Exercise Set 3

Prof. Kenny Paterson
Jan Gilcher, Kien Tuong Truong

Problem 1 (Polynomial-vector transformations). Denote by $\mathbb{Z}[x]$ the ring of polynomials with integer coefficients and fix an integer $X \in \mathbb{Z}$.

In the lectures, we have defined a way to convert between polynomials of at most degree d in $\mathbb{Z}[x]$ and (column) vectors in $\mathbb{Z}^{d+1}$.

Consider the following function:

$$\begin{aligned}\mathsf{poly2vec} :&\mathbb{Z}[x] \to \mathbb{Z}^{d+1} \\ &a_0 + a_1 x + a_2 x^2 + \ldots + a_d x^d \mapsto [a_0, a_1 X, a_2 X^2, \ldots, a_d X^d]\end{aligned}$$

Let $\mathsf{vec2poly}$ be the following operation:

$$\begin{aligned}\mathsf{vec2poly} :&\mathbb{Z}^{d+1} \to \mathbb{Z}[x] \\ &[v_0, v_1, v_2, \ldots, v_d] \mapsto v_0 + \frac{v_1}{X} x + \frac{v_2}{X^2} x^2 + \ldots + \frac{v_d}{X^d} x^d\end{aligned}$$

- Consider a polynomial $P(x) \in \mathbb{Z}[x]$. Prove that the result of $\mathsf{poly2vec}(P)$ can be computed by taking the coefficient vector of $P(xX)$ (i.e. the polynomial P evaluated at $x \cdot X$).
- Argue that the function $\mathsf{vec2poly}$ is well defined. That is, prove that, for any polynomial $P(x)$ of degree at most d $\mathsf{vec2poly}(\mathsf{poly2vec}(P)) = P$ and that all operations are well defined.
- Consider two polynomials $P_1(x), P_2(x) \in \mathbb{Z}[x]$ of degree at most d with a common root x_0 and their corresponding vectors $\mathbf{v}_i := \mathsf{poly2vec}(P_i)$, for $i \in \{1, 2\}$. Prove that the following operations are well-defined and their results are polynomials that also have a root in x_0.
  - $\mathsf{vec2poly}(\mathsf{poly2vec}(P_1) + \mathsf{poly2vec}(P_2))$
  - $\mathsf{vec2poly}(k \cdot \mathsf{poly2vec}(P_1)), \forall k \in R$
- Consider $\mathbb{Z}_N$, where N is an RSA modulus. Assume we use Coppersmith's method to find a small root x_0 of a polynomial $P(x) \in \mathbb{Z}_N[x]$. Argue that the matrix *after* the application of LLL consists of rows, all of which encode polynomials with x_0 as one of the roots.

Problem 2 (Generalizing Coppersmith's Method). In the lecture you have seen that Coppersmith's method can be used to find small roots of a polynomial $P(x)$ modulo N, even when the factorization of N is not known. In this exercise, we show that Coppersmith's method can also be employed to find small roots of a polynomial $P(x)$ *modulo a divisor of N, even if we do not know the divisor*. This, however, requires changing the algorithm a bit.

Let N be a large integer of unknown factorization.[1] Let b be an integer such that $b < N^\beta$ for some $0 < \beta \leq 1$. Note that the case $\beta = 1$ corresponds to the case already analyzed in the lectures. Let $P(x) \in \mathbb{Z}_b[x]$ be a polynomial of degree d with a root x_0, $|x_0| < X$ for some $X \in \mathbb{Z}$. Let h be a positive integer to be fixed later.

Consider the sequence of polynomials from the "Full Coppersmith Method" from the lectures:

$$G_{i,j}(x) = N^{h-1-j} P(x)^j x^i, \quad 0 \leq i < d,\ 0 \leq j < h$$

[1] Recall that, if the factorization is known, one can split the problem into sub-problems, one for each factor. Each sub-problem consists of finding a root modulo a prime p, which is easy. One can then compose the final solution by using the Chinese Remainder Theorem

Note that all $G_{i,j}(x_0) = 0 \mod N^{h-1}$ and that $G_{i,j}$ has degree $dj + i$. Let $\mathcal{L}$ be the lattice with $\mathsf{poly2vec}(G_{i,j})$ as basis vectors. Note that $\mathcal{L}$ has dimension dh.[2]

- Consider $P(x) = x + a$. Assume that $P(x_0) = 0 \mod b$, where $b < N^{\frac{1}{2}}$ (thus $\beta = 1/2$) and $|x_0| < X$ for some $X \in \mathbb{Z}$. Show that the method above cannot provably find this small root x_0, even for large values of h (e.g. $h = 10$).

  Hint: this requires you to show that $X < 1$. In other words, the only root that we can hope to find would be 0.

- Let $t = \lfloor dh(1/\beta - 1) \rfloor$. Consider now the following additional polynomials:

$$H_i(x) = x^i P(x)^h, \quad 0 \leq i < t$$

  Show that for $h = 2$, including both polynomials $G_{i,j}$ and H_i, we can provably find the root x_0 for the polynomial above if $X < N^{\frac{1}{6}}$.

[2]The maximum degree of any polynomial is $d \cdot (h-1) + (d-1) = dh - 1$, which means that there are $dh - 1 + 1 = dh$ coefficients