Journal de Théorie des Nombres
de Bordeaux **14** (2002), 151–169

A fast algorithm for polynomial factorization over $\mathbb{Q}_p$

par David FORD*, Sebastian PAULI† et Xavier-François ROBLOT*

Résumé. Dans cet article, nous présentons un algorithme qui retourne pour un polynôme $\Phi(x)$ à coefficients dans l'anneau $\mathbb{Z}_p$ des entiers p-adiques, soit un facteur propre de ce polynôme, soit, dans le cas où $\Phi(x)$ est irréductible, un élément générateur de l'anneau des entiers de $\mathbb{Q}_p[x]/\Phi(x)\mathbb{Q}_p[x]$. Cet algorithme se fonde sur l'algorithme Round Four pour le calcul de l'ordre maximal. Les expérimentations montrent que le nouvel algorithme est cependant beaucoup plus performant que l'algorithme Round Four.

Abstract. We present an algorithm that returns a proper factor of a polynomial $\Phi(x)$ over the p-adic integers $\mathbb{Z}_p$ (if $\Phi(x)$ is reducible over $\mathbb{Q}_p$) or returns a power basis of the ring of integers of $\mathbb{Q}_p[x]/\Phi(x)\mathbb{Q}_p[x]$ (if $\Phi(x)$ is irreducible over $\mathbb{Q}_p$). Our algorithm is based on the Round Four maximal order algorithm. Experimental results show that the new algorithm is considerably faster than the Round Four algorithm.

1. Introduction.

We consider the problem of factoring polynomials with p-adic coefficients.

Restricting our attention to monic, square-free polynomials in $\mathbb{Z}_p[x]$, we present a method to compute the complete factorization of such polynomials into irreducible factors in $\mathbb{Z}_p[x]$. Our algorithm has its origins in the Round Four algorithm of Zassenhaus, but with substantial modifications. The new algorithm is much faster than the "classical" Round Four algorithm, and also more straightforward.

In Section 2 we establish some notation. In Section 3 we establish a criterion for a polynomial to be reducible over $\mathbb{Q}_p$.

If $\Phi(x)$ is a monic, square-free polynomial in $\mathbb{Z}_p[x]$, then $\Phi(x)$ is reducible over $\mathbb{Q}_p$ if and only if there exists a polynomial $\theta(x)$ in $\mathbb{Q}_p[x]$ such that the polynomial resultant $\operatorname{Res}_x\big(\Phi(x), t-\theta(x)\big)$ of

Manuscrit reçu le 5 avril 2001.
*supported in part by NSERC (Canada) and FCAR/CICMA (Québec).
†supported in part by ISM and FCAR/CICMA (Québec).

$\Phi(x)$ and $t-\theta(x)$ belongs to $\mathbb{Z}_p[t]$ and has more than one distinct irreducible factor modulo p.

We further show how to construct a proper factorization of $\Phi(x)$ if such a polynomial $\theta(x)$ is known.

In Section 4 we define polynomials of "Eisenstein form" and give a criterion for $\Phi(x)$ to be irreducible over $\mathbb{Q}_p$.

The polynomial $\Phi(x)$ is irreducible over $\mathbb{Q}_p$ if and only if there exists a polynomial $\alpha(x)$ in $\mathbb{Q}_p[x]$ such that the resultant $\mathrm{Res}_x\big(\Phi(x), t-\alpha(x)\big)$ belongs to $\mathbb{Z}_p[t]$ and is of Eisenstein form.

We say that such a polynomial $\alpha(x)$ *certifies (the irreducibility of)* $\Phi(x)$.

In Section 5 we describe procedures which, given $\Phi(x)$, yield a proper factorization of $\Phi(x)$ if $\Phi(x)$ is reducible, or return a certifying polynomial $\alpha(x)$ for $\Phi(x)$, if $\Phi(x)$ is irreducible.

In Section 6 we show how the results of these procedures can be used to determine ideal factorizations and $\mathbb{Z}_p$-bases for p-maximal orders.

In four Appendices we give details regarding p-adic GCD computation, the Hensel lifting threshhold, factorization of resultant polynomials modulo p, and experimental results.

2. Notation.

In what follows, Φ is a monic separable polynomial with coefficients in $\mathbb{Z}_p$, which we aim to factorize completely over $\mathbb{Q}_p$. We take $\xi_1, \ldots, \xi_n$ to be the roots of Φ in some fixed algebraic closure of $\mathbb{Q}_p$, and we denote by v_p the p-adic valuation of $\mathbb{Q}_p$, extended to $\mathbb{Q}_p(\xi_1, \ldots, \xi_n)$ and normalized so that $v_p(p) = 1$. For $\varphi(t)$ in $\mathbb{Z}_p[t]$ we denote by $\overline{\varphi}(t)$ its image $\varphi(t) + p\mathbb{Z}_p[t]$ in $\mathbb{Z}_p[t]/p\mathbb{Z}_p[t] \cong \mathbb{F}_p[t]$.

Let $\mathrm{Res}_x\big(f(x), g(x)\big)$ denote the resultant of the polynomials $f(x)$ and $g(x)$ with respect to the variable x. It is well known that $\mathrm{Res}_x\big(f(x), g(x)\big) = 0$ if and only if $f(x)$ and $g(x)$ have a common root. Suppose $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$. Then $\mathrm{Res}_x\big(f(x), \lambda - g(x)\big) = 0$ if and only if $\lambda = g(\alpha_i)$ for some i, and it follows that

$$\mathrm{Res}_x\big(f(x), t-g(x)\big) = \big(t-g(\alpha_1)\big)\cdots\big(t-g(\alpha_n)\big).$$

Definition 2.1. For $\theta(x) \in \mathbb{Q}_p[x]$ we define

$$\chi_\theta(t) = \big(t-\theta(\xi_1)\big)\cdots\big(t-\theta(\xi_n)\big) \quad \text{and} \quad \Delta_\theta = \prod_{i<j}\big(\theta(\xi_i)-\theta(\xi_j)\big)^2.$$

We also define

$$\mathcal{O}_\Phi = \big\{\, \theta(x) \in \mathbb{Q}_p[x] \;\big|\; \chi_\theta(t) \in \mathbb{Z}_p[t] \,\big\}.$$

For $\theta(x)$ in $\mathcal{O}_\Phi$ with $\Delta_\theta \neq 0$, the *reduced discriminant* of χ_θ is p^{d_θ}, given by

$$p^{d_\theta}\mathbb{Z}_p = \big(\chi_\theta(t)\mathbb{Z}_p[t] + \chi'_\theta(t)\mathbb{Z}_p[t]\big) \cap \mathbb{Z}_p.$$

Remark 2.2. It is clear that $\chi_\theta(t) = \mathrm{Res}_x\big(\Phi(x), t - \theta(x)\big) \in \mathbb{Q}_p[t]$.

Remark 2.3. If $\theta_1(x) \equiv \theta_2(x) \bmod \Phi(x)\mathbb{Z}_p[x]$ then $\chi_{\theta_1}(t) = \chi_{\theta_2}(t)$.

Remark 2.4. $\theta(x)$ belongs to $\mathcal{O}_\Phi$ if and only if $\theta(\xi_1), \ldots, \theta(\xi_n)$ are all integral over $\mathbb{Z}_p$.

Remark 2.5. χ_θ is not necessarily the characteristic polynomial of a single field element; in general it is the product of several such characteristic polynomials.

Remark 2.6. The reduced discriminant p^{d_θ} can be obtained directly from the p-adic Hermite normal form of the Sylvester matrix of χ_θ and χ'_θ.

Remark 2.7. Let $\theta(x) \in \mathcal{O}_\Phi$ with $\Delta_\theta \neq 0$ and let ξ be an arbitrary root of $\Phi(x)$. If $\mathcal{O}_K$ is the ring of integers of the field $K = \mathbb{Q}_p(\xi)$ then $p^{d_\theta}\mathcal{O}_K \subseteq \mathbb{Z}_p[\theta(\xi)] \subseteq \mathcal{O}_K$.

3. Reducibility over $\mathbb{Q}_p$.

Let $\theta(x) \in \mathcal{O}_\Phi$ with $\chi_\theta(t) = t^n + c_1 t^{n-1} + \cdots + c_n$, and define

$$v_p^*(\theta) = \min_{1 \le k \le n} \frac{v_p(c_k)}{k}.$$

Taking $\theta_i = \theta(\xi_i)$ for $i = 1, \ldots, n$ and expressing $c_1, \ldots, c_n$ as symmetric functions in the θ_i's, it is easily seen (as in [9, Section 3-1]) that

$$v_p^*(\theta) = \min\big(v_p(\theta_1), \ldots, v_p(\theta_n)\big).$$

Because $v_p(c_n)/n = \big(v_p(\theta_1) + \cdots + v_p(\theta_n)\big)/n$, it follows that $v_p^*(\theta) = v_p(c_n)/n$ if and only if $v_p(\theta_1) = \cdots = v_p(\theta_n)$.

But suppose $v_p^*(\theta) = A/B < v_p(c_n)/n$. Taking $\varphi(x) = \theta(x)^B/p^A$ and $\varphi_i = \varphi(\xi_i)$ for $i = 1, \ldots, n$, we have

$$\min\big(v_p(\varphi_1), \ldots, v_p(\varphi_n)\big) = 0 < \max\big(v_p(\varphi_1), \ldots, v_p(\varphi_n)\big)$$

and consequently $\chi_\varphi(t)$ will have at least two distinct irreducible factors modulo p.

Proposition 3.1. *If there exists $\theta(x)$ in $\mathcal{O}_\Phi$ such that $\chi_\theta(t)$ has at least two distinct non-trivial irreducible factors modulo p then $\Phi(x)$ is reducible in $\mathbb{Z}_p[x]$.*

Proof. Assume $\theta(x)$ belongs to $\mathcal{O}_\Phi$ with $\chi_\theta(t)$ having at least two distinct non-trivial irreducible factors modulo p.

Hensel lifting gives relatively prime monic polynomials $\varphi_1(t)$ and $\varphi_2(t)$ in $\mathbb{Z}_p[t]$ with $0 < \deg\varphi_1 < \deg\chi_\theta$, $0 < \deg\varphi_2 < \deg\chi_\theta$, such that

$$\chi_\theta(t) = \varphi_1(t)\varphi_2(t).$$

Reordering the roots of Φ if necessary, we may write

$$\varphi_1(t) = \big(t - \theta(\xi_1)\big)\cdots\big(t - \theta(\xi_r)\big), \quad \varphi_2(t) = \big(t - \theta(\xi_{r+1})\big)\cdots\big(t - \theta(\xi_n)\big)$$

with $1 \le r \le n-1$, and it follows that

$$\Phi(x) = \gcd\Big(\Phi(x),\, \varphi_1\big(\theta(x)\big)\Big)\cdot\gcd\Big(\Phi(x),\, \varphi_2\big(\theta(x)\big)\Big)$$

is a proper factorization of $\Phi(x)$. □

Remark 3.2. See Appendix A for details of the computation of the p-adic GCD.

Example 3.3. Let

$$p = 5, \quad \Phi(x) = x^4 + 25x^2 + 50x + 25, \quad \theta(x) = \tfrac{1}{5}x^2$$

and observe that $\sqrt{-1} \in \mathbb{Z}_5$. Then

$$\chi_\theta(t) = t^4 + 10t^3 + 27t^2 - 10t + 1 \equiv (t+2)^2(t-2)^2 \bmod 5$$

and $\overline{\chi}_\theta(t)$ has two distinct irreducible factors in $\mathbb{F}_5[t]$. The Hensel construction leads to

$$\varphi_1(t) = t^2 + (5 - 2\sqrt{-1})t - 1$$
$$\varphi_2(t) = t^2 + (5 + 2\sqrt{-1})t - 1$$

$$\varphi_1\big(\theta(x)\big) = \tfrac{1}{25}\big(x^4 + (25 - 10\sqrt{-1})x^2 - 25\big)$$
$$\varphi_2\big(\theta(x)\big) = \tfrac{1}{25}\big(x^4 + (25 + 10\sqrt{-1})x^2 - 25\big)$$

$$\gcd\Big(\Phi(x),\, \varphi_1\big(\theta(x)\big)\Big) = x^2 - 5\sqrt{-1}x - 5\sqrt{-1}$$
$$\gcd\Big(\Phi(x),\, \varphi_2\big(\theta(x)\big)\Big) = x^2 + 5\sqrt{-1}x + 5\sqrt{-1}$$

and we have a proper factorization of $\Phi(x)$.

Definition 3.4. Let $\theta(x) \in \mathcal{O}_\Phi$ with $\chi_\theta(t) = t^n + c_1t^{n-1} + \cdots + c_n$.

(i) We say θ passes the Hensel test if $\overline{\chi}_\theta(t) = \overline{\nu}_\theta(t)^e$ for some $e \ge 1$ and some irreducible monic polynomial $\overline{\nu}_\theta(t)$ in $\mathbb{F}_p[t]$.

(ii) We say θ passes the Newton test if

$$\frac{v_p(c_n)}{n} \le \frac{v_p(c_k)}{k} \quad \text{for } k = 1, \ldots, n-1.$$

Remark 3.5. If θ passes the Hensel test and $\overline{\nu}_\theta(t) \neq t$ then θ passes the Newton test.

Remark 3.6. If θ passes the Newton test then

$$v_p\big(\theta(\xi_1)\big) = \cdots = v_p\big(\theta(\xi_n)\big) = v_p^*(\theta).$$

Proposition 3.7. *If any member of $\mathcal{O}_\Phi$ fails either the Hensel test or the Newton test then $\Phi(x)$ is reducible in $\mathbb{Z}_p[x]$.*

Proof. This follows from Proposition 3.1. □

4. Irreducibility over $\mathbb{Q}_p$.

Definition 4.1. A monic polynomial $\chi(t)$ in $\mathbb{Z}_p[t]$ is of *Eisenstein form* if there exists a monic polynomial $\nu(t)$ in $\mathbb{Z}_p[t]$, irreducible modulo p, such that

$$\chi(t) = \nu(t)^k + p\big(q(t)\nu(t) + r(t)\big)$$

with $q(t)$ in $\mathbb{Z}_p[t]$, $r(t)$ in $\mathbb{Z}_p[t] \setminus p\mathbb{Z}_p[t]$, $\deg r < \deg \nu$, and $k > 0$.

Remark 4.2. If $\chi(t)$ is irreducible modulo p then $\chi(t)$ is of Eisenstein form. (Take $\nu(t) = \chi(t) - p$, for example.)

Remark 4.3. An *Eisenstein polynomial* is a polynomial of Eisenstein form with $\nu(t) = t$.

Proposition 4.4. *If $\chi(t)$ is of Eisenstein form then $\chi(t)$ is irreducible in $\mathbb{Z}_p[t]$.*

Proof. If there is a factorization $\chi(t) = \big(\nu(t)^{k_1} + p\varphi_1(t)\big)\big(\nu(t)^{k_2} + p\varphi_2(t)\big)$, with $k_1 > 0$, $k_2 > 0$, and with χ and ν satisfying the conditions of the definition, then the requirement $r(t) \notin p\mathbb{Z}_p[t]$ cannot be met. □

Proposition 4.5. *Let K be a finite extension of $\mathbb{Q}_p$ with $\mathcal{O}_K$ its ring of integers and $\mathfrak{P}$ its prime ideal. Let $\nu(x)$ be a monic polynomial in $\mathbb{Z}_p[x]$ with $\nu(x)$ irreducible modulo p and let α be an element of $\mathcal{O}_K$ such that $\nu(\alpha) \in \mathfrak{P}$. Then the minimal polynomial of α over $\mathbb{Q}_p$ is of Eisenstein form if and only if $\nu\big(\alpha\big)$ is a prime element of $\mathcal{O}_K$ and $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_p[\overline{\alpha}]$.*

Proof. If the minimal polynomial of α is of Eisenstein form then it is congruent modulo p to a power of ν, and it follows directly that $\nu\big(\alpha\big)$ is prime and $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_p[\overline{\alpha}]$.

To prove the converse, let $\pi = \nu(\alpha)$, $v_p(\pi) = 1/E$, $\deg \nu = F$, and define

$$R_x = \big\{\, c_0 + c_1 x + \cdots + c_{F-1}x^{F-1} \;\big|\; c_i \in \mathbb{Z},\ \lceil -(p-1)/2 \rceil \le c_i \le \lfloor p/2 \rfloor \text{ for } 0 \le i \le F-1 \,\big\}.$$

Then the set R_α is a complete set of representatives of $\mathcal{O}_K/\mathfrak{P}$ and π^E/p is a unit in $\mathcal{O}_K$. Therefore π^E/p has the π-adic expansion

$$\begin{aligned}\pi^E/p = \quad & \lambda_{1,0} + \lambda_{1,1}\pi + \cdots + \lambda_{1,E-1}\pi^{E-1} \\ + \quad & p\big(\lambda_{2,0} + \lambda_{2,1}\pi + \cdots + \lambda_{2,E-1}\pi^{E-1}\big) \\ + \; & p^2\big(\lambda_{3,0} + \lambda_{3,1}\pi + \cdots + \lambda_{3,E-1}\pi^{E-1}\big) \\ + \; & \cdots\end{aligned}$$

with each $\lambda_{j,k}$ belonging to R_α and $v_p(\lambda_{1,0}) = 0$. For $1 \le j < \infty$ and $0 \le k \le E-1$ there exists $\delta_{j,k}(x)$ in R_x such that $\lambda_{j,k} = \delta_{j,k}\big(\alpha\big)$. The polynomial

$$\beta(x) = \nu(x)^E - p\sum_{k=0}^{E-1}\left(\sum_{j=1}^{\infty} p^{j-1}\delta_{j,k}(x)\right)\nu(x)^k$$

is of Eisenstein form (since $\lambda_{1,0}$ is a unit) and $\beta\big(\alpha\big) = 0$. It follows that $\beta(x)$ is the minimal polynomial of α over $\mathbb{Q}_p$. □

Definition 4.6. Let $\Psi(x)$ be a monic polynomial belonging to $\mathbb{Z}_p[x]$ and let $\alpha(x) \in \mathbb{Q}_p[x]$. We say $\alpha(x)$ *certifies* Ψ *if* $\mathrm{Res}_x\big(\Psi(x), t-\alpha(x)\big)$ *is of Eisenstein form.*

Proposition 4.7. *If* $\alpha(x)$ *certifies* Φ *and* $\widehat{\alpha}(x) \in \mathbb{Q}_p[x]$ *such that* $\widehat{\alpha}(x) \equiv \alpha(x) \bmod p^2\mathbb{Z}_p[x]$ *then* $\widehat{\alpha}(x)$ *also certifies* Φ.

Proof. Let $h(t) = \big(\chi_{\widehat{\alpha}}(t) - \chi_\alpha(t)\big)/p^2$. The coefficients of $h(t)$ are integral and lie in $\mathbb{Q}_p$, hence $h(t) \in \mathbb{Z}_p[t]$. It follows that $\chi_{\widehat{\alpha}}(t)$ is of Eiseinstein form, if $\chi_\alpha(t)$ is. □

Definition 4.8. For $\theta(x)$ belonging to $\mathcal{O}_\Phi$ and passing the Hensel and Newton tests we define $\nu_\theta(t)$ to be an arbitrary monic polynomial in $\mathbb{Z}_p[t]$, with $\overline{\nu}_\theta(t)$ irreducible in $\mathbb{F}_p[t]$, such that $\overline{\chi}_\theta(t) = \overline{\nu}_\theta(t)^e$ for some $e \ge 1$, and we set

$$F_\theta = \deg(\overline{\nu}_\theta).$$

If $\nu_\theta(\theta)$ also passes the Hensel and Newton tests we additionally define

$$\begin{aligned}N_\theta/E_\theta &= v_p^*\big(\nu_\theta(\theta)\big),\\ \pi_\theta(t) &= \nu_\theta(t)^r/p^s\end{aligned}$$

with $\gcd(N_\theta, E_\theta) = 1$, $rN_\theta - sE_\theta = 1$, and $0 \le r \le E_\theta - 1$.

Remark 4.9. $v_p^*(\pi_\theta(\theta)) = 1/E_\theta$.

Remark 4.10. If $E_\theta = 1$ then $\pi_\theta(\theta) = p$.

Remark 4.11. If θ and $\nu_\theta(\theta)$ both pass the Hensel and Newton tests then $E_\theta \mid n$ and $F_\theta \mid n$.

Remark 4.12. If $\alpha(x)$ belongs to $\mathcal{O}_\Phi$ and passes the Hensel and Newton tests and $d_\alpha = 0$ then $\overline{\chi}_\alpha(t) = \overline{\nu}_\alpha(t)$, which is irreducible in $\mathbb{F}_p[t]$, and it follows that $\alpha(x)$ certifies $\Phi(x)$.

Proposition 4.13. *Let Φ be irreducible over $\mathbb{Q}_p$, with ξ an arbitrary root of Φ, and let $\mathcal{O}_K$ be the ring of integers of the field $K = \mathbb{Q}_p(\xi)$. For $\alpha(x)$ in $\mathcal{O}_\Phi$ the following are equivalent.*
(i) *$\alpha(x)$ certifies Φ.*
(ii) *$\pi_\alpha(\alpha) = \nu_\alpha(\alpha)$ and $E_\alpha F_\alpha = n$.*
(iii) *$\mathcal{O}_K = \mathbb{Z}_p[\alpha(\xi)]$.*

Proof. By Proposition 3.1 we have $\overline{\chi}_\alpha(t) = \overline{\nu}_\alpha(t)^k$ for some $k \geq 1$, and hence we may write $\chi_\alpha(t) = \nu_\alpha(t)^k + p\big(q(t)\nu_\alpha(t) + r(t)\big)$ with $q(t) \in \mathbb{Z}_p[t]$, $r(t) \in \mathbb{Z}_p[t]$, and $\deg r < \deg \nu_\alpha$. Moreover, we have $\mathcal{O}_K = \{\, \theta(\xi) \mid \theta(x) \in \mathcal{O}_\Phi \,\}$ and $v_p^*(\theta) = v_p\big(\theta(\xi)\big)$ for all $\theta(x) \in \mathcal{O}_\Phi$.

(i) $\Longrightarrow$ (ii). If $\overline{\chi}_\alpha(t)$ is irreducible in $\mathbb{F}_p[t]$ then $E_\alpha = 1$ and $F_\alpha = n$. Otherwise $v_p^*\big(r(\alpha)\big) = 0$, so that $kN_\alpha/E_\alpha = v_p^*\big(\nu_\alpha(\alpha)^k\big) = 1 + v_p^*\big(q(\alpha)\nu_\alpha(\alpha) + r(\alpha)\big) = 1$, hence $E_\alpha/N_\alpha = k \in \mathbb{Z}$, hence $N_\alpha = 1$, hence $\pi_\alpha(\alpha) = \nu_\alpha(\alpha)$ and $n = kF_\alpha = E_\alpha F_\alpha$.

(ii) $\Longrightarrow$ (iii). Let $\mu(t) \in \mathbb{Z}_p[t]$ be a monic polynomial of minimal degree such that $\mu\big(\alpha(\xi)\big) \in p\mathcal{O}_K$. Then $\mu(t) \equiv \nu_\alpha(t)^e \bmod p\mathbb{Z}_p[t]$ for some $e \geq 1$ (otherwise $\deg\gcd(\overline{\mu}, \overline{\chi}_\alpha) < \deg\overline{\mu}$, and the degree of μ could be reduced), so $e/E_\alpha = v_p^*\big(\nu_\alpha(\alpha)^e\big) \geq 1$ and $\deg\mu = eF_\alpha \geq E_\alpha F_\alpha = n$. Hence $K = \mathbb{Q}_p\big(\alpha(\xi)\big)$, and it is clear that any integral basis for K must be contained in $\mathbb{Z}_p[\alpha(\xi)]$.

(iii) $\Longrightarrow$ (i). If $\overline{\chi}_\alpha(t)$ is not irreducible in $\mathbb{F}_p[t]$ then $k > 1$, and we have $r(t) \notin p\mathbb{Z}_p[t]$ because otherwise $\nu_\alpha\big(\alpha(\xi)\big)^{k-1}/p$ would be a root of $X^2 + q\big(\alpha(\xi)\big)X + \nu_\alpha\big(\alpha(\xi)\big)^{k-2} r\big(\alpha(\xi)\big)/p$ and so would belong to $\mathcal{O}_K$ but not to $\mathbb{Z}_p[\alpha(\xi)]$. □

Proposition 4.14. *Φ is irreducible over $\mathbb{Q}_p$ if and only if some $\alpha(x)$ in $\mathbb{Q}_p[x]$ certifies Φ.*

Proof. By Proposition 4.4, Φ is irreducible over $\mathbb{Q}_p$ if $\alpha(x)$ certifies Φ. For the converse, let ξ be a root of Φ and let $K = \mathbb{Q}_p(\xi)$. By [6, Proposition 5.6] there exists $\alpha(x) \in \mathbb{Q}_p[x]$ such that $1, \alpha(\xi), \ldots, \alpha(\xi)^{n-1}$ is an integral basis for K. By Proposition 4.13, $\alpha(x)$ certifies Φ. □

5. Factorization Algorithms

In this section we describe Algorithms 5.1 and 5.3, which together produce a polynomial $\alpha(x) \in \mathbb{Q}_p[x]$ certifying $\Phi(x)$ or else find a proper factorization of $\Phi(x)$.

Algorithm 5.1, below, takes monic polynomials $\chi(x)$ and $\nu(x)$ with

- $\chi(x) \in \mathbb{Z}_p[x]$ squarefree,

- $\nu(x) \in \mathbb{Z}_p[x]$ irreducible modulo p,
- $\chi(x) \equiv \nu(x)^e \bmod p\mathbb{Z}_p[x]$ for some $e > 0$,
- $\chi(x) = (x - \alpha_1)\cdots(x - \alpha_n)$,
- $v_p(\nu(\alpha_1)) = \cdots = v_p(\nu(\alpha_n)) = 1/E$,
- $\deg \nu = F$,
- $EF < n$,

and returns either

- a proper factorization of $\chi(x)$, or
- a polynomial $\varphi(x)$ such that $E_\varphi F_\varphi > EF$, with $E_\varphi \geq E$ and $F_\varphi \geq F$.

The algorithm attempts to construct the π-adic expansion given in the proof of Proposition 4.5. The algorithm proceeds by computing the digits $\lambda_{j,k}$ as roots of polynomials over the finite field $\mathbb{F}_p[\overline{\alpha}]$. Because $\deg \beta = EF < \deg \chi$, there will at some point be more than one choice for $\delta_{j,k}(x)$, and this condition suffices to factorize $\chi(x)$. Also, for each j, k the algorithm checks if the threshhold for Hensel lifting has been reached (see Appendix B), in which case $\beta_{j,k}(x)$ approximates $\beta(x)$ sufficiently well to give a factorization of $\chi(x)$.

If $\mathcal{O}_K/\mathfrak{P} \supsetneqq \mathbb{F}_p[\overline{\alpha}]$ then the π-adic expansion does not exist, and the construction will eventually come to a digit $\lambda_{j,k}$ not belonging to R_α. This gives an element $\gamma \in \mathcal{O}_K$ such that $\mathbb{F}_p[\overline{\alpha}, \overline{\gamma}] \supsetneqq \mathbb{F}_p[\overline{\alpha}]$, which leads to the construction of a polynomial $\varphi(x) \in \mathcal{O}_\Phi$ with $F_\varphi > F$ and $E_\varphi \geq E$.

If $\nu(\alpha)$ is not a prime element of $\mathcal{O}_K$ then the π-adic expansion does not exist, and the construction will reach a point where $v_p(\beta_{j,k}(\alpha))$ is not a multiple of $1/E$. This leads to the construction of a polynomial $\varphi(x) \in \mathcal{O}_\Phi$ with $E_\varphi > E$ and $F_\varphi = F$.

Algorithm 5.1.

Note: References to field elements apply to all embeddings simultaneously; "$\beta(\alpha) \in \mathbb{Z}_p[\theta(\alpha)]$" means "$\beta(\alpha_i) \in \mathbb{Z}_p[\theta(\alpha_i)]$ for $i = 1, \ldots, n$", *etc.*

1. Find $\kappa(x) \in \mathbb{Q}_p[x]$ with $\kappa(x)\nu(x) \equiv 1 \bmod \chi(x)$. [$\kappa(\alpha) = 1/\nu(\alpha)$.]
Set $\beta(x) = \nu(x)^E$. [Initially $N_\beta/E_\beta = v_p(\beta(\alpha)) = 1$.]

2. Set $j = \lfloor v_p(\beta(\alpha)) \rfloor$, $k = (v_p(\beta(\alpha)) - j)E$. [$k \in \mathbb{Z}$, as $E_\beta \mid E$.]
Set $\gamma(x) = p^{-j}\kappa(x)^k\beta(x) \bmod \chi(x)$.
[$v_p(\gamma(\alpha)) = 0$, because $\gamma(\alpha) = \beta(\alpha)/p^j\nu(\alpha)^k$.]
If γ fails the Hensel test then go to step **13**.
If $F_\gamma \nmid F$ then go to step **12**.

3. Find $\delta(x) = c_0 + c_1x + \cdots + c_{F-1}x^{F-1}$ such that $\overline{\nu}_\gamma(\delta(\overline{\alpha})) = \overline{0}$ and $v_p(\gamma(\alpha_j) - \delta(\alpha_j)) > 0$ for some j.
[$\overline{\nu}_\gamma(x)$ splits completely over $\mathbb{F}_p[\overline{\alpha}]$, because $F_\gamma \mid F$.]
If $\gamma - \delta$ fails either the Hensel test or the Newton test then go to step **13**.

4. Replace $\beta(x) \leftarrow \beta(x) - p^j \nu(x)^k \delta(x)$.
[$N_\beta/E_\beta \leftarrow N_\beta/E_\beta + N_{\gamma-\delta}/E_{\gamma-\delta}$.]
If $E_\beta \nmid E$ then go to step **11**.
If $\beta(x)$ is sufficiently precise then go to step **13**.
[Hensel lifting applies.]
Go to step **2**.

11. Find a, b, $c \geq 0$ such that $(aN_\beta - cE_\beta)E + bE_\beta = \gcd(E, E_\beta)$.
Set $\varphi(x) = x + \nu(x)^b \beta(x)^a / p^c \bmod \chi(x)$.
[$E_\varphi = \mathrm{lcm}(E, E_\beta) > E,\ F_\varphi = F$.]
Return $\varphi(x)$.

12. Find $\varphi(x) \in \mathbb{Z}_p[x, \gamma(x)]$ with $\mathbb{F}_p[\overline{\varphi}] = \mathbb{F}_p[\overline{\alpha}, \overline{\gamma}]$. [$F_\varphi = \mathrm{lcm}(F, F_\gamma)$.]
If φ fails the Hensel test then go to step **13**.
If $\nu_\varphi(\varphi)$ fails the Newton test then go to step **13**.
If $E_\varphi < E$, replace $\varphi(x) \leftarrow \varphi(x) + \nu(x)$. [$E_\varphi \geq E,\ F_\varphi > F$.]
Return $\varphi(x)$.

13. **Return** a proper factorization of $\chi(x)$. [$\chi(x)$ is reducible.]

Remark 5.2. In [7] it is shown that Algorithm 5.1 above terminates before $v_p(\beta_{j,k}(\alpha))$ becomes greater than $2v_p(\mathrm{disc}\chi)/\deg(\Phi)$.

With $\Phi(x)$ as input, Algorithm 5.3 returns either

- a polynomial $\alpha(x)$ in $\mathcal{O}_\Phi$ certifying $\Phi(x)$ or
- a proper factorization of $\chi(x)$.

Initially $\alpha(x) = x$; then $\alpha(x)$ is iteratively replaced by $\varphi(x)$ until either

- Algorithm 5.1 gives a proper factorization of $\chi(x)$ or
- $E_\alpha F_\alpha = n$.

The condition $E_\alpha F_\alpha = n$ implies that $\chi_\alpha(x)$ is of Eisenstein form, so that $\alpha(x)$ certifies Φ.

Algorithm 5.3.

1. Set $\alpha(x) = x$.

2. While $\Delta_\alpha = 0$, replace $\alpha(x) \leftarrow \alpha(x) + px$.
[This makes χ_α separable.]
If $\alpha(x)$ or $\nu_\alpha(\alpha(x))$ fails either the Hensel test or the Newton test, go to step **11**.
If $N_\alpha > 1$ then replace $\alpha(x) \leftarrow \alpha(x) + \pi_\alpha(\alpha(x))$.
[This gives $v_p(\nu_\alpha(\alpha)) = 1/E_\alpha$, with ν_α and E_α unchanged.]
If $E_\alpha F_\alpha = n$ then go to step **12**.
[If $E_\alpha F_\alpha = n$ then χ_α is of Eisenstein form.]

3. Apply Algorithm 5.1 to the pair $[\chi_\alpha(x), \nu_\alpha(x)]$.
If Algorithm 5.1 returns a proper factorization of $\chi_\alpha(x)$ then go to step **11**.
Replace $\alpha(x) \leftarrow \varphi(x)$.
Go to step **2**.

11. Return a proper factorization of $\Phi(x)$. [$\Phi(x)$ is reducible.]

12. Return $\alpha(x)$. [$\Phi(x)$ is irreducible; $\alpha(x)$ confirms $\Phi(x)$.]

Example 5.4. Let

$$p = 5, \quad \chi(x) = x^4 + 127x^3 + 43x^2 + 42x - 259, \quad \nu(x) = x^2 + x + 1.$$

Then

$$\chi(x) = \nu(x)^2 + p\big(q(x)\nu(x) + r(x)\big)$$

with $q(x) = 25x - 17$, $r(x) = -35$, so $\chi(x)$ is not of Eisenstein form. Now

$$\chi_\nu(t) = t^4 - (2^4 \cdot 5 \cdot 199)t^3 + (5^4 \cdot 53)t^2 + (5^3 \cdot 7 \cdot 59)t + (5^4 \cdot 7^2)$$

and so $v_p\big(\nu(\alpha)\big) = 1$. Our initial approximation to the minimal polynomial of α is

$$\beta_{0,0}(x) = \nu(x) = x^2 + x + 1.$$

Because $v_p\big(\beta_{0,0}(\alpha)\big) = 1$, the element

$$\gamma(\alpha) = \beta_{0,0}(\alpha)/p = (\alpha^2 + \alpha + 1)/5$$

must be a unit. We have

$$\chi_\gamma(t) = t^4 - 3184t^3 + 1325t^2 + 413t + 49 \equiv (t^2 + 3t + 3)^2 \bmod p\mathbb{Z}_p[t],$$
$$\overline{\nu}_\gamma(t) = t^2 + 3t + 3 = (t + \overline{\alpha} + 2)(t - \overline{\alpha} + 1).$$

This gives two choices for $\delta(x)$, namely $\delta(x) = -x - 2$ or $\delta(x) = x - 1$, and in fact $\gamma(x) - \delta(x)$ fails the Hensel test for each choice. Note that if we choose $\delta(x) = -x - 2$ and set

$$\psi_1(x) = \beta_{0,0}(x) - p\delta(x) = x^2 + 6x + 11, \quad \psi_2(x) = x^2 + 121x - 694,$$

$\psi_2(x)$ being the euclidean quotient of $\chi(x)$ on division by $\psi_1(x)$, then

$$\chi(x) \equiv \psi_1(x)\psi_2(x) \bmod p^3\mathbb{Z}_p[x],$$
$$p \equiv (6x + 3)\psi_1(x) + (19x + 12)\psi_2(x) \bmod p^2\mathbb{Z}_p[x],$$

which are sufficient conditions to apply Hensel lifting.

Example 5.5. Let

$$p = 2, \quad \Phi(x) = x^6 + 16x^5 + 8x^4 - 20.$$

Initially $\alpha(x) = x$, so that

$$\pi_\alpha(t) = \nu_\alpha(t) = t, \quad F_\alpha = 1, \quad E_\alpha = 3.$$

For $j = 1$, $k = 0$:

$$\beta_{1,0}(x) = \nu_\alpha(x)^{E_\alpha} = x^3,$$

$$v_p\big(\beta_{1,0}(\alpha)\big) = 1, \quad \gamma(x) = \beta_{1,0}(x)/p = x^3/2,$$

$$\chi_\gamma(t) \equiv (t+1)^6 \bmod 2\mathbb{Z}_p[t], \quad \nu_\gamma(t) = t+1, \quad \delta_{1,0}(x) = 1,$$

$$v_p\big(\gamma(\alpha) - \delta_{1,0}(\alpha)\big) = 1.$$

For $j = 2$, $k = 0$:

$$\beta_{2,0}(x) = \beta_{1,0}(x) - p\delta_{1,0}(x) = x^3 - 2,$$

$$v_p\big(\beta_{2,0}(\alpha)\big) = 2, \quad \gamma(x) = \beta_{2,0}(x)/p^2 = (x^3-2)/4,$$

$$\chi_\gamma(t) \equiv (t^2+t+1)^3 \bmod 2\mathbb{Z}_p[t], \quad \nu_\gamma(t) = t^2+t+1.$$

Now $F_\gamma \nmid F_\alpha$, with $\mathbb{F}_2[\overline{\alpha},\overline{\gamma}] = \mathbb{F}_2[\overline{\gamma}] \supsetneqq \mathbb{F}_2[\overline{\alpha}]$. Replacing $\alpha(x) \leftarrow (x^3-2)/4$ gives $\nu_\alpha(t) = \nu_\gamma(t) = t^2+t+1$ and

$$\begin{aligned}\chi_\alpha(t) &= \chi_\gamma(t) = t^6 + 931t^5 + 2352t^4 + 2499t^3 + 1388t^2 + 399t + 45 \\ &= \nu_\alpha(t)^3 + 2\big((464t^3 + 709t^2 + 73t - 91)\nu_\alpha(t) + 216t + 113\big)\end{aligned}$$

which is of Eisenstein form, so that $\alpha(x)$ certifies Φ.

6. Ideal Factorization and Integral Bases

Proposition 6.1. *Let ξ be a root of Φ and let $K = \mathbb{Q}_p(\xi)$, with $\mathcal{O}_K$ its ring of integers and $\mathfrak{P}$ the unique non-zero prime ideal of $\mathcal{O}_K$. Assume $\alpha(x) \in \mathbb{Q}_p[x]$ and $\alpha(x)$ certifies Φ. Then:*

(i) $\mathcal{O}_K = \mathbb{Z}_p[\alpha(\xi)]$.
(ii) *If $\overline{\chi}_\alpha(t)$ is irreducible in $\mathbb{F}_p[t]$ then $\mathfrak{P} = p\mathcal{O}_K$.*
(iii) *If $\overline{\chi}_\alpha(t) = \overline{\nu}_\alpha(t)^e$ with $e > 1$ and $\overline{\nu}_\alpha(t)$ monic and irreducible in $\mathbb{F}_p[t]$, then*

$$\mathfrak{P} = \nu_\alpha\big(\alpha(\xi)\big)\mathcal{O}_K \quad \text{and} \quad p\mathcal{O}_K = \mathfrak{P}^e.$$

Proposition 6.2. *Let $f(x)$ be an irreducible monic polynomial in $\mathbb{Z}[x]$, let ξ be a root of f, let $K = \mathbb{Q}(\xi)$, and let $\mathcal{O}$ be the ring of integers of K. If $f(x) = \varphi_1(x)\cdots\varphi_m(x)$ is the complete factorization of $f(x)$ into distinct monic irreducible polynomials in $\mathbb{Z}_p[x]$ and if $\alpha_i(x)$ certifies $\varphi_i(x)$ for $i = 1, \ldots, m$, then*

$$p\mathcal{O} = \mathfrak{p}_1^{e_1}\cdots\mathfrak{p}_m^{e_m}$$

is the complete factorization of $p\mathcal{O}$ into prime ideals in $\mathcal{O}$, where

$$\begin{aligned}\mathfrak{p}_i &= p\mathcal{O} + \pi_i\mathcal{O} \\ e_i &= e_{K/\mathbb{Q}}(\mathfrak{p}_i) = \deg\varphi_i/\deg\nu_{\alpha_i} \\ f_i &= f_{K/\mathbb{Q}}(\mathfrak{p}_i) = \deg\nu_{\alpha_i}\end{aligned}$$

for $i = 1, \ldots, m$, *with* χ_{α_i} *and* ν_{α_i} *being computed with respect to* φ_i *and* π_i *being any element of* K *satisfying*

$$\pi_i \equiv \nu_{\alpha_i}\big(\alpha_i(\xi)\big) \bmod p\mathbb{Z}_p[\xi].$$

Proposition 6.3. *Let* f, *etc., be as in Proposition 6.2. For* $i = 1, \ldots, m$ *let* ξ_i *be a root of* φ_i *and let* $\varepsilon_i(x) \in \mathbb{Q}_p[x]$, *satisfying*

$$\varepsilon_i(\xi_j) = \begin{cases} 1 & \text{if } \varphi_i(\xi_j) = 0, \\ 0 & \text{if } \varphi_i(\xi_j) \neq 0 \end{cases}$$

for $j = 1, \ldots, n$. *Then*

$$\mathcal{O}_p = \widehat{\varepsilon}_1(\xi)\mathbb{Z}[\widehat{\alpha}_1(\xi)] + \cdots + \widehat{\varepsilon}_m(\xi)\mathbb{Z}[\widehat{\alpha}_m(\xi)]$$

is a p*-maximal order in* $\mathcal{O}$; *that is to say,* $p \nmid [\mathcal{O} : \mathcal{O}_p]$. *Here we are taking*

$$\widehat{\alpha}_i(x) \in \mathbb{Q}[x],\ \widehat{\alpha}_i(x) \equiv \alpha_i(x) \bmod p^2\mathbb{Z}_p[x],$$
$$\widehat{\varepsilon}_i(x) \in \mathbb{Q}[x],\ \widehat{\varepsilon}_i(x) \equiv \varepsilon_i(x) \bmod p^{d+1}\mathbb{Z}_p[x]$$

with d *a natural number such that* $p^d\alpha_i(x) \in \mathbb{Z}_p[x]$ *for* $i = 1, \ldots, m$.

Appendix A. Computing the p-adic GCD.

Let relatively prime polynomials $\Psi_1(x)$ and $\Psi_2(x)$ in $\mathbb{Z}_p[x]$ be given, such that

$$\Phi(x) \mid \Psi_1(x)\Psi_2(x) \quad \text{and} \quad p^{r_0}\mathbb{Z}_p[x] = \big(\Psi_1(x)\mathbb{Z}_p[x] + \Psi_2(x)\mathbb{Z}_p[x]\big) \cap \mathbb{Z}_p.$$

Define

$$\mathrm{G}_1(x) = \gcd\big(\Phi(x), \Psi_1(x)\big),\ \mathrm{H}_1(x) = \Psi_1(x)/\mathrm{G}_1(x),$$
$$\mathrm{G}_2(x) = \gcd\big(\Phi(x), \Psi_2(x)\big),\ \mathrm{H}_2(x) = \Psi_2(x)/\mathrm{G}_2(x),$$

so that

$$\Phi(x) = \mathrm{G}_1(x)\mathrm{G}_2(x),$$

and let

$$p^{s_1}\mathbb{Z}_p = \big(\mathrm{G}_2(x)\mathbb{Z}_p[x] + \mathrm{H}_1(x)\mathbb{Z}_p[x]\big) \cap \mathbb{Z}_p,$$
$$p^{s_2}\mathbb{Z}_p = \big(\mathrm{G}_1(x)\mathbb{Z}_p[x] + \mathrm{H}_2(x)\mathbb{Z}_p[x]\big) \cap \mathbb{Z}_p.$$

Because $\Psi_1(x) = G_1(x)H_1(x)$ and $\Psi_2(x) = G_2(x)H_2(x)$ we have $s_1 \leq r_0$ and $s_2 \leq r_0$.

For $j = 1, 2$ let S_{Φ,Ψ_j} be the Sylvester matrix of Φ and Ψ_j. It is clear that row-reduction of S_{Φ,Ψ_j} over $\mathbb{Q}_p$ gives the coefficients of $G_j(x)$ in its last non-zero row. It follows (because the rank is invariant) that row-reduction of S_{Φ,Ψ_j} over $\mathbb{Z}_p$ gives the coefficients of $p^{r_j}G_j(x)$ in its last non-zero row, for some $r_j \geq 0$. Since

$$p^{s_j}\mathrm{G}_j(x) \in \Phi(x)\mathbb{Z}_p[x] + \Psi_j(x)\mathbb{Z}_p[x]$$

it follows that $r_j \le s_j$, and since

$$p^{r_j} \in \frac{\Phi(x)}{\mathrm{G}_j(x)}\mathbb{Z}_p[x] + \frac{\Psi_j(x)}{\mathrm{G}_j(x)}\mathbb{Z}_p[x]$$

it follows that $s_j \le r_j$; hence $r_j = s_j$.

If $m > r_0$ then row-reduction of S_{Φ,Ψ_j} over $\mathbb{Z}_p$ performed modulo p^m gives in its last non-zero row the coefficients of $p^{s_j}\Phi_j(x)$, with $\Phi_j(x)$ in $\mathbb{Z}_p[x]$, $\Phi_j(x)$ monic, and

$$\Phi_j(x) \equiv \mathrm{G}_j(x) \pmod{p^{m-s_j}\mathbb{Z}_p[x]}.$$

It follows that

$$\begin{aligned}\Phi_1(x) &\equiv \gcd\big(\Phi(x), \Psi_1(x)\big) \pmod{p^{m-r_0}\mathbb{Z}_p[x]},\\ \Phi_2(x) &\equiv \gcd\big(\Phi(x), \Psi_2(x)\big) \pmod{p^{m-r_0}\mathbb{Z}_p[x]}.\end{aligned}$$

Remark A.1. In the construction of $\Phi_1(x)$ and $\Phi_2(x)$ it is sufficient to have approximations to $\Phi(x)$, $\Psi_1(x)$, and $\Psi_2(x)$ that are correct modulo $p^m\mathbb{Z}_p[x]$.

Appendix B. Hensel Lifting

The well-known technique of Hensel lifting allows a sufficiently accurate approximate p-adic factorization of a polynomial to be refined to any desired degree of precision.

Suppose $f(x)$, $f_1(x)$, $f_2(x)$, ..., $f_m(x)$ are monic polynomials belonging to $\mathbb{Z}_p[x]$ and $a_1(x)$, $a_2(x)$, ..., $a_m(x)$ are polynomials in $\mathbb{Z}_p[x]$ such that

$$\begin{aligned} f(x) &\equiv \prod_{j=1}^{m} f_j(x) \pmod{p^e\mathbb{Z}_p[x]},\\ p^d &\equiv \sum_{j=1}^{m} a_j(x)\prod_{i\ne j} f_i(x) \pmod{p^{d+1}\mathbb{Z}_p[x]},\end{aligned}$$

with $d \ge 0$ and $e \ge 2d+1$. Taking

$$u(x) = p^{-e}\Big(f(x) - \prod_{j=1}^{m} f_j(x)\Big)$$

and defining

$$\begin{aligned} g_j(x) &= u(x)a_j(x) \bmod f_j(x),\\ \widehat{f}_j(x) &= f_j(x) + p^{e-d}g_j(x),\end{aligned}$$

for $1 \le j \le m$, gives

$$f(x) \equiv \prod_{j=1}^{m} \widehat{f}_j(x) \pmod{p^{e+1}\mathbb{Z}_p[x]},$$
$$p^d \equiv \sum_{j=1}^{m} a_j(x) \prod_{i \neq j} \widehat{f}_i(x) \pmod{p^{d+1}\mathbb{Z}_p[x]},$$

with $\widehat{f}_j(x) \equiv f_j(x) \bmod p^{e-d}\mathbb{Z}_p[x]$ for $1 \le j \le m$.

Appendix C. Fast Computation of $\boldsymbol{\nu_\gamma}$

Let $\gamma(x) \in \mathcal{O}_\Phi$ and let p^d be the reduced discriminant of Φ. For $0 \le k \le n$ let

$$a_{k,1}x^{n-1} + a_{k,2}x^{n-2} + \cdots + a_{k,n} = \gamma(x)^k \bmod \Phi(x) \in p^{-d}\mathbb{Z}_p[x].$$

Define

$$G = \begin{pmatrix} a_{n,1} & a_{n,2} & \cdots & a_{n,n-1} & a_{n,n} \\ a_{n-1,1} & a_{n-1,2} & \cdots & a_{n-1,n-1} & a_{n-1,n} \\ \vdots & \vdots & & \vdots & \vdots \\ a_{1,1} & a_{1,2} & \cdots & a_{1,n-1} & a_{1,n} \\ a_{0,1} & a_{0,2} & \cdots & a_{0,n-1} & a_{0,n} \end{pmatrix}$$

and let

$$A = \begin{pmatrix} p^d G & I \\ p^{d+1} I & 0 \\ 0 & pI \end{pmatrix}.$$

Row-reduction of A over $\mathbb{Z}_p$ yields its p-adic Hermite normal form

$$\mathrm{HNF}_p(A) = \begin{pmatrix} B & * \\ 0 & C \\ 0 & 0 \end{pmatrix}$$

with

$$B = \begin{pmatrix} * & * & \cdots & * & * \\ & * & \cdots & * & * \\ & & \ddots & \vdots & \vdots \\ & 0 & & * & * \\ & & & & * \end{pmatrix}, \quad C = \begin{pmatrix} c_{n,0} & c_{n,1} & \cdots & c_{n,n-1} & c_{n,n} \\ & c_{n-1,1} & \cdots & c_{n-1,n-1} & c_{n-1,n} \\ & & \ddots & \vdots & \vdots \\ & 0 & & c_{1,n-1} & c_{1,n} \\ & & & & c_{0,n} \end{pmatrix}.$$

For $0 \le k \le n$ let

$$h_k(t) = c_{k,n-k}t^k + c_{k,n-k+1}t^{k-1} + \cdots + c_{k,n}$$

and define

$$\begin{aligned} H &= p\mathbb{Z}_p[x] + p\mathbb{Z}_p[\gamma(x)] + \Phi(x)\mathbb{Q}_p[x], \\ L &= \{ h(t) \in \mathbb{Z}_p[t] \mid h(\gamma(x)) \in H \}, \\ J &= h_0(t)\mathbb{Z}_p[t] + h_1(t)\mathbb{Z}_p[t] + \cdots + h_n(t)\mathbb{Z}_p[t], \\ P &= \{ h(t) \in \mathbb{Z}_p[t] \mid v_p^*(h(\gamma)) > 0 \}. \end{aligned}$$

Observe the following.

1. $L = h_0(t)\mathbb{Z}_p + h_1(t)\mathbb{Z}_p + \cdots + h_n(t)\mathbb{Z}_p + \chi_\gamma(t)\mathbb{Z}_p[t]$.
2. $p\mathbb{Z}_p[t] \subseteq L$.
3. $\chi_\gamma(t) - h_n(t) \in h_0(t)\mathbb{Z}_p + h_1(t)\mathbb{Z}_p + \cdots + h_{n-1}(t)\mathbb{Z}_p$.
4. $L \subseteq J \subseteq P$.
5. J is an ideal in $\mathbb{Z}_p[t]$ and $\chi_\gamma(t) \in J$.
6. There exists a monic polynomial $\lambda(t) \in \mathbb{Z}_p[t]$ such that
$$J = \lambda(t)\mathbb{Z}_p[t] + p\mathbb{Z}_p[t].$$
7. $\overline{\lambda}(t) = \gcd(\overline{h}_0(t), \ldots, \overline{h}_n(t))$.
8. P is an ideal in $\mathbb{Z}_p[t]$ and $p\mathbb{Z}_p[t] \subseteq P$.
9. There exists a monic polynomial $\mu(t) \in \mathbb{Z}_p[t]$ such that
$$P = \mu(t)\mathbb{Z}_p[t] + p\mathbb{Z}_p[t].$$
10. The polynomial $\mu(t)$ is congruent modulo p to the product of the distinct irreducible factors of $\chi_\gamma(t)$ modulo p. In other words, $\overline{\mu}(t)$ is the squarefree part of $\overline{\chi}_\gamma(t)$ in $\mathbb{F}_p[t]$.
11. $\overline{\mu}(t) \mid \overline{\lambda}(t)$, since $J \subseteq P$.
12. $p^{d+1}\mathcal{O}_\Phi \subseteq p\mathbb{Z}_p[x] + \Phi(x)\mathbb{Q}_p[x] \subseteq H$.
13. $$\begin{aligned} v_p^*(\mu(\gamma)) \geq 1/n &\implies v_p^*(\mu(\gamma)^{n(d+1)}) \geq d+1 \\ &\implies \mu(\gamma(x))^{n(d+1)} \in p^{d+1}\mathcal{O}_\Phi \\ &\implies \mu(\gamma(x))^{n(d+1)} \in H \\ &\implies \mu(t)^{n(d+1)} \in L \\ &\implies \mu(t)^{n(d+1)} \in J. \end{aligned}$$
    Therefore $\overline{\lambda}(t) \mid \overline{\mu}(t)^{n(d+1)}$.

It follows that the distinct irreducible factors of $\overline{\mu}(t)$ and $\overline{\lambda}(t)$ in $\mathbb{F}_p[t]$ are the same, and therefore that the distinct irreducible factors of $\overline{\lambda}(t)$ and $\overline{\chi}_\gamma(t)$ in $\mathbb{F}_p[t]$ are the same. If $\lambda(t)$ is a power of a single irreducible polynomial modulo p then that irreducible polynomial is $\nu_\gamma(t)$, modulo p; otherwise γ fails the Hensel test.

Appendix D. Experimental Results

The new algorithm is included in the forthcoming Pari/GP 2.2.0. Tests were run to compare the new version with Pari/GP 2.0.16, Kant V4/Kash 2.2, and Magma 2.7. The tests were run on a Pentium MMX 200MHz with 80Mo of RAM. Computations running more than one hour were interrupted. (Polynomial f_{30} produced an error with Magma.) Execution times are expressed in seconds.

POLY-NOMIAL	LOCAL DISC	REDUCED DISC	GP 2.2.0	GP 2.0.16	KASH 2.2	MAGMA 2.7
f_1	2^{15}	2^4	0.12	0.11	0.09	0.53
f_2	2^{10}	2^2	0.05	0.06	0.06	0.57
f_3	3^9	3	0.04	0.04	0.05	0.35
f_4	3^6	3^2	0.09	0.11	0.06	1.78
f_5	2^{10}	2	0.02	0.02	0.02	1.20
f_6	2^{15}	2^6	0.06	0.05	0.06	2.22
f_7	2^{15}	2^4	0.14	0.16	0.12	0.50
f_8	5^4	5^2	0.09	0.11	0.10	0.96
f_9	2^{14}	2^4	0.07	0.13	0.16	0.45
f_{10}	1289^2	1289^2	0.15	0.17	0.10	2.59
f_{11}	2^{22}	2^4	0.08	0.11	0.11	2.55
f_{12}	3^{20}	3^2	0.07	0.08	0.05	0.94
f_{13}	11^3	11^2	0.16	0.17	0.13	1.45
f_{14}	17^2	17^2	0.11	0.13	0.09	1.69
f_{15}	2^{32}	2^3	0.10	0.13	0.10	0.40
f_{16}	2^{12}	2^2	0.10	0.13	0.12	0.90
f_{17}	2^{16}	2^3	0.18	0.21	0.19	3.08
f_{18}	7^{14}	7	0.10	0.10	0.11	0.51
f_{19}	71^2	71^2	0.26	0.30	0.20	3.77
f_{20}	3^{15}	3	0.34	0.43	0.21	1.70
f_{21}	5^{20}	5^2	0.08	0.09	0.11	0.79
f_{22}	3^{15}	3	0.14	0.16	0.11	2.09
f_{23}	3^{15}	3	0.39	0.47	0.28	3.27
f_{24}	2^{72}	2^{13}	0.27	0.40	0.53	4.19
f_{25}	47^{20}	47^2	1.50	1.76	0.81	16.22
f_{26}	61^{98}	61^{16}	1.63	54.47	18.30	7.05
f_{27}	2^{92}	2^9	1.42	421.00	710.00	7.10
f_{28}	3^{166}	3^{20}	1.97	73.00	175.00	> 1 hr
f_{29}	3^{82}	3^8	1.37	16.64	7.75	15.01
f_{30}	2^{284}	2^9	7.16	> 1 hr	1960.00	(error)
f_{31}	2^{544}	2^{28}	45.20	> 1 hr	> 1 hr	22.60
f_{32}	2^{240}	2^{18}	13.60	> 1 hr	235.00	370.00

Examples from Ford & Letard [4]

$$
\begin{aligned}
f_1 &= x^9 - 2x^4 - 10x^3 + x - 2\\
f_2 &= x^9 - 2x^5 + 17x^3 + 4\\
f_3 &= x^9 - 2x^3 - 10\\
f_4 &= x^{10} + 7x^9 - 2x^8 - 2x^7 - 3x^5 + x^4 + 1\\
f_5 &= x^{10} - 4x^9 - 8x^5 + 5x^4 + 1\\
f_6 &= x^{10} - 2x^9 - 15\\
f_7 &= x^{11} + x^8 - 2x^2 + 4\\
f_8 &= x^{11} - x^6 - 2x^3 - 12x^2 - 6\\
f_9 &= x^{11} - x^{10} - x^4 - 4\\
f_{10} &= x^{12} - 3x^9 + 4x^8 - x^6 - x^2 + 10\\
f_{11} &= x^{12} + 4x^{11} + 5x^{10} + 6x^6 - 3x^4 + 12\\
f_{12} &= x^{12} + x^9 - 9x^7 - 2x^6 - 9x^5 - 6\\
f_{13} &= x^{13} + 6x^{10} - 10x^5 + 9x^2 - 2\\
f_{14} &= x^{13} + x^{10} + x^9 - 4x^8 - x^4 + x^2 - 1\\
f_{15} &= x^{13} + x^{11} - 8\\
f_{16} &= x^{14} - x^{12} - x^7 + 10x^5 - 4\\
f_{17} &= x^{14} + 2x^8 + 6x - 1\\
f_{18} &= x^{14} - 8x^7 + 418\\
f_{19} &= x^{15} + 4x^{11} + 12x^{10} + x^3 - 4\\
f_{20} &= x^{15} + 9x^5 + 1\\
f_{21} &= x^{15} - 13x^5 - 2\\
f_{22} &= x^{15} - 30x^{13} + 360x^{11} - 2200x^9 + 7200x^7 - 12096x^5 + 8960x^3 - 120x\\
&\quad - 249\\
f_{23} &= x^{15} - 30x^{13} + 360x^{11} - 2200x^9 + 7200x^7 - 12096x^5 + 8960x^3 - 120x\\
&\quad - 257\\
f_{24} &= x^{16} + 132x^{14} + 6868x^{12} + 179570x^{10} + 2494972x^8\\
&\quad + 18111820x^6 + 65000173x^4 + 102234000x^2 + 46240000\\
f_{25} &= x^{21} - 42x^{19} + 756x^{17} - 7616x^{15} + 47040x^{13} - 183456x^{11}\\
&\quad + 448448x^9 - 658944x^7 + 532224x^5 - 197120x^3 + 21504x - 1691
\end{aligned}
$$

Examples for which PARI 2.0.16 performs poorly

$$\begin{aligned}
f_{26} = x^{12} &- 181170x^{11} \\
&+ 13676070375x^{10} \\
&- 564635734535475x^{9} \\
&+ 14120575648656756795x^{8} \\
&- 224213861531349946866060x^{7} \\
&+ 2299324928127100837257833640x^{6} \\
&- 15120132032108410885407953780505x^{5} \\
&+ 61607021939453175254804920116967515x^{4} \\
&- 144536083330213614666317706146365094565x^{3} \\
&+ 170426077617455313511361437803852538934904x^{2} \\
&- 83139235455474245627641509862888062014092560x \\
&+ 12253655221465755667504199645608996691723374656
\end{aligned}$$

$$\begin{aligned}
f_{27} = x^{16} &- 12x^{14} - 84x^{13} - 196x^{12} + 2856x^{11} + 6328x^{10} \\
&- 42336x^{9} - 64820x^{8} + 352464x^{7} + 298928x^{6} - 1776096x^{5} \\
&- 262416x^{4} + 5458656x^{3} - 1875872x^{2} - 6688416x + 7866576
\end{aligned}$$

$$\begin{aligned}
f_{28} = x^{16} &- 432x^{14} + 68688x^{12} - 4717440x^{10} + 112637304x^{8} \\
&+ 409406400x^{6} + 2774305728x^{4} + 4041156096x^{2} + 11224978704
\end{aligned}$$

$$\begin{aligned}
f_{29} = x^{24} &+ 57x^{22} + 1197x^{20} + 13681x^{18} + 136854x^{16} + 1048044x^{14} \\
&+ 4603892x^{12} + 11460015x^{10} + 16001100x^{8} + 11131014x^{6} \\
&+ 2739339x^{4} - 368793x^{2} - 7569
\end{aligned}$$

$$f_{30} = x^{32} + 16$$

$$\begin{aligned}
f_{31} = x^{32} &+ 160x^{30} + 11216x^{28} + 455360x^{26} + 11928052x^{24} \\
&+ 212540000x^{22} + 2645190320x^{20} + 23223642560x^{18} \\
&+ 143402547926x^{16} + 613283590880x^{14} + 1764753386480x^{12} \\
&+ 3275906117440x^{10} + 3788371498452x^{8} + 2940754348320x^{6} \\
&+ 1769278869776x^{4} + 73445288000x^{2} + 87782430961
\end{aligned}$$

$$\begin{aligned}
f_{32} = x^{40} &- 2x^{39} + 3x^{38} - 22x^{37} + 26x^{36} - 2x^{35} + 185x^{34} - 120x^{33} \\
&- 270x^{32} - 1232x^{31} + 689x^{30} + 1972x^{29} + 4298x^{28} - 2588x^{27} \\
&- 6040x^{26} - 5558x^{25} + 19939x^{24} + 21850x^{23} + 12277x^{22} \\
&- 20890x^{21} + 4071x^{20} + 28388x^{19} + 35210x^{18} + 10304x^{17} \\
&+ 18728x^{16} + 1408x^{15} - 3352x^{14} - 16288x^{13} + 20512x^{12} \\
&+ 16320x^{11} - 37728x^{10} - 13312x^{9} - 7168x^{8} + 2560x^{7} - 1280x^{6} \\
&- 7680x^{5} + 10496x^{4} + 7168x^{3} + 512x^{2} + 2048x + 1024
\end{aligned}$$

Example f_{26} is from [1]; example f_{32} is from [3]. The other examples are due to Karim Belabas, Bill Allombert, and Igor Schein of the PARI development team.

References

See [4] for a list of references earlier than 1994. Some recent related work appears in [8], [5], and [7]. For details of the algorithm used in PARI 2.0.16 see [4] and for KANT V4 see [2]. MAGMA 2.7 is the product of the Computational Algebra Group at the University of Sydney. Its factorization and integral basis algorithms were designed by Bernd Souvignier and implemented by Nicole Sutherland and Geoff Bailey.

[1] A. ASH, R. PINCH, R. TAYLOR, *An* $\widehat{A}_4$ *extension of* $\mathbb{Q}$ *attached to a non-selfdual automorphic form on* GL(3). Math. Annalen **291** (1991), 753–766.

[2] G. BAIER, *Zum Round 4 Algorithmus*, Diplomarbeit, Technische Universität Berlin, 1996, `http://www.math.TU-Berlin.DE/~kant/publications/diplom/baier.ps.gz`.

[3] H. COHEN, Personal communication, 1996.

[4] D. FORD, P. LETARD, *Implementing the Round Four maximal order algorithm.* J. Théor. Nombres Bordeaux **6** (1994) 39–80, `http://almira.math.u-bordeaux.fr:80/jtnb/1994-1/jtnb6-1.html`.

[5] E. HALLOUIN *Calcul de fermeture intégrale en dimension 1 et factorisation.* Thèse, Université de Poitiers, 1998.

[6] W. NARKIEWICZ, *Elementary and Analytic Theory of Algebraic Numbers* (second edition). Springer-Verlag, Berlin, 1990.

[7] S. PAULI, *Factoring Polynomials over Local Fields.* Journal of Symbolic Computation, accepted 2001.

[8] X.-R. ROBLOT, *Algorithmes de factorisation dans les extensions relatives et applications de la conjecture de Stark à la construction des corps de classes de rayon.* Thèse, Université Bordeaux I, 1997, `http://www.desargues.univ-lyon1.fr/home/roblot/papers.html#1`.

[9] E. WEISS, *Algebraic number theory.* McGraw-Hill, 1963.

David FORD, Sebastian PAULI
Centre Interuniversitaire en Calcul Mathématique Algébrique
Department of Computer Science
Concordia University
Montréal, Québec
E-mail : `ford@cs.concordia.ca, pauli@mathstat.concordia.ca`

Xavier-François ROBLOT
Institut Girard Desargues
Université Claude Bernard (Lyon I)
43, boulevard du 11 Novembre 1918
69622 VILLEURBANNE cedex, France
E-mail : `roblot@desargues.univ-lyon1.fr`