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:

$$\begin{aligned} \mathsf{poly2vec} :& \mathbb{Z}[x] \to \mathbb{Z}^{d+1} \\ & a_0 + a_1x + a_2x^2 + \ldots + a_dx^d \mapsto [a_0, a_1X, a_2X^2, \ldots, a_dX^d] \end{aligned}$$

Let 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 $x \cdot X$).

  Solution. Let $P(x) = a_0 + a_1x + \cdots + a_dx^d$. Then $P(Xx) = a_0 + a_1Xx + a_2(Xx)^2 + \ldots + a_d(Xx)^d = a_0 + a_1Xx + a_2X^2x^2 + \ldots + a_dX^dx^d$, whose coefficient vector is $[a_0, a_1X, \ldots, a_dX^d] = \mathsf{poly2vec}(P)$

- Argue that the function 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.

  Solution. Since we are in a ring, not all divisions are well defined. We first have to prove that we can always divide by X. This is easy to see, as the result of poly2vec is $[v_0, v_1, \ldots, v_d] = [a_0, a_1X, \ldots, a_dX^d]$, which means that v_i is always divisible by X^i. Proving that vec2poly is the inverse operaton of poly2vec can be done by noting that in the latter we're dividing the term of degree i by x^i and multiplying it by X^i, collecting each result in a vector, while vec2poly does exactly the opposite operation.

- 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.

  Solution. We start by defining common notation. Let $P_1 = \sum_{i=0}^{d} a_ix^i$ and $P_2 = \sum_{i=0}^{d} b_ix^i$. We assume that if either polynomial has degree $d' < d$, all coefficients with index in $\{d' + 1, ..., d\}$ are 0. Then:

  $$\mathsf{poly2vec}(P_1) = [a_0, a_1X, \ldots, a_dX^d]$$

  $$\mathsf{poly2vec}(P_2) = [b_0, b_1X, \ldots, b_dX^d]$$

  - $\mathsf{vec2poly}(\mathsf{poly2vec}(P_1) + \mathsf{poly2vec}(P_2))$

Solution.

$$\mathsf{poly2vec}(P_1) + \mathsf{poly2vec}(P_2) = [a_0 + b_0, (a_1 + b_1)X, \ldots, (a_d + b_d)X^d]$$

The latter corresponds to a new polynomial $P_{\text{sum}}(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots + (a_d + b_d)x^d = (P_1 + P_2)(x)$. Thus, this transformation simply sums two polynomials. We know that if P_1 and P_2 share a root x_0, then their sum will also have that root: $P_1(x_0) = 0 \land P_2(x_0) = 0 \Rightarrow P_1(x_0) + P_2(x_0) = (P_1 + P_2)(x_0) = 0$.

– $\mathsf{vec2poly}(k \cdot \mathsf{poly2vec}(P_1)), \forall k \in R$

Solution.

$$k \cdot \mathsf{poly2vec}(P_1) = [k \cdot a_0, k \cdot a_1 X, \ldots k \cdot a_d X^d]$$

$$\mathsf{vec2poly}(k \cdot \mathsf{poly2vec}(P_1)) = ka_0 + ka_1 x + \ldots + ka_d x^d = k \cdot P_1(x)$$

If $P_1(x_0) = 0$, then clearly $k \cdot P_1(x_0) = 0$.

- 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.

Solution. The first step is to visualize $P(x)$ as a polynomial in $\mathbb{Z}[x]$ rather than $\mathbb{Z}_N[x]$. Recall that all elements of $\mathbb{Z}_N$ are equivalence classes modulo N: $\mathbb{Z}_N = \{[0], [1], ..., [N-1]\}$. Each equivalence class is the set of all numbers that are equivalent to each other modulo N, e.g. $[3] = \{3, 3+N, 3-N, 3+2N, ...\} \subset \mathbb{Z}$ (the square bracket notation is commonly used to differentiate elements of $\mathbb{Z}_N$, which are sets, from elements of $\mathbb{Z}$, which are integers). The natural way of projecting the polynomial to $\mathbb{Z}[x]$ is to map each coefficient $[k] \in \mathbb{Z}_N$ to its smallest positive representative $k \in \mathbb{Z}$.

Next, recall that Coppersmith's method begins by finding a set of polynomials all containing a root in x_0, then converting each of the polynomials to a vector. These vectors form the rows of the basis matrix B of a lattice $\mathcal{L}$. Then, when LLL is applied to B, it will only apply elementary row operations. By the previous point, we proved that these transformations yield vectors that, when converted back into polynomials in $\mathbb{Z}[x]$, preserve the root x_0.

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.

[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

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

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

Note that all $G_{i,j}(x_0) = 0 \mod b^{h-1}$ 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. $h = 50$).

  Hint: this requires you to show that there does not exist any value of X that satisfies the Howgrave-Graham condition.

Solution. We build the matrix as above. Note that the degree of P is $d = 1$. The polynomials will all be of the form:

$$G_j(x) = N^{h-1-j}(x + a)^j, \quad 0 \le j < h$$

which induce the following basis matrix (we omit all the terms below the diagonal):

$$M = \begin{bmatrix} N^{h-1} & 0 & 0 & 0 & \dots & 0 & 0 \\ - & N^{h-2}X & 0 & 0 & \dots & 0 & 0 \\ - & - & N^{h-3}X^2 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ - & - & - & - & - & NX^{h-2} & 0 \\ - & - & - & - & - & - & X^{h-1} \end{bmatrix}$$

The corresponding lattice $\mathcal{L}$ (of dimension $n = h$) will have a determinant $\det(\mathcal{L}) = (NX)^{(h-1)+\ldots+1} = (NX)^{h(h-1)/2}$. By the LLL guarantees, we get that, after basis reduction, the first vector of the basis $\mathbf{b_1}$ will have a length of at most:

$$|\mathbf{b_1}| \le 2^{(n-1)/4} \det(\mathcal{L})^{1/n} = 2^{(h-1)/4}(NX)^{h(h-1)/(2h)} = 2^{(h-1)/4}(NX)^{(h-1)/2}$$

We want this vector to respect Howgrave-Graham's condition, where the modulus is $b < N^{\beta}$, which requires:

$$2^{(h-1)/4}(NX)^{(h-1)/2} < \frac{b^{h-1}}{\sqrt{dh}} \le \frac{(N^{\beta})^{h-1}}{\sqrt{h}} = \frac{N^{\frac{h-1}{2}}}{\sqrt{h}}$$

which, in turn, implies that:

$$X < \frac{1}{2 \cdot h^{1/(h-1)}} < 1$$

[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

Since X is a positive integer, one can see that the upper bound is too small and does not allow for any value of X.

- 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 $X < N^{\frac{1}{6}}/2^{\frac{7}{6}}$.

Solution. By plugging in $d = 1$, $h = 2$ and $\beta = 1/2$, we get that $t = 2$. Note that the i-th polynomial h_i has degree $dh + i$. Adding 2 of these polynomials, gives us the following matrix:

$$M = \left[\begin{array}{cccc} N & 0 & 0 & 0 \\ - & X & 0 & 0 \\ \hline - & - & X^2 & 0 \\ - & - & - & X^3 \end{array}\right]$$

The determinant of the matrix is $\det(\mathcal{L}) = N \cdot X^6$.

Once again, by the LLL guarantees, we get that, after basis reduction, the first vector of the basis $\mathbf{b_1}$ will have a length of at most:

$$|\mathbf{b_1}| \leq 2^{(n-1)/4} \det(\mathcal{L})^{1/n} = 2^{3/4} N^{1/4} X^{6/4}$$

We want this vector to respect Howgrave-Graham's condition, where the modulus is $b < N^\beta$, which requires:

$$2^{3/4} N^{1/4} X^{6/4} < \frac{b^{h-1}}{\sqrt{dh+t}} \leq \frac{(N^\beta)^{h-1}}{\sqrt{dh+t}} = \frac{N^{\frac{1}{2}}}{\sqrt{4}} = \frac{N^{\frac{1}{2}}}{2}$$

which, in turn, implies that:

$$X < \frac{N^{\frac{1}{6}}}{2^{\frac{7}{6}}}$$

Concretely, for a 1024-bit modulus N, this allows us to recover roots of size up to $\sim 2^{169}$ bits.