Finding small roots of polynomial equations using LLL

Recall that using $\varepsilon = 1/4$, given as input a basis of an integer lattice L of rank d, the LLL algorithm outputs in polynomial time a non-zero vector $\vec{u} \in L$ such that $\|\vec{u}\| \leq 2^{(d-1)/4}\mathrm{vol}(L)^{1/d}$.

1. Coppersmith's Theorem. (⋆⋆)

Let $P(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree δ : the coefficient of its x^δ monomial is 1. Let N be a positive integer, whose factorization is unknown. We say that $Q(x) \in \mathbb{Q}[x]$ is (N, P)-good if for every integer $x_0 \in \mathbb{Z}$ such that $P(x_0) \equiv 0 \pmod N$, we have $Q(x_0) \in \mathbb{Z}$. If $Q(x) = \sum_{i=0}^{d} q_i x^i \in \mathbb{Q}[x]$, we define $\|Q\| = (\sum_{i=0} q_i^2)^{1/2}$. Let $X > 0$.

---

1. *Assume that $Q(x) \in \mathbb{Q}[x]$ is (N, P)-good and that $\|Q(xX)\| < 1/\sqrt{n+1}$ where n is the degree of Q. Show that if $P(x_0) \equiv 0 \pmod N$ and $|x_0| \leq X$, then $Q(x_0) = 0$.*
2. *For any integers $u, v \geq 0$, define $Q_{u,v}(x) = x^u(P(x)/N)^v$. Show that any integral linear combinations of polynomials $Q_{u,v}(x)$ is (N, P)-good.*
3. *Given as input N and $P(x)$, show that one can find in polynomial time a non-zero (N, P)-good polynomial $Q(x) \in \mathbb{Q}[x]$ such that $Q(x)$ is an integral linear combination of $Q_{0,0}(x), Q_{1,0}(x), \ldots, Q_{\delta-1,0}(x), Q_{0,1}(x)$ and*
$$\|Q(xX)\| \leq 2^{\delta/4} X^{\delta/2} N^{-1/(\delta+1)}.$$
4. *Deduce Håstad's theorem : one can find in polynomial time all the integers $x_0 \in \mathbb{Z}$ such that $|x_0| \leq N^{2/(\delta(\delta+1))}$ and $P(x_0) \equiv 0 \pmod N$.*
5. *Using the polynomials $Q_{u,v}(x)$ where $0 \leq u \leq \delta - 1$ and $0 \leq v \leq h$ for some well-chosen integer h, show Coppersmith's theorem : one can find in polynomial time all the integers $x_0 \in \mathbb{Z}$ such that $|x_0| \leq N^{1/\delta}$ and $P(x_0) \equiv 0 \pmod N$.*
6. *What can we do if $P(x)$ is not monic ?*
7. *If we want to find all roots x_0 such that $|x_0| \leq C \times N^{1/\delta}$ for some $C > 1$, what can we do ?*

---

2. The GCD generalization. (⋆ ⋆ ⋆)

We take the same notation. Let $\alpha \in \mathbb{Q}$ such that $0 < \alpha \leq 1$. We want to find all $x_0 \in \mathbb{Z}$ such that $\gcd(P(x_0), N) \geq N^\alpha$.

---

1. *Consider an integral linear combination $Q(x) \in \mathbb{Q}[x]$ of the $h\delta$ polynomials $Q_{u,v}(x)$ where $0 \leq u \leq \delta - 1$ and $0 \leq v \leq h$ for some well-chosen integer h. Show that if $x_0 \in \mathbb{Z}$ and $\gcd(P(x_0), N) \geq N^\alpha$ then the rational $Q(x_0)$ has a denominator $\leq N^{(1-\alpha)h}$.*
2. *Deduce that one can find in polynomial time all the integers $x_0 \in \mathbb{Z}$ such that $\gcd(P(x_0), N) \geq N^\alpha$ and $|x_0| \leq N^{\alpha^2/\delta}$.*
