Polynomial Factorization I

1. Kronecker's method

Suppose we want to determine if a polynomial $f(x) \in \mathbb{Z}[x]$ of degree n has a factor of degree m. *Kronecker's method* is to find integers $x_0 < x_1 < \cdots < x_m$ with $f(x_0) \neq 0,\ f(x_1) \neq 0,\ \ldots,\ f(x_m) \neq 0$.

For each sequence $u_0, u_1, \ldots, u_m$ of divisors of $f(x_0), f(x_1), \ldots, f(x_m)$ respectively, *Lagrange interpolation* gives us the *unique* polynomial $h(x)$ of degree at most m with $h(x_0) = u_0,\ h(x_1) = u_1,\ \ldots,\ h(x_m) = u_m$.

We test values of $u_0, u_1, \ldots, u_m$ until either finding a factor of $f(x)$ of degree at most m or else exhausting all the possibilities (in which case $f(x)$ has no such factor).

As an example we might search for a quadratic factor of the polynomial

$$f(x) \;=\; x^4 - 4x^3 - 17x^2 - 18x + 3.$$

Choosing $x_0 = -1$, $x_1 = 0$, $x_2 = 1$ gives

$$f(x_0) = 9, \qquad f(x_1) = 3, \qquad f(x_2) = -35,$$

which results in six choices for u_0, four choices for u_1, and eight choices for u_2. Among these 192 cases we find

$$\begin{array}{llll} u_0 = 1, & u_1 = 3, & u_2 = 7, & h(x) = x^2 + 3x + 3, \\ u_0 = 9, & u_1 = 1, & u_2 = -5, & h(x) = x^2 - 7x + 1, \end{array}$$

and sure enough

$$x^4 - 4x^3 - 17x^2 - 18x + 3 \;=\; (x^2 + 3x + 3)(x^2 - 7x + 1).$$

Kronecker's method requires that we know the complete factorizations of $f(x_0)$ through $f(x_m)$ and that we have enough time to check all the cases. And there are lots of cases, at least 2^m.

So Kronecker's method is useful only for very small values of m.

2. Approximating roots

There are ways (like Newton's method) to approximate the roots of a polynomial. For example, the polynomial

$$f(x) \;=\; x^4 - 4x^3 - 17x^2 - 18x + 3$$

has the approximate roots

$$\begin{array}{ll} w_1 = -1.5000000000 - 0.8660254038\,i, & w_3 = 0.1458980338, \\ w_2 = -1.5000000000 + 0.8660254038\,i, & w_4 = 6.8541019662. \end{array}$$

To search for quadratic factors of $f(x)$ we can take the six pairs of roots (w_j, w_k) with $1 \le j < k \le 4$ and form the polynomial

$$h_{jk}(x) \;=\; x^2 - (w_j + w_k)\,x + w_j w_k.$$

We get

$$\begin{aligned}
h_{12}(x) &= x^2 + 3.0000000000\,x + 3.0000000000, \\
h_{13}(x) &= x^2 + (1.3541019662 + 0.8660254038\,i)\,x \\
&\qquad - 0.2188470506 - 0.1263514036\,i, \\
h_{23}(x) &= x^2 + (1.3541019662 - 0.8660254038\,i)\,x \\
&\qquad - 0.2188470506 + 0.1263514036\,i, \\
h_{14}(x) &= x^2 - (5.3541019662 - 0.8660254038\,i)\,x \\
&\qquad - 10.2811529494 - 5.9358264229\,i, \\
h_{24}(x) &= x^2 - (5.3541019662 + 0.8660254038\,i)\,x \\
&\qquad - 10.2811529494 + 5.9358264229\,i, \\
h_{34}(x) &= x^2 - 7.0000000000\,x + 1.0000000000.
\end{aligned}$$

This is a simple enough idea, but like Kronecker's method it is practical only for very small m. To exclude the possibility of a degree m factor of a polynomial of degree n would require $\binom{n}{m}$ tests, and if n and m are large then

$$\binom{n}{m} \;\sim\; \frac{2^n}{\sqrt{\pi n/2}}\, e^{-\frac{(2m-n)^2}{2n}}.$$

3. Factoring via short vectors

The LLL algorithm

Let's look at the example

$$x^4 + bx^3 + cx^2 + dx + e \;=\; (x^2 + px + q)(x^2 + rx + s)$$

with

$$\begin{aligned} f(x) &= x^4 + bx^3 + cx^2 + dx + e, \\ g(x) &= x^2 + px + q, \\ h(x) &= x^2 + rx + s. \end{aligned}$$

If α is a root of f, *i.e.*, $f(\alpha) = 0$, then either $g(\alpha) = 0$ or $h(\alpha) = 0$.

For any given $\lambda > 0$ let

$$M_\lambda \;=\; \begin{bmatrix} \lambda\,\alpha^2 & 1 & 0 & 0 \\ \lambda\,\alpha^1 & 0 & 1 & 0 \\ \lambda\,\alpha^0 & 0 & 0 & 1 \end{bmatrix}.$$

If c_1, c_2, c_3 are integers then

$$\begin{aligned} (c_1,\, c_2,\, c_3) \cdot M_\lambda &= c_1 \cdot \mathrm{row}(1, M_\lambda) \;+\; c_2 \cdot \mathrm{row}(2, M_\lambda) \;+\; c_3 \cdot \mathrm{row}(3, M_\lambda) \\ &= \big(\lambda\, c_1\, \alpha^2 + \lambda\, c_2\, \alpha + \lambda\, c_3,\; c_1,\; c_2,\; c_3\big) \end{aligned}$$

and in particular if $g(\alpha) = 0$ then

$$(1,\, p,\, q) \cdot M_\lambda \;=\; \big(\lambda\, g(\alpha),\, 1,\, p,\, q\big) \;=\; \big(0,\, 1,\, p,\, q\big)$$

and if $h(\alpha) = 0$ then

$$(1,\, r,\, s) \cdot M_\lambda \;=\; \big(\lambda\, h(\alpha),\, 1,\, r,\, s\big) \;=\; \big(0,\, 1,\, r,\, s\big).$$

The ingenious trick we will now perform is to *inflate* the powers of α (by choosing a large value for λ) and then to exploit a *short vector algorithm* to find integers c_1, c_2, c_3 such that

$$\begin{aligned} |\lambda\, c_1\, \alpha^2 + \lambda\, c_2\, \alpha + \lambda\, c_3| &\ll \lambda, \\ c_1\, \alpha^2 + c_2\, \alpha + c_3 &\approx 0. \end{aligned}$$

Ordinarily we would work with an approximate value for α, which explains why the expression $c_1\, \alpha^2 + c_2\, \alpha + c_3$ is only approximately 0.

Let's again consider the polynomial $f(x) = x^4 - 4x^3 - 17x^2 - 18x + 3$.

If $\alpha = 6.854101966249684\ldots$ then $\alpha^2 = 46.978713763747791\ldots$ and $f(\alpha) = 0$.

With $\lambda = 10^{10}$ we have

$$M_\lambda \;=\; \begin{bmatrix} \mathrm{round}(\lambda\alpha^2) & 1 & 0 & 0 \\ \mathrm{round}(\lambda\alpha^1) & 0 & 1 & 0 \\ \mathrm{round}(\lambda\alpha^0) & 0 & 0 & 1 \end{bmatrix} \;=\; \begin{bmatrix} 469787137637 & 1 & 0 & 0 \\ 68541019662 & 0 & 1 & 0 \\ 10000000000 & 0 & 0 & 1 \end{bmatrix}.$$

The *LLL algorithm* (presented below) returns

$$\mathrm{LLL}(M_\lambda) \;=\; \begin{bmatrix} 3 & 1 & -7 & 1 \\ 77803 & -8775 & 45969 & 97162 \\ -327891 & 7305 & -95248 & 309660 \end{bmatrix}$$

which reveals the factor $h(x) = x^2 - 7x + 1$.

Another example: the polynomial

$$f(x) \;=\; x^6 - x^5 + 4x^4 - 7x^3 + 11x^2 + 8x - 56$$

has these six roots:

$$\begin{aligned} \alpha_1 &= -1.38829144100474453\ldots, \\ \alpha_2,\, \alpha_3 &= -0.80585427949762773\ldots \pm 2.26121155188278563\ldots\, i, \\ \alpha_4,\, \alpha_5 &= 1.14238738078245477\ldots \pm 1.66614757361205966\ldots\, i, \\ \alpha_6 &= 1.71522523843509044\ldots, \end{aligned}$$

so that $\alpha_1^2 = 1.92735312516703007\ldots$ and $\alpha_1^3 = -2.67572784746313394\ldots$.

With $\lambda = 10^{12}$ we have

$$M_\lambda \;=\; \begin{bmatrix} \mathrm{round}(\lambda\alpha_1^3) & 1 & 0 & 0 & 0 \\ \mathrm{round}(\lambda\alpha_1^2) & 0 & 1 & 0 & 0 \\ \mathrm{round}(\lambda\alpha_1^1) & 0 & 0 & 1 & 0 \\ \mathrm{round}(\lambda\alpha_1^0) & 0 & 0 & 0 & 1 \end{bmatrix} \;=\; \begin{bmatrix} -2675727847463 & 1 & 0 & 0 & 0 \\ 1927353125167 & 0 & 1 & 0 & 0 \\ -1388291441005 & 0 & 0 & 1 & 0 \\ 1000000000000 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The LLL algorithm returns

$$\mathrm{LLL}(M_\lambda) \;=\; \begin{bmatrix} -2 & 1 & 3 & 8 & 8 \\ 2119 & -2523 & -2010 & 1872 & -278 \\ 5743 & 1811 & 4358 & 1310 & -1735 \\ 5310 & 3692 & -1027 & -4443 & 5690 \end{bmatrix}$$

which gives us the factor $h(x) = x^3 + 3x^2 + 8x + 8$.

On the other hand,

$$\begin{aligned}
\alpha_4 &= 1.14238738078245477\ldots + 1.66614757361205966\ldots i,\\
\alpha_4^2 &= -1.47099880928235644\ldots + 3.80677192523144619\ldots i,\\
\alpha_4^3 &= -8.02309428338906396\ldots + 1.89790711202930749\ldots i,
\end{aligned}$$

and with $\lambda = 10^8$ we have

$$M_\lambda \;=\; \begin{bmatrix} \mathrm{round}(\Re(\lambda\alpha_4^3)) & \mathrm{round}(\Im(\lambda\alpha_4^3)) & 1 & 0 & 0 & 0 \\ \mathrm{round}(\Re(\lambda\alpha_4^2)) & \mathrm{round}(\Im(\lambda\alpha_4^2)) & 0 & 1 & 0 & 0 \\ \mathrm{round}(\Re(\lambda\alpha_4^1)) & \mathrm{round}(\Im(\lambda\alpha_4^1)) & 0 & 0 & 1 & 0 \\ \mathrm{round}(\Re(\lambda\alpha_4^0)) & \mathrm{round}(\Im(\lambda\alpha_4^0)) & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} -802309428 & 189790711 & 1 & 0 & 0 & 0 \\ -147099881 & 380677193 & 0 & 1 & 0 & 0 \\ 114238738 & 166614757 & 0 & 0 & 1 & 0 \\ 100000000 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The LLL $\mathrm{algorithm}$ returns

$$\mathrm{LLL}(M_\lambda) \;=\; \begin{bmatrix} 0 & -5 & 1 & -4 & 8 & -7 \\ -315602 & -138150 & 4916 & 6490 & -20428 & 72325 \\ 117192 & 196407 & 61850 & -108578 & 177623 & 133596 \\ 2111 & -207284 & 27949 & -19955 & 13756 & 179169 \end{bmatrix}$$

which exposes the factor $h(x) = x^3 - 4x^2 + 8x - 7$.

You probably noticed that in constructing M_λ we made all its entries *integers*. There is such a thing as *floating-point error*, and its effects are disgusting. By working only with integers we avoid floating-point error entirely.

You also might be wondering how big λ should be. For now we will ignore that question. We will come back to it later in connection with the more efficient factorization methods that we will present below.

The use of short vector techniques is a big step forward, because the LLL algorithm does its work in *polynomial time* (as a function of the number of rows of M_λ and the size of its entries).

So now we have a method that works for all values of n and m and is not prohibitively time-consuming.

LLL lattice basis reduction

Input: Lattice basis vectors $\{ v_1, \ldots, v_n \}$.
Output: LLL-reduced basis $\{ v_1, \ldots, v_n \}$.

$w_0 \leftarrow (0, \ldots, 0)$; $k \leftarrow 1$;
while $k \le n$ **do**
  $w_k \leftarrow v_k$;
  for $j \leftarrow k-1, k-2, \ldots, 1$ **do**
    $r_j \leftarrow \langle w_k, w_j\rangle / \langle w_j, w_j\rangle$; $w_k \leftarrow w_k - r_j w_j$;
    $h_j \leftarrow \mathrm{round}\big(\langle v_k, w_j\rangle / \langle w_j, w_j\rangle\big)$; $v_k \leftarrow v_k - h_j v_j$;
  od;
  if $\langle w_{k-1}, w_{k-1}\rangle > 2\langle w_k, w_k\rangle$ **then**
    $v_k \leftrightarrow v_{k-1}$; $k \leftarrow k-1$;
  else
    $k \leftarrow k+1$;
  fi;
od;

Exercises. *Assume the LLL algorithm has terminated and let*

$$D \;=\; \|w_1\| \cdots \|w_n\|.$$

Prove the following.

1. *The vectors $w_1, \ldots, w_n$ are orthogonal, i.e., $\langle w_k, w_j\rangle = 0$ if $k \ne j$.*
2. *For $k = 1, \ldots, n$ and $j = 1, \ldots, k$ we have $\|w_j\|^2 \le 2^{k-j}\|w_k\|^2$.*
3. *For $k = 1, \ldots, n$ we have*
$$v_k \;=\; \theta_{k,1}w_1 + \theta_{k,2}w_2 + \cdots + \theta_{k,k-1}w_{k-1} + w_k$$
with $|\theta_{k,j}| \le \frac{1}{2}$ for $j = 1, \ldots, k-1$.
4. *For $k = 1, \ldots, n$ we have $\|v_k\|^2 \le 2^{k-1}\|w_k\|^2$.*
5. $\|v_1\| \cdots \|v_n\| \;\le\; 2^{n(n-1)/4}\, D$.
6. $\|v_1\| \;\le\; 2^{n(n-1)/4}\, D^{1/n}$.

Example. Here is how LLL revealed the factor $h(x) = x^2 - 7x + 1$ in the example above.

	469787137637	1	0	0
	68541019662	0	1	0
	10000000000	0	0	1
$v_2 \leftrightarrow v_1$	68541019662	0	1	0
	469787137637	1	0	0
	10000000000	0	0	1
$v_2 \leftarrow v_2 - 7v_1$	68541019662	0	1	0
	−9999999997	1	−7	0
	10000000000	0	0	1
$v_2 \leftrightarrow v_1$	−9999999997	1	−7	0
	68541019662	0	1	0
	10000000000	0	0	1
$v_2 \leftarrow v_2 + 7v_1$	−9999999997	1	−7	0
	−1458980317	7	−48	0
	10000000000	0	0	1
$v_2 \leftrightarrow v_1$	−1458980317	7	−48	0
	−9999999997	1	−7	0
	10000000000	0	0	1
$v_2 \leftarrow v_2 - 7v_1$	−1458980317	7	−48	0
	212862222	−48	329	0
	10000000000	0	0	1
$v_2 \leftrightarrow v_1$	212862222	−48	329	0
	−1458980317	7	−48	0
	10000000000	0	0	1
$v_2 \leftarrow v_2 + 7v_1$	212862222	−48	329	0
	31055237	−329	2255	0
	10000000000	0	0	1
$v_2 \leftrightarrow v_1$	31055237	−329	2255	0
	212862222	−48	329	0
	10000000000	0	0	1
$v_2 \leftarrow v_2 - 7v_1$	31055237	−329	2255	0
	−4524437	2255	−15456	0
	10000000000	0	0	1
$v_2 \leftrightarrow v_1$	−4524437	2255	−15456	0
	31055237	−329	2255	0
	10000000000	0	0	1
$v_2 \leftarrow v_2 + 7v_1$	−4524437	2255	−15456	0
	−615822	15456	−105937	0
	10000000000	0	0	1
$v_2 \leftrightarrow v_1$	−615822	15456	−105937	0
	−4524437	2255	−15456	0
	10000000000	0	0	1
$v_2 \leftarrow v_2 - 7v_1$	−615822	15456	−105937	0
	−213683	−105937	726103	0
	10000000000	0	0	1
$v_3 \leftarrow v_3 + 2255v_2 + 15456v_1$	−615822	15456	−105937	0
	−213683	−105937	726103	0
	3	1	−7	1
$v_3 \leftrightarrow v_2 \leftrightarrow v_1$	3	1	−7	1
	−615822	15456	−105937	0
	−213683	−105937	726103	0
$v_2 \leftarrow v_2 + 18174v_1$	3	1	−7	1
	−561300	33630	−233155	18174
	−213683	−105937	726103	0
$v_3 \leftarrow v_3 + 97162v_1$	3	1	−7	1
	−561300	33630	−233155	18174
	77803	−8775	45969	97162
$v_3 \leftrightarrow v_2$	3	1	−7	1
	77803	−8775	45969	97162
	−561300	33630	−233155	18174
$v_3 \leftarrow v_3 + 3v_2$	3	1	−7	1
	77803	−8775	45969	97162
	−327891	7305	−95248	309660

4. The p-adic numbers

For a prime p, the *p-adic digits* are $0, 1, \ldots, p-1$, *i.e.*, the digits in base p.

A *p-adic integer* is just an integer expanded in base p, but with infinitely many digits. Addition, subtraction, and multiplication are carried out just as you would imagine (except that they never end).

The ring of p-adic integers is denoted $\mathbb{Z}_p$.

If a p-adic integer has 0 in all but finitely many places then it actually has a finite value; it is in fact a nonnegative *rational* integer.

Suppose the p-adic integer α has $p-1$ in all but finitely many places, say from the p^ks digit onwards. Then the p-adic integer $\beta = \alpha + p^k$ has 0 in all but finitely many places, hence is a rational integer, so $\alpha = \beta - p^k$ is also a rational integer (albeit a nonnonegative one, seeing as how $\beta < p^k$). Conversely, a negative rational integer α satisfies $0 < \alpha + p^k < p^k$ for some k, so the p-adic representation of $\alpha + p^k$ has 0 from the p^ks digit onwards, so the p-adic representation of $\alpha = (\alpha + p^k) - p^k$ has $p-1$ from the p^ks digit onwards.

Let α_k denote the p-adic integer α truncated to the left of the p^ks digit. If $\alpha_0 \neq 0$ then $\gcd(\alpha_k, p^k) = 1$ and hence the congruence $\alpha_k\beta_k \equiv 1 \pmod{p^k}$ has a solution β_k and this solution is unique modulo p^k. The sequence $\beta_0, \beta_1, \beta_2, \ldots$ is *p-adically convergent*: for $h \geq k$ the first k digits of β_h and β_k coincide, and so the sequence $\beta_0, \beta_1, \beta_2, \ldots$ determines a p-adic integer β, and $\alpha\beta = 1$.

Thus every rational number a/b with $a, b \in \mathbb{Z}$ and $p \nmid b$ is included in $\mathbb{Z}_p$. To get the others we define the *field of p-adic numbers*:

$$\mathbb{Q}_p \;=\; \big\{\, p^k\alpha \;\big|\; \alpha \in \mathbb{Z}_p,\, k \in \mathbb{Z} \,\big\}.$$

Example. In $\mathbb{Z}_7$ we have

$$5^{-1} \;=\; [\cdots 1\,2\,5\,4\,1\,2\,5\,4\,1\,2\,5\,4\,1\,2\,5\,4\,1\,2\,5\,4\,1\,2\,5\,4\,1\,2\,5\,4\,1\,3]_7,$$

while in $\mathbb{Z}_5$ we have

$$7^{-1} \;=\; [\cdots 4\,1\,2\,0\,3\,2\,4\,1\,2\,0\,3\,2\,4\,1\,2\,0\,3\,2\,4\,1\,2\,0\,3\,2\,4\,1\,2\,0\,3\,3]_5.$$

Exercise. *Show that the p-adic integer α is rational if and only if its p-adic expansion is eventually periodic.*

Since the congruence $x^2 \equiv 5 \pmod 7$ has no integer solution there is no square root of 5 in $\mathbb{Z}_7$. On the other hand,

$$\sqrt{2} \;=\; [\cdots 3\,6\,5\,5\,3\,6\,6\,2\,3\,1\,6\,4\,1\,1\,2\,0\,1\,1\,2\,6\,6\,4\,2\,1\,2\,1\,6\,2\,1\,3]_7.$$

Exercise. *Let $\alpha = [\cdots d_3\, d_2\, d_1\, d_0\,]_p$ be a p-adic integer with $d_0 \neq 0$.*

- *Show that α has an inverse in $\mathbb{Z}_p$.*
- *Show that α has a square root in $\mathbb{Z}_p$ if and only if the congruence $x^2 \equiv d_0 \pmod p$ has an integer solution.*

The *p-adic valuation* is the map

$$v_p : \mathbb{Z}_p \to \mathbb{Z} \cup \{\infty\}$$

defined as $v_p(\alpha)$ being the number of consecutive zeros at the beginning of the p-adic expansion of α. We extend v_p to $\mathbb{Q}_p$ by defining

$$v_p(p^k\alpha) = k + v_p(\alpha).$$

Exercise. *Show that the p-adic valuation has the following properties.*

- $v_p(\alpha) = \infty$ *if and only if* $\alpha = 0$.
- $v_p(\alpha\beta) = v_p(\alpha) + v_p(\beta)$.
- $v_p(\alpha + \beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$.
- $v_p(\alpha + \beta) = \min\{v_p(\alpha), v_p(\beta)\}$ *if* $v_p(\alpha) \neq v_p(\beta)$.

Sometimes it is convenient to use the *p-adic absolute value*:

$$|\alpha|_p \;=\; p^{-v_p(\alpha)}.$$

Now it makes sense to write $\alpha_n \to \alpha$ when $|\alpha_n - \alpha|_p \to 0$.

Exercise. *Show that the p-adic absolute value has the following properties.*

- $|\alpha|_p = 0$ *if and only if* $\alpha = 0$.
- $|\alpha\beta|_p = |\alpha|_p|\beta|_p$.
- $|\alpha + \beta|_p \leq \max\{|\alpha|_p, |\beta|_p\}$.
- $|\alpha + \beta|_p = \max\{|\alpha|_p, |\beta|_p\}$ *if* $|\alpha|_p \neq |\beta|_p$.

5. Hensel factorization

Returning to the example

$$f(x) \;=\; x^4 - 4\,x^3 - 17\,x^2 - 18\,x + 3$$

let us use the Euclidean algorithm to compute $\gcd\big(f(x), f'(x)\big)$.

The successive remainders are

$$\begin{aligned}
f(x) \;&=\; r_0(x) \;=\; x^4 - 4\,x^3 - 17\,x^2 - 18\,x + 3,\\
f'(x) \;&=\; r_1(x) \;=\; 4\,x^3 - 12\,x^2 - 34\,x - 18,\\
r_0(x) \textbf{ mod } r_1(x) \;&=\; r_2(x) \;=\; -\tfrac{23}{2}\,x^2 - 22\,x - \tfrac{3}{2},\\
r_1(x) \textbf{ mod } r_2(x) \;&=\; r_3(x) \;=\; \tfrac{1626}{529}\,x - \tfrac{8166}{529},\\
r_2(x) \textbf{ mod } r_3(x) \;&=\; r_4(x) \;=\; -\tfrac{29526135}{73441},\\
r_3(x) \textbf{ mod } r_4(x) \;&=\; r_5(x) \;=\; 0
\end{aligned}$$

and so $f(x)$ and $f'(x)$ have no factors in common, *i.e.*, $\gcd(f(x), f'(x)) = 1$.

Now let us repeat this computation but performing every operation *modulo p* for various primes p. The results are in Table 1.

In these examples we are in effect computing in $\mathbb{F}_p$, the *field with p elements*. We can summarize our results as

$$\gcd\big(f(x),\, f'(x)\big) \;=\; \begin{cases} x^4 + x^2 + 1 & \text{in } F_2[x],\\ x^2 + x & \text{in } F_3[x],\\ x + 4 & \text{in } F_5[x],\\ 1 & \text{in } F_7[x]. \end{cases}$$

We usually think of the gcd as a monic polynomial, so we have factored out the leading coefficients.

A prime p is *good* for $f(x)$ if $\gcd\big(f(x),\, f'(x)\big) = 1$ in $\mathbb{F}_p[x]$. From our list we see that 2, 3, and 5 are bad and 7 is good for this particular choice of $f(x)$.

$$\begin{array}{lrcccl}
p=2: & f(x) \textbf{ mod } 2 &=& r_0(x) &=& x^4 + x^2 + 1\\
& f'(x) \textbf{ mod } 2 &=& r_1(x) &=& 0\\[1ex]
p=3: & f(x) \textbf{ mod } 3 &=& r_0(x) &=& x^4 + 2x^3 + x^2\\
& f'(x) \textbf{ mod } 3 &=& r_1(x) &=& x^3 + 2x\\
& \big[r_0(x) \textbf{ mod } r_1(x)\big] \textbf{ mod } 3 &=& r_2(x) &=& 2x^2 + 2x \;\equiv\; 2(x^2 + x)\\
& \big[r_1(x) \textbf{ mod } r_2(x)\big] \textbf{ mod } 3 &=& r_3(x) &=& 0\\[1ex]
p=5: & f(x) \textbf{ mod } 5 &=& r_0(x) &=& x^4 + x^3 + 3x^2 + 2x + 3\\
& f'(x) \textbf{ mod } 5 &=& r_1(x) &=& 4x^3 + 3x^2 + x + 2\\
& \big[r_0(x) \textbf{ mod } r_1(x)\big] \textbf{ mod } 5 &=& r_2(x) &=& x^2 + 3x + 1\\
& \big[r_1(x) \textbf{ mod } r_2(x)\big] \textbf{ mod } 5 &=& r_3(x) &=& 4x + 1 \;\equiv\; 4(x + 4)\\
& \big[r_2(x) \textbf{ mod } r_3(x)\big] \textbf{ mod } 5 &=& r_4(x) &=& 0\\[1ex]
p=7: & f(x) \textbf{ mod } 7 &=& r_0(x) &=& x^4 + 3x^3 + 4x^2 + 3x + 3\\
& f'(x) \textbf{ mod } 7 &=& r_1(x) &=& 4x^3 + 2x^2 + x + 3\\
& \big[r_0(x) \textbf{ mod } r_1(x)\big] \textbf{ mod } 7 &=& r_2(x) &=& 6x^2 + 6x + 2\\
& \big[r_1(x) \textbf{ mod } r_2(x)\big] \textbf{ mod } 7 &=& r_3(x) &=& 4x + 6\\
& \big[r_2(x) \textbf{ mod } r_3(x)\big] \textbf{ mod } 7 &=& r_4(x) &=& 3 \;\equiv\; 3 \cdot 1\\
& \big[r_3(x) \textbf{ mod } r_4(x)\big] \textbf{ mod } 7 &=& r_5(x) &=& 0
\end{array}$$

Table 1: GCD **mod** p

The first step in our p-adic construction will be *to factorize* $f(x)$ *modulo* p (or in other words *to factorize* $f(x)$ *in* $\mathbb{F}_p[x]$). This means to find (monic) polynomials $f_1(x), \ldots, f_r(x)$ such that

$$f(x) - f_1(x) \cdots f_r(x) \in p\mathbb{Z}[x]$$

(*i.e.*, $f(x) = f_1(x) \cdots f_r(x)$ in $\mathbb{F}_p[x]$). You can check that

$$\begin{aligned}
f(x) - (x^2+x+1)^2 &= 2\,(-3x^3 - 10x^2 - 10x + 1) &\in 2\mathbb{Z}[x],\\
f(x) - x^2(x+1)^2 &= 3\,(-2x^3 - 6x^2 - 6x + 1) &\in 3\mathbb{Z}[x],\\
f(x) - (x^2+3x+3)(x+4)^2 &= 5\,(-3x^3 - 12x^2 - 18x - 9) &\in 5\mathbb{Z}[x],\\
f(x) - (x+4)(x+6)(x^2+1) &= 7\,(-2x^3 - 6x^2 - 4x - 3) &\in 7\mathbb{Z}[x];
\end{aligned}$$

that is to say,

$$f(x) = \begin{cases} (x^2+x+1)^2 & \text{in } F_2[x],\\ x^2(x+1)^2 & \text{in } F_3[x],\\ (x^2+3x+3)(x+4)^2 & \text{in } F_5[x],\\ (x+4)(x+6)(x^2+1) & \text{in } F_7[x]. \end{cases}$$

Exercise. *Show that*

- x^2+x+1 *is irreducible in* $F_2[x]$,
- x^2+3x+3 *is irreducible in* $F_5[x]$.

You might have noticed in the tables above that for

$$f(x) = x^4 - 4\,x^3 - 17\,x^2 - 18\,x + 3$$

the conditions

- p is a good prime for $f(x)$,
- the $\gcd$ of $f(x)$ and $f'(x)$ in $\mathbb{F}_p[x]$ is 1,
- $f(x)$ has no repeated factors in $\mathbb{F}_p[x]$

all hold for $p = 7$ and all fail to hold for $p = 2$, 3, or 5.

And indeed, the three conditions are equivalent in general.

The mod-p factorization of $f(x)$ for a good prime p is the starting point of *Hensel factorization*, a highly efficient procedure that is the standard factorization algorithm in many computer-algebra systems.

Supposing $f(x)$ has degree n, we don't want to check all $p^{\lfloor n/2 \rfloor}$ monic polynomials in $\mathbb{F}_p[x]$ of degree at most $n/2$ before concluding that $f(x)$ is irreducible (in $\mathbb{F}_p[x]$). Instead, we have the choice of two effective mod-p factorization algorithms, the Berlekamp algorithm (deterministic, but with execution time proportional to p) and the Cantor-Zassenhaus algorithm (fast, but probabilistic).

Anyhow, let's not worry about that. Let us simply assume that p is a good prime for $f(x)$ and that we have polynomials $f_1(x), \ldots, f_r(x)$ that are relatively prime in $\mathbb{F}_p[x]$ such that $f(x) = f_1(x) \cdots f_r(x)$ in $\mathbb{F}_p[x]$. Since $f_1(x), \ldots, f_r(x)$ are relatively prime we can find $a_1(x), \ldots, a_r(x)$ in $\mathbb{F}_p[x]$ such that

$$\sum_{j=1}^{r} \Big(a_j(x) \prod_{k \neq j} f_k(x) \Big) = 1$$

in $\mathbb{F}_p[x]$. In other words, we have

$$\begin{aligned}
f(x) &\equiv f_1(x) \cdots f_r(x) && \pmod{p\mathbb{Z}[x]},\\
1 &\equiv \sum_{j=1}^{r} \Big(a_j(x) \prod_{k \neq j} f_k(x) \Big) && \pmod{p\mathbb{Z}[x]}.
\end{aligned}$$

Exercise: Hensel Lifting (with p a good prime).

Suppose $f(x)$, $f_1(x)$, $f_2(x)$, $f_3(x)$ *are monic polynomials in* $\mathbb{Z}[x]$ *such that*

$$f(x) \equiv f_1(x)\, f_2(x)\, f_3(x) \pmod{p^e\, \mathbb{Z}[x]},$$

with $e \geq 1$, *and* $a_1(x)$, $a_2(x)$, $a_3(x)$ *are polynomials in* $\mathbb{Z}[x]$ *such that*

$$1 \equiv a_1(x) f_2(x) f_3(x) + a_2(x) f_1(x) f_3(x) + a_3(x) f_1(x) f_2(x) \pmod{p\, \mathbb{Z}[x]}.$$

Show that if

$$u(x) = \frac{f(x) - f_1(x)\, f_2(x)\, f_3(x)}{p^e},$$

$$\begin{aligned}
g_1(x) &= \big[\, a_1(x)\, u(x) \ \mathbf{mod}\ f_1(x) \,\big] \ \mathbf{mod}\ p, & \widehat{f}_1(x) &= f_1(x) + p^e g_1(x),\\
g_2(x) &= \big[\, a_2(x)\, u(x) \ \mathbf{mod}\ f_2(x) \,\big] \ \mathbf{mod}\ p, & \widehat{f}_2(x) &= f_2(x) + p^e g_2(x),\\
g_3(x) &= \big[\, a_3(x)\, u(x) \ \mathbf{mod}\ f_3(x) \,\big] \ \mathbf{mod}\ p, & \widehat{f}_3(x) &= f_3(x) + p^e g_3(x),
\end{aligned}$$

then $\widehat{f}_1(x)$, $\widehat{f}_2(x)$, $\widehat{f}_3(x)$ *are monic and*

$$f(x) \equiv \widehat{f}_1(x)\, \widehat{f}_2(x)\, \widehat{f}_3(x) \pmod{p^{e+1}\, \mathbb{Z}[x]}.$$

Let's apply Hensel lifting with

$$f(x) \;=\; x^4 - 4\,x^3 - 17\,x^2 - 18\,x + 3$$

and $p = 7$. Earlier we found that if

$$f_1(x) = x + 4, \quad f_2(x) = x + 6, \quad f_3(x) = x^2 + 1$$

then

$$f(x) \;\equiv\; f_1(x)\,f_2(x)\,f_3(x) \pmod{7\mathbb{Z}[x]}.$$

If $a_1(x) = c_{10}$ and $a_2(x) = c_{20}$ and $a_3(x) = c_{31}x + c_{30}$ then the equation

$$a_1(x)\,f_2(x)\,f_3(x) + a_2(x)\,f_1(x)\,f_3(x) + a_3(x)\,f_1(x)\,f_2(x) \;=\; 1$$

is equivalent to the 4×4 linear system

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 6 & 4 & 3 & 1 \\ 1 & 1 & 3 & 3 \\ 6 & 4 & 0 & 3 \end{bmatrix} \begin{bmatrix} c_{10} \\ c_{20} \\ c_{31} \\ c_{30} \end{bmatrix} \;=\; \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

which has the solution

$$\begin{bmatrix} c_{10} \\ c_{20} \\ c_{31} \\ c_{30} \end{bmatrix} \;=\; \begin{bmatrix} -\frac{5}{26} \\ \frac{11}{26} \\ -\frac{3}{13} \\ \frac{2}{13} \end{bmatrix} \;\equiv\; \begin{bmatrix} 6 \\ 5 \\ 3 \\ 5 \end{bmatrix} \quad \pmod{7\mathbb{Z}^4}.$$

So we let

$$a_1(x) = 6, \quad a_2(x) = 5, \quad a_3(x) = 3x + 5$$

and confirm that

$$\begin{aligned} &a_1(x)\,f_2(x)\,f_3(x) + a_2(x)\,f_1(x)\,f_3(x) + a_3(x)\,f_1(x)\,f_2(x) \\ &\qquad \;=\; 7\,(2x^3 + 10x^2 + 5x + 10) + 1 \;\equiv\; 1 \pmod{7\mathbb{Z}[x]}. \end{aligned}$$

With

$$u(x) \;=\; \frac{f(x) - f_1(x)\,f_2(x)\,f_3(x)}{p} \;=\; -2x^3 - 6x^2 - 4x - 3$$

we have

$$\begin{aligned} g_1(x) &= \big[\,6\,(-2x^3 - 6x^2 - 4x - 3)\ \textbf{mod}\ (x+4)\,\big]\ \textbf{mod}\ 7 \;=\; 4, \\ g_2(x) &= \big[\,5\,(-2x^3 - 6x^2 - 4x - 3)\ \textbf{mod}\ (x+6)\,\big]\ \textbf{mod}\ 7 \;=\; 2, \\ g_3(x) &= \big[\,(3x+5)(-2x^3 - 6x^2 - 4x - 3)\ \textbf{mod}\ (x^2+1)\,\big]\ \textbf{mod}\ 7 \;=\; 6x. \end{aligned}$$

so that

$$\widehat{f}_1(x) \;=\; x + 32, \quad \widehat{f}_2(x) \;=\; x + 20, \quad \widehat{f}_3(x) \;=\; x^2 + 42x + 1$$

and

$$f(x) \;-\; \widehat{f}_1(x)\,\widehat{f}_2(x)\,\widehat{f}_3(x) \;=\; 7^2(-2x^3 - 58x^2 - 550x - 13) \;\in\; p^2\mathbb{Z}[x].$$

And now, if we replace $f_1(x) \leftarrow \widehat{f}_1(x)$, $f_2(x) \leftarrow \widehat{f}_2(x)$, $f_3(x) \leftarrow \widehat{f}_3(x)$, we have satisfied the conditions of the exercise with $e = 2$. We can iterate!

Continuing on, this is what we get.

e	$f_1(x)$	$f_2(x)$	$f_3(x)$
1	$x + 4$	$x + 6$	$x^2 + 1$
2	$x + 32$	$x + 20$	$x^2 + 42x + 1$
3	$x + 326$	$x + 20$	$x^2 + 336x + 1$
4	$x + 1355$	$x + 1049$	$x^2 + 2394x + 1$
5	$x + 1355$	$x + 15455$	$x^2 + 16800x + 1$
6	$x + 34969$	$x + 82683$	$x^2 + 117642x + 1$
7	$x + 740863$	$x + 82683$	$x^2 + 823536x + 1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

with

$$f(x) \;\equiv\; f_1(x)\,f_2(x)\,f_3(x) \pmod{7^e\,\mathbb{Z}[x]}$$

in each case.

Some of the coefficients of $f_1(x)$, $f_2(x)$, $f_3(x)$ change as e increases. Let's look at them as p-adic digits.

e	$f_1(x)$	$f_2(x)$	$f_3(x)$
1	$x+[\cdots 0000004]$	$x+[\cdots 0000006]$	$x^2+[\cdots 0000000]x+1$
2	$x+[\cdots 0000044]$	$x+[\cdots 0000026]$	$x^2+[\cdots 0000060]x+1$
3	$x+[\cdots 0000644]$	$x+[\cdots 0000026]$	$x^2+[\cdots 0000660]x+1$
4	$x+[\cdots 0003644]$	$x+[\cdots 0003026]$	$x^2+[\cdots 0006660]x+1$
5	$x+[\cdots 0003644]$	$x+[\cdots 0063026]$	$x^2+[\cdots 0066660]x+1$
6	$x+[\cdots 0203644]$	$x+[\cdots 0463026]$	$x^2+[\cdots 0666660]x+1$
7	$x+[\cdots 6203644]$	$x+[\cdots 0463026]$	$x^2+[\cdots 6666660]x+1$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

The coefficient of x in $f_3(x)$ seems to be "converging" to -7:

$$f_3(x) \;\to\; x^2 - 7x + 1.$$

And ... sure enough ... $x^2 - 7x + 1$ is a factor of $f(x)$:

$$f(x) \;=\; x^4 - 4x^3 - 17x^2 - 18x + 3 \;=\; (x^2 + 3x + 3)(x^2 - 7x + 1).$$

It doesn't look like $f_1(x)$ and $f_2(x)$ are going anywhere, but if we look at their product we see this.

e	$f_1(x)\,f_2(x)$	$f_1(x)\,f_2(x)$
1	$x^2 + 10x + 24$	$x^2+[\cdots 0000013]x+[\cdots 0000033]$
2	$x^2 + 52x + 640$	$x^2+[\cdots 0000103]x+[\cdots 0001603]$
3	$x^2 + 346x + 6520$	$x^2+[\cdots 0001003]x+[\cdots 0025003]$
4	$x^2 + 2404x + 1421395$	$x^2+[\cdots 0010003]x+[\cdots 5040003]$
5	$x^2 + 16810x + 20941525$	$x^2+[\cdots 0100003]x+[\cdots 3000003]$
6	$x^2 + 117652x + 2891341827$	$x^2+[\cdots 1000003]x+[\cdots 6000003]$
7	$x^2 + 823546x + 61256775429$	$x^2+[\cdots 0000003]x+[\cdots 0000003]$
$\vdots$	$\vdots$	$\vdots$

It appears that

$$f_1(x)\,f_2(x) \;\to\; x^2 + 3\,x + 3$$

and indeed, $x^2 + 3\,x + 3$ is the other factor of $f(x)$.

Exercise: Symmetric Remainders.

1. *Suppose a is an integer and m is a positive integer. Show that if*

$$q \;=\; \left\lceil \frac{a}{m} - \frac{1}{2} \right\rceil$$

and

$$r \;=\; a - q\,m$$

then

$$r \;\equiv\; a \pmod{m}$$

and

$$-\frac{m}{2} \;<\; r \;\leq\; +\frac{m}{2}.$$

The number r is called the symmetric remainder (of a on division by m) *and is denoted*

$$r \;=\; a \;\mathbf{mods}\; m.$$

2. *Show that if n is an integer and $-\frac{1}{2}p^k < n < 0$ then*

$$n \;\mathbf{mods}\; p^k \;=\; n.$$

Here is why we are interested in symmetric remainders.

e	$f_3(x)$	$f_3(x)$ **mods** 7^e	$f_1(x)f_2(x)$	$f_1(x)f_2(x)$ **mods** 7^e
1	x^2+1	x^2+1	$x^2+10x+24$	x^2+3x+3
2	$x^2+42x+1$	x^2-7x+1	$x^2+52x+640$	x^2+3x+3
3	$x^2+336x+1$	x^2-7x+1	$x^2+346x+6520$	x^2+3x+3
4	$x^2+2394x+1$	x^2-7x+1	$x^2+2404x+1421395$	x^2+3x+3
5	$x^2+16800x+1$	x^2-7x+1	$x^2+16810x+20941525$	x^2+3x+3
6	$x^2+117642x+1$	x^2-7x+1	$x^2+117652x+2891341827$	x^2+3x+3
7	$x^2+823536x+1$	x^2-7x+1	$x^2+823546x+61256775429$	x^2+3x+3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

The story for $f_1(x)$ and $f_2(x)$ is less suggestive.

e	$f_1(x)$	$f_1(x)$ **mods** 7^e	$f_2(x)$	$f_2(x)$ **mods** 7^e
1	$x+4$	$x-3$	$x+6$	$x-1$
2	$x+32$	$x-17$	$x+20$	$x+20$
3	$x+326$	$x-17$	$x+20$	$x+20$
4	$x+1355$	$x-1046$	$x+1049$	$x+1049$
5	$x+1355$	$x+1355$	$x+15455$	$x-1352$
6	$x+34969$	$x+34969$	$x+82683$	$x-34966$
7	$x+740863$	$x-82680$	$x+82683$	$x+82683$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Let's try again, with

$$f(x) \;=\; x^4 - 4\,x^3 - 17\,x^2 - 18\,x + 3$$

as before and this time with $p = 19$. We find that if

$$f_1(x) = x - 9, \quad f_2(x) = x - 6, \quad f_3(x) = x + 2, \quad f_4(x) = x + 9$$

then

$$f(x) \;\equiv\; f_1(x)\,f_2(x)\,f_3(x)\,f_4(x) \pmod{19\mathbb{Z}[x]}.$$

Hensel lifting (with symmetric remainders) gives us this.

e	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
1	$x-9$	$x-6$	$x+2$	$x+9$
2	$x+124$	$x+70$	$x-131$	$x-67$
3	$x-2764$	$x-2818$	$x+2757$	$x+2821$
4	$x+38390$	$x-2818$	$x-38397$	$x+2821$
5	$x+559674$	$x-133139$	$x-559681$	$x+133142$
6	$x+5511872$	$x+2342960$	$x-5511879$	$x-2342957$
7	$x-88579890$	$x-44702921$	$x+88579883$	$x+44702924$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Let's see what happens if we take these factors two at a time (modulo 19^7).

$$\begin{aligned}
f_1(x)\,f_2(x) &= x^2 - 133282811x + 424699549 \\
f_1(x)\,f_3(x) &= x^2 - 7x + 1 \\
f_1(x)\,f_4(x) &= x^2 - 43876966x + 203432520 \\
f_2(x)\,f_3(x) &= x^2 + 43876962x - 111779102 \\
f_2(x)\,f_4(x) &= x^2 + 3x + 3 \\
f_3(x)\,f_4(x) &= x^2 + 133282807x + 377518751
\end{aligned}$$

This is reminiscent of what we did earlier: given a polynomial of degree n, we took close approximations $\alpha_1, \ldots, \alpha_n$ of its (complex) roots, then tested products of the form

$$(x - \alpha_{i_1}) \cdots (x - \alpha_{i_r})$$

and checked if any of them had coefficients that were all close to integer values.

The *Hensel factorization* algorithm, widely used in computer-algebra systems, follows the same outline.

- For $f(x)$ a monic polynomial and p a good prime for $f(x)$, find the mod-p factorization of $f(x)$.
- Apply Hensel lifting to the mod-p factors of $f(x)$ until their coefficients are known to "sufficiently many" p-adic digits.
- Test products of the lifted factors and check if any of them have coefficients that are all p-adically close to integers.

If B is a bound on the absolute value of a coefficient of a factor of $f(x)$, then "sufficiently many digits" means modulo p^e, with $p^e > 2B$. In (Mignotte 1974) the bound

$$B \;=\; \binom{\lfloor n/2 \rfloor}{\lfloor n/4 \rfloor} \left(1 + \textstyle\sum_{i=1}^{n} |a_i|^2\right)^{1/2}$$

is given for $f(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$.

In theory, Hensel factorization has the same drawback as the complex-root method: if $f(x)$ had r irreducible factors modulo p it would take $2^{r-1} - 1$ tests to establish that $f(x)$ is irreducible in $\mathbb{Z}[x]$. Usually (but not always!) this theoretical difficulty can be avoided in practice by finding a good prime p for which the number of irreducible mod-p factors of $f(x)$ is small. But the fact remains that the worst case is very bad.

6. Short vectors and Hensel factorization

As we did with the complex-root method, we will apply LLL to ameliorate the worst case for Hensel factorization.

Let

$$f(x) \;=\; x^4 - 4\,x^3 - 17\,x^2 - 18\,x + 3$$

and let

$$f_1(x) \;=\; x + 740863, \quad f_2(x) \;=\; x + 82683, \quad f_3(x) \;=\; x^2 + 823536\,x + 1,$$

with $p = 7$ and $e = 7$. Then

$$f(x) \;\equiv\; f_1(x)\,f_2(x)\,f_3(x) \quad (\mathrm{mod}\; p^e\mathbb{Z}[x]).$$

So $f_1(x)$ approximates, to e digits of accuracy, a factor $x+\alpha$ in $\mathbb{Z}_p[x]$ of $f(x)$. We now ask this question: is there a polynomial $g_1(x) = x^2 + c_1 x + c_2$ in $\mathbb{Z}[x]$ such that $x+\alpha$ is a factor of $g_1(x)$ in $\mathbb{Z}_p[x]$? If so there would exist $x+\beta$ in $\mathbb{Z}_p[x]$ such that

$$g_1(x) \;=\; (x+\alpha)(x+\beta) \;=\; 1\cdot(x^2+\alpha x) \;+\; \beta\cdot(x+\alpha)$$

and therefore $(1,\,c_1,\,c_2)$ would be a short vector among all the $\mathbb{Z}$-linear combinations of $(1,\,\alpha\ \textbf{mod}\ p^e,\,0)$ and $(0,\,1,\,\alpha\ \textbf{mod}\ p^e)$.

With the polynomial vector

$$\begin{bmatrix} x^1 f_1(x) \\ x^0 f_1(x) \\ x^0 p^e \end{bmatrix} \;=\; \begin{bmatrix} 1\cdot x^2 & + & \alpha\cdot x & + & 0\cdot 1 \\ 0\cdot x^2 & + & 1\cdot x & + & \alpha\cdot 1 \\ 0\cdot x^2 & + & 0\cdot x & + & p^e\cdot 1 \end{bmatrix}$$

in mind, we construct the coefficient matrix

$$\begin{bmatrix} 1 & \alpha\ \textbf{mod}\ p^e & 0 \\ 0 & 1 & \alpha\ \textbf{mod}\ p^e \\ 0 & 0 & p^e \end{bmatrix} \;=\; \begin{bmatrix} 1 & 740863 & 0 \\ 0 & 1 & 740863 \\ 0 & 0 & 823543 \end{bmatrix}$$

which we then put in LLL-reduced form

$$\begin{bmatrix} 1 & 3 & 3 \\ -200 & 157 & -92 \\ 437 & 305 & -452 \end{bmatrix}$$

and it looks like $g_1(x) = x^2 + 3x + 3$.

Here is another example. Let

$$\begin{aligned} f(x) \;&=\; x^6 - x^5 + 4\,x^4 - 7\,x^3 + 11\,x^2 + 8\,x - 56, \\ f_1(x) \;&=\; x + 71928037431846, \\ f_2(x) \;&=\; x + 23254434711859, \\ f_3(x) \;&=\; x^2 + 23439394208775\,x + 24785150945108, \\ f_4(x) \;&=\; x^2 + 72112996928769\,x + 56711443678437, \end{aligned}$$

with $p = 5$ and $e = 20$. Then

$$f(x) \;\equiv\; f_1(x)\,f_2(x)\,f_3(x)\,f_4(x) \quad (\mathrm{mod}\; p^e\mathbb{Z}[x]).$$

Regarding $f_1(x)$ as an approximation to a factor $x+\alpha$ of $f(x)$ in $\mathbb{Z}_p[x]$ we will look for a cubic factor of $f(x)$ in $\mathbb{Z}[x]$ that has $x+\alpha$ as a factor in $\mathbb{Z}_p[x]$.

With $p^e = 95367431640625$ and $\alpha\,\textbf{mod}\,p^e = 71928037431846$, the polynomial vector gives the coefficient matrix, which is then LLL-reduced,

$$\begin{bmatrix} x^2 f_1(x) \\ x^1 f_1(x) \\ x^0 f_1(x) \\ x^0 p^e \end{bmatrix} \;\rightarrow\; \begin{bmatrix} 1 & 71928037431846 & 0 & 0 \\ 0 & 1 & 71928037431846 & 0 \\ 0 & 0 & 1 & 71928037431846 \\ 0 & 0 & 0 & 95367431640625 \end{bmatrix}$$

$$\rightarrow\; \begin{bmatrix} 1 & -4 & 8 & -7 \\ 9522 & -8055 & 6116 & 12958 \\ -15342 & -8692 & -3148 & -823 \\ -7868 & 10991 & 18487 & 13723 \end{bmatrix},$$

indicating that $x^3 - 4\,x^2 + 8\,x - 7$ should be a factor of $f(x)$, and indeed

$$f(x) \;=\; (x^3 - 4\,x^2 + 8\,x - 7)\,(x^3 + 3\,x^2 + 8\,x + 8).$$

Yet another example, again with

$$f(x) = x^6 - x^5 + 4\,x^4 - 7\,x^3 + 11\,x^2 + 8\,x - 56.$$

Let

$$\begin{aligned} f_1(x) &= x + 322471, & f_3(x) &= x^2 + 9443150\,x + 4460733, \\ f_2(x) &= x + 1118109, & f_4(x) &= x^2 + 8647519\,x + 8131562, \end{aligned}$$

with $p = 5$ and $e = 10$. Then

$$f(x) \equiv f_1(x)\,f_2(x)\,f_3(x)\,f_4(x) \pmod{p^e\,\mathbb{Z}[x]}.$$

Regarding $f_4(x)$ as an approximation to a factor $x^2 + \alpha x + \beta$ of $f(x)$ in $\mathbb{Z}_p[x]$ we seek a cubic factor of $f(x)$ in $\mathbb{Z}[x]$ that has $x^2 + \alpha x + \beta$ as a factor in $\mathbb{Z}_p[x]$.

With $p^e = 9765625$, α **mod** $p^e = 8647519$, and β **mod** $p^e = 8131562$, the polynomial vector gives the coefficient matrix, which is then LLL-reduced,

$$\begin{bmatrix} x^1 f_1(x) \\ x^0 f_1(x) \\ x^1 p^e \\ x^0 p^e \end{bmatrix} \to \begin{bmatrix} 1 & 8647519 & 8131562 & 0 \\ 0 & 1 & 8647519 & 8131562 \\ 0 & 0 & 9765625 & 0 \\ 0 & 0 & 0 & 9765625 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 3 & 8 & 8 \\ 8567 & -14860 & 3502 & 1004 \\ -1755 & -13082 & -13813 & 18931 \\ -19998 & -3572 & 784 & 3055 \end{bmatrix},$$

identifying the factor $x^3 + 3\,x^2 + 8\,x + 8$ of $f(x)$.