# Polynomial Factorization II

## 1. Factorization over $\mathbb{Z}_p[x]$

For $f(x)$ a monic polynomial in $\mathbb{Z}[x]$, Hensel factorization efficiently gives the irreducible factors of $f(x)$ in $\mathbb{Z}[x]$.

1. *Replace $f \leftarrow f/\gcd(f, f')$, to ensure $f$ is square free, so $\operatorname{disc} f \neq 0$.*
2. *Choose a prime $p$ not dividing $\operatorname{disc} f$, i.e., a good prime for $f$.*
3. *Construct the complete factorization of $f(x)$ modulo $p\mathbb{Z}[x]$.*

   *By Hensel's Lemma these factors are the irreducible factors of $f(x)$ in $\mathbb{Z}_p[x]$, reduced moduolo $p\mathbb{Z}_p[x]$. And since $\mathbb{Z}_p$ is an extension of $\mathbb{Z}$, the factorization of $f(x)$ in $\mathbb{Z}_p[x]$ is a refinement of the factorization of $f(x)$ in $\mathbb{Z}[x]$.*
4. *Lift the factorization to a sufficient $p$-adic precision.*
5. *Choosing one of these lifted factors, say $\widehat{g}(x)$, apply LLL reduction to*

$$x^0\,\widehat{g}(x),\ x^1\,\widehat{g}(x),\ \ldots,\ x^{k-1}\,\widehat{g}(x),$$

   *with $k = \deg f - \deg \widehat{g}$, to uncover a proper factor $g(x)$ of $f(x)$ in $\mathbb{Z}[x]$.*

   *If no proper factor $g(x)$ appears after step 5 then $f(x)$ is irreducible in $\mathbb{Z}[x]$; otherwise the procedure is repeated with $g(x)$ in place of $f(x)$.*

Hensel factorization proceeds without difficulty, provided we are free to choose a good prime $p$ in step 2. But often we are not free to make this choice. For instance, in the ring of integers $\mathcal{O}$ of an algebraic number field, factorization of the ideal $p\mathcal{O}$ corresponds exactly to the factorization over $\mathbb{Z}_p$ of the polynomial defining the field as an extension of $\mathbb{Q}$.

The fact that unique factorization does not hold in $\mathbb{Z}[x]/p^m\mathbb{Z}[x]$ when $m > 1$ is at the heart of the problem. For example,

$$x^2 - 1 \equiv (x-1)(x+1) \equiv (x-3)(x+3) \pmod{2^3\mathbb{Z}[x]}.$$

For lifting purposes the factorization in step 3 will be ambiguous; the lifting in step 4 can proceed only when a factorization correct to several digits has been found. The precise threshhold is given by congruences (1) and (2) in the "Hensel Lifting" exercise below.

## 2. Hensel Lifting: General Case

***Exercise: p-adic Newton's Method (for an arbitrary prime p).***

*Let $r \in \mathbb{Z}$ and let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ with*

$$d = v_p\big(f'(r)\big), \qquad e = v_p\big(f(r)\big), \qquad 0 \le d \le \tfrac{1}{2}(e-1).$$

*Use the fact that*

$$f(x) = f(r) + f'(r)(x-r) + (x-r)^2 g(x)$$

*for some $g(x) \in \mathbb{Z}[x]$ to show that if*

$$a\,\frac{f'(r)}{p^d} \equiv 1 \pmod{p}, \qquad u = \frac{f(r)}{p^e}, \qquad \widehat{r} = r - p^{e-d}au$$

*then*

$$v_p\big(f'(\widehat{r})\big) = d, \qquad v_p\big(f(\widehat{r})\big) \ge e+1, \qquad \widehat{r} \equiv r \pmod{p^{e-d}}.$$

**Example.** Let $f(x) = x^3 - 29x^2 - 17x - 19$ and $p = 2$.

| $r$ | $f'(r)$ | $d$ | $2d+1$ | $f(r)$ | $e$ |
|---|---|---|---|---|---|
| 0 | $-17$ | 0 | 1 | $-19$ | 0 |
| 1 | $-2^3\cdot 9$ | 3 | 7 | $-2^6\cdot 1$ | 6 |
| 2 | $-121$ | 0 | 1 | $-161$ | 0 |
| 3 | $-2^2\cdot 41$ | 2 | 5 | $-2^4\cdot 19$ | 4 |
| 4 | $-201$ | 0 | 1 | $-487$ | 0 |
| 5 | $-2^3\cdot 29$ | 3 | 7 | $-2^6\cdot 11$ | 6 |
| 6 | $-257$ | 0 | 1 | $-949$ | 0 |
| 7 | $-2^2\cdot 69$ | 2 | 5 | $-2^6\cdot 19$ | 6 |

| $r$ base $p$ | $d$ | $e$ | $e-d$ | $r$ |
|---|---|---|---|---|
| 111 | 2 | 6 | 4 | 7 |
| 100110111 | 2 | 7 | 5 | 311 |
| 1110010111 | 2 | 10 | 8 | 919 |
| 1011010010111 | 2 | 12 | 10 | 5783 |
| 110001010010111 | 2 | 14 | 12 | 25239 |
| 11001001010010111 | 2 | 16 | 14 | 103063 |

**Proposition.** *If $r \in \mathbb{Z}$ and $f(x)$ is a monic polynomial in $\mathbb{Z}[x]$ with*

$$d = v_p\big(f'(r)\big), \qquad e = v_p\big(f(r)\big), \qquad 0 \le d \le \tfrac{1}{2}(e-1)$$

*then there exists $\rho \in \mathbb{Z}_p$ with $\rho \equiv r \pmod{p^{e-d}}$ such that $f(\rho) = 0$.*

***Exercise: Hensel Lifting (with p an arbitrary prime).***

*Suppose* $f(x)$, $f_1(x)$, $f_2(x)$, $a_1(x)$, $a_2(x)$ *are polynomials in* $\mathbb{Z}[x]$ *such that*

$$(1) \qquad f(x) \;\equiv\; f_1(x)\,f_2(x) \qquad (\mathrm{mod}\ p^e\mathbb{Z}[x]),$$

$$(2) \qquad p^d \;\equiv\; a_1(x)\,f_2(x) \,+\, a_2(x)\,f_1(x) \quad (\mathrm{mod}\ p^{d+1}\mathbb{Z}[x]),$$

*with* $d \geq 0$ *and* $e \geq 2d+1$. *Show that if* $f(x)$, $f_1(x)$, $f_2(x)$ *are monic with*

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

$$g_1(x) \;=\; a_1(x)\,u(x) \ \mathbf{mod}\ f_1(x), \qquad \widehat{f}_1(x) \;=\; f_1(x) \,+\, p^{e-d}g_1(x),$$

$$g_2(x) \;=\; a_2(x)\,u(x) \ \mathbf{mod}\ f_2(x), \qquad \widehat{f}_2(x) \;=\; f_2(x) \,+\, p^{e-d}g_2(x),$$

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

$$f(x) \;\equiv\; \widehat{f}_1(x)\,\widehat{f}_2(x) \qquad (\mathrm{mod}\ p^{e+1}\mathbb{Z}[x]),$$

$$p^d \;\equiv\; a_1(x)\,\widehat{f}_2(x) \,+\, a_2(x)\,\widehat{f}_1(x) \quad (\mathrm{mod}\ p^{d+1}\mathbb{Z}[x]).$$

If $f_1(x)$ and $f_2(x)$ satisfy congruence (1) then $a_1(x)$, $a_2(x)$, and $d$ satisfying (2) can be found from the Hermite-reduction of a Sylvester matrix:

$$p^d\mathbb{Z}_p \;=\; \big(f_2(x)\mathbb{Z}_p[x] + f_1(x)\mathbb{Z}_p[x]\big) \cap \mathbb{Z}_p.$$

In this computation we have $d \leq d_r \leq v_p(\operatorname{disc} f)$ with

$$p^{d_r}\mathbb{Z}_p \;=\; \big(f(x)\mathbb{Z}_p[x] + f'(x)\mathbb{Z}_p[x]\big) \cap \mathbb{Z}_p.$$

If $e \geq 2d+1$ then Hensel lifting may proceed; otherwise the precision of the first congruence must be increased some other way.

**Example.** Let $f(x) = x^4 + 2x^3 + 15x^2 + 14x - 31$ and $p = 2$.

Efficient algorithms (Berlekamp, Cantor-Zassenhaus) give the factorization

$$f(x) \;\equiv\; (x^2+x+1)^2 \quad (\mathrm{mod}\ p\mathbb{Z}[x])$$

of $f(x)$ modulo $p$. Some strenuous effort produces the refinement

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

with $e = 9$ and

$$f_1(x) = x^2 - 7x + 35, \qquad f_2(x) = x^2 + 9x + 43.$$

Hermitian reduction over $\mathbb{Z}$ of the corresponding Sylvester matrix gives

$$\begin{bmatrix} \langle\, x^1 f_2(x) \,\rangle \\ \langle\, x^0 f_2(x) \,\rangle \\ \langle\, x^1 f_1(x) \,\rangle \\ \langle\, x^0 f_1(x) \,\rangle \end{bmatrix} = \begin{bmatrix} 1 & 9 & 43 & 0 \\ 0 & 1 & 9 & 43 \\ 1 & -7 & 35 & 0 \\ 0 & 1 & -7 & 35 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 2 & 253 \\ \cdot & 1 & 1 & 659 \\ \cdot & \cdot & 8 & 624 \\ \cdot & \cdot & \cdot & 1240 \end{bmatrix}$$

so that $(f_2(x)\mathbb{Z}_p[x] + f_1(x)\mathbb{Z}_p[x]) \cap \mathbb{Z}_p = 1240\,\mathbb{Z}_p = 2^3 \cdot 155\,\mathbb{Z}_p = 2^3\mathbb{Z}_p$, and thus $d = 3$. Coefficients $a_1(x) = -2x + 15$ and $a_2(x) = 2x + 17$ satisfying (2) are given by the same computation (if the original matrix is augmented by the identity).

Since the conditions for Hensel lifting are satisfied, it follows that $f(x)$ has two distinct quadratic factors in $\mathbb{Z}_p[x]$, and (since $e - d = 6$) that these factors are approximated correctly to six $p$-adic digits by $f_1(x)$ and $f_2(x)$.

A similar computation gives the "reduced discriminant" $p^{d_r}$, which serves as an upper bound for $p^d$:

$$\begin{bmatrix} \langle\, x^2 f(x) \,\rangle \\ \langle\, x^1 f(x) \,\rangle \\ \langle\, x^0 f(x) \,\rangle \\ \langle\, x^3 f'(x) \,\rangle \\ \langle\, x^2 f'(x) \,\rangle \\ \langle\, x^1 f'(x) \,\rangle \\ \langle\, x^0 f'(x) \,\rangle \end{bmatrix} = \begin{bmatrix} 1 & 2 & 15 & 14 & -31 & 0 & 0 \\ 0 & 1 & 2 & 15 & 14 & -31 & 0 \\ 0 & 0 & 1 & 2 & 15 & 14 & -31 \\ 4 & 6 & 30 & 14 & 0 & 0 & 0 \\ 0 & 4 & 6 & 30 & 14 & 0 & 0 \\ 0 & 0 & 4 & 6 & 30 & 14 & 0 \\ 0 & 0 & 0 & 4 & 6 & 30 & 14 \end{bmatrix} \to \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 40 & 74603 \\ \cdot & 1 & 0 & 1 & 0 & 57 & 86484 \\ \cdot & \cdot & 1 & 0 & 1 & 148 & 37645 \\ \cdot & \cdot & \cdot & 2 & 0 & 12 & 78386 \\ \cdot & \cdot & \cdot & \cdot & 2 & 2 & 65294 \\ \cdot & \cdot & \cdot & \cdot & \cdot & 160 & 44160 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 88160 \end{bmatrix},$$

$$\big(f(x)\mathbb{Z}_p[x] + f'(x)\mathbb{Z}_p[x]\big) \cap \mathbb{Z}_p \;=\; 88160\,\mathbb{Z}_p \;=\; 2^5 \cdot 2755\,\mathbb{Z}_p \;=\; 2^5\mathbb{Z}_p.$$

Thus $d_r = 5$, while $\operatorname{disc} f = -56422400 = -2^{12} \cdot 13775$ and $v_p(\operatorname{disc} f) = 12$.

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

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

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

$$p^d \;\equiv\; a_1(x)\,f_2(x) \,+\, a_2(x)\,f_1(x) \quad (\mathrm{mod}\ p^{d+1}\mathbb{Z}[x])$$

*with*

$$0 \;\leq\; d \;\leq\; \tfrac{1}{2}(e-1)$$

*then there exist monic polynomials* $\varphi_1(x)$, $\varphi_2(x)$ *in* $\mathbb{Z}_p[x]$ *such that*

$$f(x) \;=\; \varphi_1(x)\,\varphi_2(x),$$

$$f_1(x) \;\equiv\; \varphi_1(x) \quad (\mathrm{mod}\ p^{e-d}\mathbb{Z}_p[x]),$$

$$f_2(x) \;\equiv\; \varphi_2(x) \quad (\mathrm{mod}\ p^{e-d}\mathbb{Z}_p[x]).$$

# 3. The Zassenhaus *Round Four* Algorithm

Earlier we examined the *Round Two* algorithm of Zassenhaus for computing integral bases of number fields efficiently. The algorithm is bounded in its performance by the solution of a system of $n^2$ linear relations in $n$ variables, which with sophisticated matrix-inversion techniques takes $O(n^{1+\log_2 7})$ operations.

It has proved to be more efficient to work with "$\pi$-adic" expansions of elements in the $p$-adic completion of a number field, this for each bad prime $p$. The ultimate result is a sufficiently precise approximation (*i.e.*, above the Hensel threshhold) to the factorization over $\mathbb{Z}_p$ of the original polynomial.

From such a factorization a $\mathbb{Z}$-basis for a "$p$-maximal order" can be found without much trouble, and the bases of these orders can be combined in a simple way to give an integral basis for the original number field.

## Properties of the Eisenstein form

Let $f(x)$ be the defining polynomial of the algebraic extension $\mathcal{K}$ of $\mathbb{Q}$.

The question is, how does $f(x)$ factorize over $\mathbb{Z}_p$? Thanks to Hensel's Lemma we need only worry about the case when $f$ is *$p$-primary*, *i.e.*, when

$$f(x) \;\equiv\; \nu(x)^e \pmod{p\mathbb{Z}[x]} \tag{3}$$

with $\nu(x)$ irreducible mod $p\mathbb{Z}[x]$ and $e > 1$.

***Exercises.*** *Let $\alpha$ be a root of $f(x)$ and let $\mathcal{K} = \mathbb{Q}(\alpha)$ and extend $v_p$ to $\mathcal{K}$. Assume $f$ satisfies (3) and let*

$$\frac{f(x) - \nu(x)^e}{p} \;=\; r_1(x)\nu(x)^{e-1} + r_2(x)\nu(x)^{e-2} + \cdots + r_e(x)$$

*with $\deg r_j < \deg \nu$ for $j = 1, \ldots, e$.*

1. THE EISENSTEIN CRITERION. *Show that if*

   $$r_e(x) \not\equiv 0 \pmod{p\mathbb{Z}[x]} \tag{4}$$

   *then $f(x)$ is irreducible in $\mathbb{Z}_p[x]$.*

2. THE DEDEKIND CRITERION. *Show that*

   $$\mathcal{O}_{\mathcal{K}} \cap \tfrac{1}{p}\mathbb{Z}[\alpha] \;=\; \mathbb{Z}[\alpha]$$

   *if and only if $f(x)$ is of Eisenstein form (i.e., $f$ satisfies (4)).*

3. *Show that $f(x)$ is of Eisenstein form if and only if*

   $$v_p\big(\nu(\alpha)\big) \;=\; \frac{\deg \nu}{\deg f}$$

   *for each choice of $\alpha$. (Hint: Use Newton polygons.)*

## Properties of $\mathbb{Q}_p[x]\,/\,f(x)\,\mathbb{Q}_p[x]$

Let $\mathcal{A}_f$ denote the $\mathbb{Q}_p$-algebra defined by $f(x)$, *i.e.*,

$$\mathcal{A}_f \;=\; \mathbb{Q}_p[x]\,/\,f(x)\mathbb{Q}_p[x],$$

and suppose

$$f(x) \;=\; f_1(x) \cdots f_r(x)$$

is the complete factorization of $f(x)$ into irreducible polynomials in $\mathbb{Z}_p[x]$.

- There exist $a_1(x), \ldots, a_r(x)$ in $\mathbb{Q}_p[x]$ such that

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

- Let $\widehat{x}$ denote the generator $x + f(x)\,\mathbb{Q}_p[x]$ of $\mathcal{A}_f$. If we define

  $$\varepsilon_j \;=\; a_j(\widehat{x}) \textstyle\prod_{k\neq j} f_k(\widehat{x}) \tag{5}$$

  for $j = 1, \ldots, r$ then $\varepsilon_1, \ldots, \varepsilon_r$ are orthogonal idempotents in $\mathcal{A}_f$, and so

  $$\mathcal{A}_f \;=\; \mathcal{A}_{f,1} \oplus \cdots \oplus \mathcal{A}_{f,r} \tag{6}$$

  where $\mathcal{A}_{f,j} = \varepsilon_j \mathcal{A}_f$ for $j = 1, \ldots, r$.

- For each $j$ the component $\mathcal{A}_{f,j}$ is a field:

  $$\mathcal{A}_{f,j} \;=\; \mathbb{Q}_p(\widehat{x}_j) \;\cong\; \mathbb{Q}_p[x]\,/\,f_j(x)\mathbb{Q}_p[x]$$

  with $\widehat{x}_j = \varepsilon_j \widehat{x}$.

The Round Four algorithm finds an element $\alpha$ of a component $\mathcal{A}_{f,j}$ with suitable properties and constructs $\mu_\alpha(x)$, its minimal polynomial over $\mathbb{Q}_p$, which from the construction will be in Eisenstein form and hence irreducible over $\mathbb{Q}_p$.

In the construction of $\mu_\alpha(x)$ the field $\mathbb{Q}_p(\alpha)$ is regarded as a totally ramified extension of an unramified extension $\mathcal{I}_\alpha$ of $\mathbb{Q}_p$. An element $\pi_\alpha$ in $\mathbb{Z}_p[\alpha]$ — presumed to be of minimal positive $p$-adic value — is found and the coefficients of its minimal polynomial over $\mathcal{I}_\alpha$ are determined.

- If $\deg \mu_\alpha = \deg f$ then $\mathcal{A}_f$ is a field and $f(x)$ itself is irreducible over $\mathbb{Q}_p$.

- If $\deg \mu_\alpha < \deg f$ then $f(x)$ has a proper factorization over $\mathbb{Q}_p$. In this case

  $$f_j(x) \;=\; \gcd\big(f(x), \mu_\alpha(\alpha(x))\big).$$

## Factorization via $\pi$-adic expansion

Let $\xi$ denote an arbitrary root of an arbitrary irreducible factor of $f$.

*That is to say, $\xi = \varepsilon_j\,\widehat{x}$ for one of the idempotents $\varepsilon_j$ defined in (5).*

When $\theta(x) \in \mathbb{Q}[x]$ we will sometimes write $\theta_\xi$ for $\theta(\xi)$, for the sake of neatness.

For $\theta(x) \in \mathbb{Q}_p[x]$ we define the *characteristic polynomial of $\theta$ in $\mathcal{A}_f$* as

$$\chi_\theta(x) \;=\; \big(x - \theta(\xi_1)\big)\cdots\big(x - \theta(\xi_n)\big),$$

where $n = \deg f$ and $\xi_1, \ldots, \xi_n$ are the roots of $f$.

For $\theta(x)$ in $\mathbb{Q}[x]$ with $\chi_\theta(x)$ in $\mathbb{Z}[x]$ and $p$-primary we define $\nu_\theta$, $N_\theta$, $E_\theta$, and $F_\theta$.

- $\nu_\theta(x)$ is a monic polynomial, irreducible modulo $p\mathbb{Z}[x]$, such that $\chi_\theta(x) \equiv \nu_\theta(x)^k$ modulo $p\mathbb{Z}[x]$ for some $k \geq 1$.
- $v_p\big(\nu_\theta(\theta_\xi)\big) = N_\theta\,/E_\theta$, in lowest terms.
- $F_\theta = \deg \nu_\theta$.

We will proceed with several conditions in mind.

Condition 1. *$f(x)$ is irreducible over $\mathbb{Q}_p$.*

We aim to confirm this condition by finding a "witness" polynomial $\alpha(x) \in \mathbb{Q}[x]$ for which $\chi_\alpha(x)$ is of Eisenstein form. It would follow that $\mathbb{Q}_p(\xi)$, which contains the degree $n$ extension $\mathbb{Q}_p(\alpha(\xi))$, is itself an extension of $\mathbb{Q}_p$ of degree $n$, and therefore that $f(x)$ is irreducible over $\mathbb{Q}_p$.

We'll start with $\alpha(x) = x$, so that $\alpha(\xi) = \xi$ and $\chi_\alpha(x) = f(x)$.

Condition 2. $\operatorname{disc}\chi_\alpha \neq 0$.

While $\operatorname{disc}\chi_\alpha = 0$ we replace $\alpha(x) \leftarrow \alpha(x) + px$. These replacements leave $\nu_\alpha(x)$ unchanged. We have $\chi_\alpha(x) = \chi_{\alpha,1}(x)\cdots\chi_{\alpha,r}(x)$ with $\chi_{\alpha,1}(x), \ldots, \chi_{\alpha,r}(x)$ pairwise relatively prime, corresponding to the decomposition (6).

Condition 3. *The polynomial $\chi_\alpha(x)$ is $p$-primary.*

Otherwise $\chi_\alpha(x)$ would have coprime factors in $\mathbb{Z}_p[x]$, and hence the algebra $\mathcal{A}_f$ would have zero-divisors, contradicting Condition 1. This situation leads readily (via a GCD computation) to a proper factorization of $f(x)$.

Condition 4. *The Newton polygon of $\chi_\alpha(x)$ consists of a single edge.*

Otherwise $v_p(\alpha_{\xi_1}), \ldots, v_p(\alpha_{\xi_n})$ would not all be equal, and this is not consistent with Condition 1. In this case it is straightforward to construct $\theta(x)$ with $\chi_\theta(x)$ not $p$-primary, from which a proper factorization of $f(x)$ can be derived.

Condition 5. $N_\alpha = 1$.

If not, let $\pi_\alpha(x) = \nu_\alpha(x)^r/p^s$ with $0 \leq r \leq E_\alpha - 1$ such that $v_p\big(\pi_\alpha(\alpha_\xi)\big) = 1/E_\alpha$. Replace $\alpha(x) \leftarrow \alpha(x) + \pi_\alpha(\alpha(x))$. This gives $v_p\big(\nu_\alpha(\alpha_\xi)\big) = 1/E_\alpha$ while leaving $\nu_\alpha$ and $E_\alpha$ unchanged. $\chi_\alpha(x)$ has changed, however; go back to Condition 2.

Condition 6. $E_\alpha\,F_\alpha < \deg f$.

Otherwise, by Exercise 3, $\chi_\alpha(x)$ is of Eisenstein form and we are done.

We now let $\mathcal{K}_\alpha$ denote the field $\mathbb{Q}_p(\alpha_\xi)$ and let $\pi_\alpha = \nu_\alpha(\alpha_\xi)$. We define

$$\mathcal{O}_\alpha \;=\; \big\{\,\theta \in \mathcal{K}_\alpha \;\big|\; v_p(\theta) \geq 0\,\big\},$$
$$\mathcal{P}_\alpha \;=\; \big\{\,\theta \in \mathcal{K}_\alpha \;\big|\; v_p(\theta) > 0\,\big\}.$$

Condition 7. *The element $\pi_\alpha$ is a prime element in $\mathcal{O}_\alpha$, i.e., $\mathcal{P}_\alpha = \pi_\alpha\mathcal{O}_\alpha$.*

Under Condition 7 the minimal polynomial of $\alpha_\xi$ must be of Eisenstein form.

*Proof.* Let $D_p = \{\,c \in \mathbb{Z} \mid 0 \leq c \leq p-1\,\}$, let $F = F_\alpha$, and define

$$R^{(x)} = \big\{\,c_0 + c_1x + \cdots + c_{F-1}x^{F-1} \;\big|\; c_0, c_1, \ldots, c_{F-1} \in D_p\,\big\}.$$

Then $R^{(\alpha_\xi)}$ is a complete set of representatives of $\mathcal{O}_\alpha/\mathcal{P}_\alpha$. If $E = E_\alpha$ then $\pi_\alpha^E/p$ is a unit in $\mathcal{O}_\alpha$ and therefore $\pi_\alpha^E/p$ has the $\pi_\alpha$-adic expansion

$$\begin{aligned}\pi_\alpha^E/p \;=\; &\lambda_{0,0} + \lambda_{0,1}\pi_\alpha + \cdots + \lambda_{0,E-1}\pi_\alpha^{E-1}\\ +\;& p\big(\lambda_{1,0} + \lambda_{1,1}\pi_\alpha + \cdots + \lambda_{1,E-1}\pi_\alpha^{E-1}\big)\\ +\;& p^2\big(\lambda_{2,0} + \lambda_{2,1}\pi_\alpha + \cdots + \lambda_{2,E-1}\pi_\alpha^{E-1}\big)\\ +\;& \cdots\end{aligned}\tag{7}$$

with each $\lambda_{j,k}$ belonging to $R^{(\alpha_\xi)}$ and $v_p(\lambda_{0,0}) = 0$. For $k = 0, 1, \ldots, E-1$ and $j = 0, 1, \ldots$ there exists $\delta_{j,k}(x) \in R^{(x)}$ such that $\lambda_{j,k} = \delta_{j,k}\big(\alpha_\xi\big)$. The polynomial

$$\beta(x) \;=\; \nu_\alpha(x)^E - p\sum\nolimits_{k=0}^{E-1}\Big(\sum\nolimits_{j=0}^{\infty} p^j\delta_{j,k}(x)\Big)\nu_\alpha(x)^k$$

is of Eisenstein form (since $\lambda_{0,0}$ is a unit) and $\beta\big(\alpha_\xi\big) = 0$. $\square$

Conditions 6 and 7 together are incompatible with Conditions 1 and 2. If the expansion in (7) reaches the Hensel threshhold then $\beta(x)$ approximates a proper factor of $\chi_\alpha(x)$ in $\mathbb{Z}_p[x]$. As in the case when Condition 3 fails, this factorization of $\chi_\alpha(x)$ leads directly to a proper factorization of $f(x)$.

Therefore, if Condition 1 holds, then any attempt to construct the expansion (7) must break down before reaching the Hensel threshhold.

## Constructing the next term in $\beta(x)$

For $j \geq 0$ and $0 \leq k \leq E-1$ let $\omega_{j,k}(x) \in \mathbb{Z}[x]$ be such that $\omega_{j,k}(\alpha_\xi)$ is the sum of the terms in the expansion (7), up to but not including the $k$th term in row $j$.

Then $p^{-1}\pi_\alpha^E - \omega_{j,k}(\alpha_\xi) = p^j \lambda_{j,k}\pi_\alpha^k + \mu$ with $v_p(\mu) > v_p(p^j\pi_\alpha^k)$.

Let $\kappa(x) \in \mathbb{Q}[x]$ be such that $\kappa(x)\,\nu_\alpha(x)$ **mod** $\chi_\alpha(x) = 1$ and let

$$\gamma(x) \;=\; \frac{\kappa(x)^k}{p^j}\left(\frac{\nu_\alpha(x)^E}{p} - \omega_{j,k}(x)\right).$$

CONDITION 8. *The polynomial $\chi_{\gamma(\alpha)}(x)$ is $p$-primary.*

As with Condition 3, failure of Condition 8 leads to a factorization of $f(x)$.

CONDITION 9. *The Newton polygon of $\chi_{\gamma(\alpha)}(x)$ consists of a single edge.*

Otherwise, as with Condition 4, we can easily construct a factorization of $f(x)$.

CONDITION 10. $F_\gamma \mid F_\alpha$.

Otherwise $\gamma(\alpha_\xi)$ has no representative in $\mathcal{O}_\alpha/\pi_\alpha\mathcal{O}_\alpha$ and Condition 7 must be false. We construct $\alpha'$ with $F_{\alpha'} = \operatorname{lcm}(F_\alpha, F_\gamma)$ and $E_{\alpha'} \geq E_\alpha$. We replace $\alpha \leftarrow \alpha'$ and try again with Condition 2.

Now $\gamma(\alpha_\xi) \equiv \lambda_{j,k}$ (mod $\mathcal{P}_\alpha$), and there exists $\delta_{j,k}(x)$ in $R^{(x)}$ such that

$$(8) \qquad \gamma(\alpha_\xi) \;\equiv\; \delta_{j,k}(\alpha_\xi) \pmod{\mathcal{P}_\alpha}.$$

Factorizing $\nu_\gamma(x)$ over the finite field $\mathbb{F}_q = \mathbb{F}_p[\overline{\alpha}_\xi]$, with $q = p^F$, we find among the roots $\rho_1, \ldots, \rho_{F_\gamma}$ of $\nu_\gamma$ a root $\rho_i = \rho_i(\overline{\alpha}_\xi)$ such that $v_p\big(\gamma(\alpha_\xi) - \rho_i(\alpha_\xi)\big) > 0$. Setting $\delta_{j,k}(x) = \rho_i(x)$ we have congruence (8).

If Condition 7 holds then there is only one choice for $\delta_{j,k}(x)$. Otherwise $\chi_{\gamma'(\alpha)}(x)$ is not $p$-primary, where $\gamma'(x) = \gamma(x) - \delta_{j,k}(x)$, and, as above, $f(x)$ factorizes.

## Performance

For conciseness we have presented the Round Four algorithm in its original "one-element" form. Instead of the "one element $\alpha$ does it all" treatment given here, the "two-element" variation of Round Four determines elements $\gamma$ and $\pi$ such that the extension defined by a root of $f$ is $\mathbb{Q}_p(\gamma, \pi)$, a totally ramified extension of $\mathbb{Q}_p(\gamma)$, which is in turn an unramified extension of $\mathbb{Q}_p$, these extensions being developed in parallel but separately.

Pauli (2001) showed that the two-element variation terminates in

$$O\big(m^{1+\epsilon}n^3 + m^{2+\epsilon}n^2\big)$$

operations, with $m = v_p(\operatorname{disc} f)$ and $n = \deg f$.

# 4. Extra Credit (avoiding a blank page)

***Exercise: A Lemma.***

*Let $f_1$, $f_2$, $f_3$, $a_1$, $a_2$, $a_3$ be polynomials in $\mathbb{Z}[x]$ such that*

$$p^d \;\equiv\; a_1 f_2 f_3 \,+\, a_2 f_1 f_3 \,+\, a_3 f_1 f_2 \pmod{p^{d+k}\mathbb{Z}[x]}$$

*with $f_1$, $f_2$, $f_3$ monic and $d \geq 0$, $k \geq 1$.*

*Show that if $w \in \mathbb{Z}[x]$ with*

$$\begin{aligned} w \ \mathbf{mod}\ f_0 &= \ \ w - q_0 f_0, \\ a_1 w \ \mathbf{mod}\ f_1 &= a_1 w - q_1 f_1, \\ a_2 w \ \mathbf{mod}\ f_2 &= a_2 w - q_2 f_2, \\ a_3 w \ \mathbf{mod}\ f_3 &= a_3 w - q_3 f_3, \end{aligned}$$

*where $f_0 = f_1 f_2 f_3$, then*

$$q_1 + q_2 + q_3 \;\equiv\; p^d q_0 \pmod{p^{d+k}\mathbb{Z}[x]}.$$

***Exercise: Quadratic Hensel Lifting (with $p$ arbitrary).***

*Let $f$, $f_1$, $f_2$, $f_3$, $a_1$, $a_2$, $a_3$ be polynomials in $\mathbb{Z}[x]$, such that*

$$(1.1) \qquad f \;\equiv\; f_1 f_2 f_3 \pmod{p^{2d+k}\mathbb{Z}[x]},$$

$$(1.2) \qquad p^d \;\equiv\; a_1 f_2 f_3 \,+\, a_2 f_1 f_3 \,+\, a_3 f_1 f_2 \pmod{p^{d+k}\mathbb{Z}[x]},$$

*with $f$, $f_1$, $f_2$, $f_3$ monic and $d \geq 0$, $k \geq 1$.*

*Show that if*

$$\begin{aligned} \widehat{f_1} &= f_1 + p^{d+k} a_1 u \ \mathbf{mod}\ f_1, & \widehat{a}_1 &= a_1 + p^k a_1 w \ \mathbf{mod}\ \widehat{f_1}, \\ \widehat{f_2} &= f_2 + p^{d+k} a_2 u \ \mathbf{mod}\ f_2, & \widehat{a}_2 &= a_2 + p^k a_2 w \ \mathbf{mod}\ \widehat{f_2}, \\ \widehat{f_3} &= f_3 + p^{d+k} a_3 u \ \mathbf{mod}\ f_3, & \widehat{a}_3 &= a_3 + p^k a_3 w \ \mathbf{mod}\ \widehat{f_3}, \end{aligned}$$

*with*

$$u \;=\; \frac{f - f_1 f_2 f_3}{p^{2d+k}}, \quad w \;=\; \frac{p^d - a_1\widehat{f_2}\widehat{f_3} - a_2\widehat{f_1}\widehat{f_3} - a_3\widehat{f_1}\widehat{f_2}}{p^{d+k}},$$

*then*

$$(2.1) \qquad f \;\equiv\; \widehat{f_1}\widehat{f_2}\widehat{f_3} \pmod{p^{2d+2k}\mathbb{Z}[x]},$$

$$(2.2) \qquad p^d \;\equiv\; \widehat{a}_1\widehat{f_2}\widehat{f_3} \,+\, \widehat{a}_2\widehat{f_1}\widehat{f_3} \,+\, \widehat{a}_3\widehat{f_1}\widehat{f_2} \pmod{p^{d+2k}\mathbb{Z}[x]}.$$

If you need to, you may assume

$$\deg a_1 < \deg f_1, \quad \deg a_2 < \deg f_2, \quad \deg a_3 < \deg f_3.$$