angabe von f_b, β, δ, x_0, jeweils für $b = q$ und $b = p$.