

Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 3, 05.11.2014, Abgabe 19.11.2014

Zu D. Coppersmith: Finding small solutions of small degree polynomials.

Sei $p(x) \in \mathbb{Z}[x]$ vom Grad d und monisch und $\text{ggT}((dh - 1)!, N) = 1$

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

$$C'_3 = C_3 \cup \{b_k(x) \mid 0 \leq k < dh\}$$

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

Es bezeichne stets $\det L'_3 = \det \mathcal{L}(L'_3)$.

Aufgabe 1. Es gibt in C'_3 zu $k = 0, \dots, dh - 1$ genau zwei Polynome vom Grad k nämlich $q(x) \in \{(p(x)/N)^j x^i, b_k(x)\}$ mit $k = jd + i, j = \lfloor k/d \rfloor$. Diese liefern zur Matrix L'_3 von C'_3 als Spalten die Koeffizientenvektoren von $q(x)B$ 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 $\det L'_3 \leq \det L_3 / \prod_{0 \leq k < dh} k!$.

Aufgabe 2. Zeige: Von L_3 auf L'_3 erhöht sich B um den Faktor

$$(\det L_3 / \det L'_3)^{\frac{2}{dh(dh-1)}} \geq (\prod_{0 \leq k < dh} k!)^{\frac{2}{dh(dh-1)}} \approx \frac{dh}{e^{3/2}}.$$

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. Beweise Theorem 14 des Kapitels 3 der Dissertation von Alexander May.