Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 3 02.12.2015, Abgabe 16.12.2015

Zu D. Coppersmith: Finding small solutions of small degree polynomials. Sei $p(x) \in \mathbb{Z}[x]$ vom Grad d und monisch und ggT$(\,(dh-1)!, N) = 1$

$$C_3 = \{(p(x)/N)^j x^i \mid 0 \le i < d, 0 \le j < h\}$$

$$C_3' = C_3 \cup \{b_k(x) \mid 0 \le k < dh\}$$

$$b_k(x) = x(x-1)\cdots(x-k+1)/k!, \text{ beachte } b_k(\mathbb{Z}) \subset \mathbb{Z}$$

Aufgabe 1. Es gibt in C_3' zu $k = 0, \ldots, dh-1$ genau zwei Polynome $q(x)$ vom Grad k nämlich $b_k(x)$ und $(p(x)/N)^j x^i$ mit $j = \lfloor k/d \rfloor$ und $i = k - jd$. Diese liefern zur Matrix L_3' von C_3' als Spalten die Koeffizientenvektoren von $q(xB)$ mit den Koeffizienten $B^k N^{-j}, B^k/k!$ für x^{k+1} in Zeile $k+1$.
Zeige: Diese beiden Spalten kann man unimodular so transformieren, dass $B^k N^{-j}, B^k/k!$ übergeht in $B^k N^{-j}/k!$ und 0. Es folgt $\det L_3' \le \det L_3 / \prod_{0 \le k < dh} k!$.

Aufgabe 2. Zeige: Von L_3 auf L_3' erhöht sich B um den Faktor $(\det L_3 / \det L_3')^{\frac{2}{dh(dh-1)}} \ge (\prod_{0 \le k < dh} k!)^{\frac{2}{dh(dh-1)}} \approx \frac{dh}{e^{3/2}}$.
Hinweis: $k! \approx (k/e)^k$, $\quad \sum_{k=1}^{dh-1} k \ln k \approx \int_1^{dh} k \ln k \, dk = \frac{1}{2}(dh)^2(\ln dh - 1/2)$.
Integriere $k \ln k$ durch partielle Integration.

Aufgabe 3. 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, $|x_0| \le 2^{2n-1} < N^{1/4}/\sqrt{2}$.
Es werden Thm 11 und Thm 12 von May kombiniert.

5 Punkte pro Aufgabe