Office Hours

This Week: Monday, 2:15-3:45 p.m.

Wednesday, 11:45 p.m.-12:30 p.m.

Goal: Find a non-trivial factorization of a given $f(x) \in \mathbb{Z}[x]$ or show no such factorization exists.

Initial Idea: Begin as in the Zassenhaus algorithm. Factor $f(x)$ into irreducibles modulo p^k where p is a prime and $k \in \mathbb{Z}^+$ is large (using Berlekamp's algorithm and Hensel lifting). Suppose $h(x)$ is a monic irreducible factor of $f(x)$ mod p^k. Let $h_0(x)$ denote an irreducible factor of $f(x)$ in $\mathbb{Z}[x]$ such that $h_0(x)$ is divisible by $h(x)$ modulo p^k. (Note that the greatest common divisor of the coefficients of $h_0(x)$ is 1.)

New Goal: Show how one can determine $h_0(x)$ using $h(x)$ and without worrying about other factors of $f(x)$ modulo p^k.

Why would this improve on the Zassenhaus approach?

What is the lattice we want to use?

What is the lattice we want to use?

$$h(x) \text{ monic irreducible factor of } f(x) \text{ modulo } p^k$$

$$h_0(x) | f(x) \text{ in } \mathbb{Z}[x],\ h(x) | h_0(x) \text{ modulo } p^k$$

$$\ell = \deg h,\ m \in \{\ell, \ell+1, \ldots, n-1\}$$

m is the possible degree of $h_0(x)$

$$w(x) = a_m x^m + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

$$\longleftrightarrow \quad \vec{b} = \langle a_0, a_1, \ldots, a_m \rangle \in \mathbb{Z}^{m+1}$$

Define $\mathcal{L}$ to be the lattice in $\mathbb{Z}^{m+1}$ spanned by the vectors associated with

$$w_j(x) = \begin{cases} p^k x^{j-1} & \text{for } 1 \le j \le \ell \\ h(x) x^{j-\ell-1} & \text{for } \ell+1 \le j \le m+1. \end{cases}$$

Define $\mathcal{L}$ to be the lattice in $\mathbb{Z}^{m+1}$ spanned by the vectors associated with

$$w_j(x) = \begin{cases} p^k x^{j-1} & \text{for } 1 \le j \le \ell \\ h(x)x^{j-\ell-1} & \text{for } \ell+1 \le j \le m+1. \end{cases}$$

Example

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4x^3 + 2x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129x + 44)(x^2 + 147x + 92)(x^2 + 127x + 31)(x^7 + 24x^6 + 91x^5 + 81x^4 + 30x^3 + 20x^2 + 2x + 34)(x + 26)$$

$$m = 5$$

Example

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4x^3 + 2x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129x + 44)(x^2 + 147x + 92)(x^2 + 127x + 31)(x^7 + 24x^6 + 91x^5 + 81x^4 + 30x^3 + 20x^2 + 2x + 34)(x + 26)$$

Claim: The lattice $\mathcal{L}$ is exactly the vectors corresponding to $w(x) \in \mathbb{Z}[x]$ of degree $\leq m$ which can be expressed as some multiple of $h(x)$ mod p^k. Hence, $\vec{b}_0 \in \mathcal{L}$, where $\vec{b}_0$ corresponds to $h_0(x)$.

$$\langle 151, 0, 0, 0, 0, 0 \rangle$$
$$\langle 0, 151, 0, 0, 0, 0 \rangle$$
$$\langle 44, 129, 1, 0, 0, 0 \rangle$$
$$\langle 0, 44, 129, 1, 0, 0 \rangle$$
$$\langle 0, 0, 44, 129, 1, 0 \rangle$$
$$\langle 0, 0, 0, 44, 129, 1 \rangle$$

$$\langle 151, 0, 0, 0, 0, 0\rangle$$
$$\langle 0, 151, 0, 0, 0, 0\rangle$$
$$\langle 44, 129, 1, 0, 0, 0\rangle$$
$$\langle 0, 44, 129, 1, 0, 0\rangle$$
$$\langle 0, 0, 44, 129, 1, 0\rangle$$
$$\langle 0, 0, 0, 44, 129, 1\rangle$$

```
> f := x^14-4*x^3+2*x^2+x-3;
```

$$f := x^{14} - 4\,x^3 + 2\,x^2 + x - 3$$

```
> Factor(f) mod 151;
```

$$(x^2 + 129\,x + 44)\,(x^2 + 147\,x + 92)\,(x^2 + 127\,x + 31)\,(x^7 + 24\,x^6 + 91\,x^5 + 81\,x^4 + 30\,x^3 + 20\,x^2 + 2\,x + 34)\,(x + 26)$$

Claim: The lattice $\mathcal{L}$ is exactly the vectors corresponding to $w(x) \in \mathbb{Z}[x]$ of degree $\leq m$ which can be expressed as some multiple of $h(x)$ mod p^k. Hence, $\vec{b}_0 \in \mathcal{L}$, where $\vec{b}_0$ corresponds to $h_0(x)$.

(Go to Maple.)

We will show that in fact if p^k is large and $\vec{b}_1, \ldots, \vec{b}_{m+1}$ is a reduced basis for $\mathcal{L}$ with

$$\vec{b}_1 = \langle a_0, a_1, \ldots, a_m\rangle,$$

then

$$\vec{b}_0 = \langle a_0/d, a_1/d, \ldots, a_m/d\rangle,$$

where $d = \gcd(a_0, \ldots, a_m)$.

Example with Rough Connection

Point of Example.

The polynomial $f(x)$ factors a certain way in $\mathbb{Z}[x]$.

The polynomial $f(x)$ factors even further modulo p.

A single irreducible factor of $f(x)$ mod p by itself determines the unique irreducible factor of $f(x)$ in $\mathbb{Z}[x]$ that it divides.

$\mathbf{13 \cdot 17 \cdot 23}$

Example with Rough Connection

Point of Example.

The polynomial $f(x)$ factors a certain way in $\mathbb{Z}[x]$.

The polynomial $f(x)$ factors even further modulo p.

A single irreducible factor of $f(x)$ mod p by itself determines the unique irreducible factor of $f(x)$ in $\mathbb{Z}[x]$ that it divides.

$$13 \cdot 17 \cdot 23 = (2+3i)\cdot(2-3i)\cdot(4+i)\cdot(4-i)\cdot 23$$

$$m = (9+4i)\cdot(9-4i)\cdot(\text{other stuff})$$

Example with Rough Connection

The polynomial $f(x)$ factors a certain way in $\mathbb{Z}[x]$.

The polynomial $f(x)$ factors even further modulo p.

A single irreducible factor of $f(x)$ mod p by itself determines the unique irreducible factor of $f(x)$ in $\mathbb{Z}[x]$ that it divides.

$$13 \cdot 17 \cdot 23 = (2 + 3i) \cdot (2 - 3i) \cdot (4 + i) \cdot (4 - i) \cdot 23$$

$$m = (9 + 4i) \cdot (9 - 4i) \cdot (\text{other stuff})$$

The comparison is not fair.

For a fixed irreducible polynomial $h(x)$ mod p, there are infinitely many irreducible $h_0(x) \in \mathbb{Z}[x]$ such that $h(x)$ divides $h_0(x)$ mod p.

Example with Rough Connection

$$13 \cdot 17 \cdot 23 = (2 + 3i) \cdot (2 - 3i) \cdot (4 + i) \cdot (4 - i) \cdot 23$$

$$m = (9 + 4i) \cdot (9 - 4i) \cdot (\text{other stuff})$$

The comparison is not fair.

For a fixed irreducible polynomial $h(x)$ mod p, there are infinitely many irreducible $h_0(x) \in \mathbb{Z}[x]$ such that $h(x)$ divides $h_0(x)$ mod p.

However, there is only one possibility for $h_0(x) \in \mathbb{Z}[x]$ with $\|h_0(x)\|$ small.

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{C}[x], \quad g(x) = \sum_{j=0}^{r} b_j x^j \in \mathbb{C}[x],$$

$$n \geq 1, \quad r \geq 1, \quad a_n b_r \neq 0$$

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & 0 & \ldots & 0 \\ 0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & 0 & \ldots & 0 \\ 0 & 0 & a_n & \ldots & a_2 & a_1 & a_0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \ldots & b_0 & 0 & 0 & \ldots & 0 \\ 0 & b_r & b_{r-1} & \ldots & b_1 & b_0 & 0 & \ldots & 0 \\ 0 & 0 & b_r & \ldots & b_2 & b_1 & b_0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}$$

If $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$, then

$$R(f,g) = a_n^r g(\alpha_1) \cdots g(\alpha_n).$$

If $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$, there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $\deg u < \deg g$, $\deg v < \deg f$, and

$$f(x)u(x) + g(x)v(x) = R(f,g).$$

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$.

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$.

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$.

If $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$, then
$$R(f, g) = a_n^r \, g(\alpha_1) \cdots g(\alpha_n).$$

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$. The definition of the resultant implies that if R is large, then $\|g_0(x)\|$ must be large (since we are viewing $h_0(x)$ as fixed).

If $\alpha_1, \ldots, \alpha_n$ are the roots of $f(x)$, then
$$R(f, g) = a_n^r g(\alpha_1) \cdots g(\alpha_n).$$

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$. The definition of the resultant implies that if R is large, then $\|g_0(x)\|$ must be large (since we are viewing $h_0(x)$ as fixed). So suppose R is not large.

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$. The definition of the resultant implies that if R is large, then $\|g_0(x)\|$ must be large (since we are viewing $h_0(x)$ as fixed). So suppose R is not large. There are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that

$$h_0(x)u(x) + g_0(x)v(x) = R.$$

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$. The definition of the resultant implies that if R is large, then $\|g_0(x)\|$ must be large (since we are viewing $h_0(x)$ as fixed). So suppose R is not large. There are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that

$$h_0(x)u(x) + g_0(x)v(x) = R.$$

The left-hand side is of the form $h(x)w(x)$ modulo p^k with $h(x)$ monic and of degree $\ell \geq 1$.

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$. The definition of the resultant implies that if R is large, then $\|g_0(x)\|$ must be large (since we are viewing $h_0(x)$ as fixed). So suppose R is not large. There are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that

$$h_0(x)u(x) + g_0(x)v(x) = R.$$

The left-hand side is of the form $h(x)w(x)$ modulo p^k with $h(x)$ monic and of degree $\ell \geq 1$. This implies $p^k | R$.

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$. The definition of the resultant implies that if R is large, then $\|g_0(x)\|$ must be large (since we are viewing $h_0(x)$ as fixed). So suppose R is not large. There are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that

$$h_0(x)u(x) + g_0(x)v(x) = R.$$

The left-hand side is of the form $h(x)w(x)$ modulo p^k with $h(x)$ monic and of degree $\ell \geq 1$. This implies $p^k | R$. Hence, given p^k is large, we deduce R is large, giving us the desired conclusion that $\|g_0(x)\|$ is large. ∎

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Proof. Suppose $g_0(x) \in \mathbb{Z}[x]$ is irreducible, of degree $\leq m$, divisible by $h(x)$ mod p^k, and different from $h_0(x)$. Let R be the resultant of $h_0(x)$ and $g_0(x)$. Note that since $h_0(x)$ and $g_0(x)$ are irreducible in $\mathbb{Z}[x]$, we have $R \neq 0$. The definition of the resultant implies that if R is large, then $\|g_0(x)\|$ must be large (since we are viewing $h_0(x)$ as fixed). So suppose R is not large. There are polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that

$$h_0(x)u(x) + g_0(x)v(x) = R.$$

The left-hand side is of the form $h(x)w(x)$ modulo p^k with $h(x)$ monic and of degree $\ell \geq 1$. This implies $p^k|R$. Hence, given p^k is large, we deduce R is large, giving us the desired conclusion that $\|g_0(x)\|$ is large. ■

Claim. If p^k is large enough, then $h_0(x)$ is the only irreducible polynomial in $\mathbb{Z}[x]$ that corresponds to a short vector in $\mathcal{L}$.

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

Definition. Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$, and let $\vec{b}_1^*, \ldots, \vec{b}_n^*$ be the corresponding basis in $\mathbb{R}^n$ obtained from the Gram-Schmidt orthogonalization process, with μ_{ij} as defined before. Then we say that $\vec{b}_1, \ldots, \vec{b}_n$ is *reduced* if both of the following hold

(i) $|\mu_{ij}| \leq \dfrac{1}{2}$ for $1 \leq j < i \leq n$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \dfrac{3}{4}\|\vec{b}_{i-1}^*\|^2$ for $1 < i \leq n$.

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

Definition. Let $\vec{b}_1, \ldots, \vec{b}_n$ be a basis for a lattice $\mathcal{L}$, and let $\vec{b}_1^*, \ldots, \vec{b}_n^*$ be the corresponding basis in $\mathbb{R}^n$ obtained from the Gram-Schmidt orthogonalization process, with μ_{ij} as defined before. Then we say that $\vec{b}_1, \ldots, \vec{b}_n$ is *reduced* if both of the following hold

(i) $|\mu_{ij}| \leq \dfrac{1}{2} \quad$ for $1 \leq j < i \leq n$

(ii) $\|\vec{b}_i^* + \mu_{i,i-1}\vec{b}_{i-1}^*\|^2 \geq \dfrac{3}{4}\|\vec{b}_{i-1}^*\|^2 \quad$ for $1 < i \leq n$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \quad \Longrightarrow \quad \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$.

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$.

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$. Let $g_0(x)$ be the polynomial associated with $\vec{b}_1$.

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$. Let $g_0(x)$ be the polynomial associated with $\vec{b}_1$. Recall

$$\|h_0(x)\| \leq 2^m \|f(x)\|.$$

Claim Revised. If $\vec{b} \in \mathcal{L}$ and $g_0(x) \in \mathcal{L}$ is the polynomial associated with $\vec{b}$, then either both $R \geq p^k$ and $\|g_0(x)\|$ is large or $R = 0$. Further, if $R = 0$, then $\vec{b}$ is a multiple of $\vec{b}_0$.

In the notation of the definition,

$$\vec{b} \in \mathcal{L},\ \vec{b} \neq 0 \implies \|\vec{b}_1\| \leq 2^{(n-1)/2}\|\vec{b}\|.$$

Thus, $\vec{b}_1$ is not far from being the shortest vector in $\mathcal{L}$.

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$. Let $g_0(x)$ be the polynomial associated with $\vec{b}_1$. Recall

$$\|h_0(x)\| \leq 2^m\|f(x)\|.$$

Taking $\vec{b} = \vec{b}_0$ above (note $n = m + 1$), we get

$$\|g_0(x)\| \leq 2^{m/2}\|h_0(x)\|.$$

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$. Let $g_0(x)$ be the polynomial associated with $\vec{b}_1$. Recall

$$\|h_0(x)\| \leq 2^m\|f(x)\|.$$

Taking $\vec{b} = \vec{b}_0$ above (note $n = m+1$), we get

$$\|g_0(x)\| \leq 2^{m/2}\|h_0(x)\|.$$

Thus,

$$\|g_0(x)\| \leq 2^{3m/2}\|f(x)\|.$$

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$. Let $g_0(x)$ be the polynomial associated with $\vec{b}_1$. Recall

$$\|h_0(x)\| \le 2^m \|f(x)\|.$$

Taking $\vec{b} = \vec{b}_0$ above (note $n = m + 1$), we get

$$\|g_0(x)\| \le 2^{m/2} \|h_0(x)\|.$$

Thus,

$$\|g_0(x)\| \le 2^{3m/2} \|f(x)\|.$$

The Sylvester determinant form of the resultant (sort-of) and Hadamard's inequality give

$$|R| \le \|g_0(x)\|^m \|h_0(x)\|^m$$

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$. Let $g_0(x)$ be the polynomial associated with $\vec{b}_1$. Recall

$$\|h_0(x)\| \le 2^m \|f(x)\|.$$

Taking $\vec{b} = \vec{b}_0$ above (note $n = m + 1$), we get

$$\|g_0(x)\| \le 2^{m/2}\|h_0(x)\|.$$

Thus,

$$\|g_0(x)\| \le 2^{3m/2}\|f(x)\|.$$

The Sylvester determinant form of the resultant (sort-of) and Hadamard's inequality give

$$|R| \le \|g_0(x)\|^m \|h_0(x)\|^m$$
$$\le \left(2^{3m/2}\|f(x)\|\right)^m \left(2^m\|f(x)\|\right)^m$$

Given $f(x)$, we take $p^k > 2^{5(\deg f)^2/2}\|f(x)\|^{2\deg f}$. We want to show $\vec{b}_1$ is a multiple of $\vec{b}_0$. It suffices to show $R < p^k$. Let $g_0(x)$ be the polynomial associated with $\vec{b}_1$. Recall

$$\|h_0(x)\| \leq 2^m\|f(x)\|.$$

Taking $\vec{b} = \vec{b}_0$ above (note $n = m + 1$), we get

$$\|g_0(x)\| \leq 2^{m/2}\|h_0(x)\|.$$

Thus,

$$\|g_0(x)\| \leq 2^{3m/2}\|f(x)\|.$$

The Sylvester determinant form of the resultant (sort-of) and Hadamard's inequality give

$$\begin{aligned} |R| &\leq \|g_0(x)\|^m\|h_0(x)\|^m \\ &\leq \left(2^{3m/2}\|f(x)\|\right)^m\left(2^m\|f(x)\|\right)^m \\ &= 2^{5m^2/2}\|f(x)\|^{2m} < p^k. \quad \blacksquare \end{aligned}$$