Gitteralgorithmen zur Faktorisierung ganzer Zahlen

Blatt 3, 21.11.2012, Abgabe 28.11.2012

Zu D. Coppersmith: Finding small solutions of small degree polynomials.
Sei $p(x) \in \mathbb{Z}[x]$ vom Grad d und monisch

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

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

$$b_k(x) = x(x-1)\cdots(x-k+1)/k!$$

Es bezeichne stets $\det L_3' = \det \mathcal{L}(L_3')$.

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

Aufgabe 2. 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: $k! \approx (k/e)^k$, $\sum_{k=0}^{dh-1} k \ln(k/e) \approx \int_1^{dh+1} k \ln k = \binom{dh}{2}$.
Integriere $k \ln k$ durch partielle Integration.

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