Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

DISTINGUISHED DEFINING POLYNOMIALS FOR EXTENSIONS OF p-ADIC FIELDS

JORDI GUÀRDIA I RÚBIES, JOHN W. JONES, KEVIN KEATING, SEBASTIAN PAULI, DAVID P. ROBERTS, AND DAVID ROE

Abstract. We give an algorithm for choosing a distinguished defining polynomial for a p-adic field extension. This algorithm formed an important ingredient in the recent expansion of the database of p-adic fields within the L-functions and modular forms database.

1. Introduction

It follows from Krasner's Lemma that a p-adic field has only finitely many extensions of a given degree. It is thus natural to seek a list of polynomials $\varphi(x)$ such that each extension is generated by exactly one $\varphi(x)$. Once the list has been created, looking up an extension defined by some other polynomial $\psi(x)$ requires an algorithm which matches $\psi(x)$ to one of the chosen $\varphi(x)$ defining an isomorphic extension. Such an algorithm, `polredpadic` (Algorithm 6.15), is the central result of this paper. Note that this algorithm also enables the creation of the list of $\varphi(x)$ in the first place by taking the list with repetition from [GJK+26, §2.4, 3.3], running `polredpadic` on all of them, and then removing duplicates.

The LMFDB [LMF25] is a massive online database of number-theoretic objects of many different types. It contains a database of p-adic fields, initially created by Jones and Roberts [JR06] and recently extended by the present authors [GJK+26]. The `polredpadic` algorithm played a central role in enabling the enumeration of the 890,111 degree 16 and the 314,543 degree 20 extensions of $\mathbb{Q}_2$. While the sheer number of fields prohibits practical enumeration in some degrees (there are over 114 billion degree 32 extensions of $\mathbb{Q}_2$), the process is now completely automated and straightforward to carry out for any particular degree. Moreover, the same approach works to enumerate fields with more restricted invariants, such as a specific discriminant or family [GJK+26, §1.2].

Our basic approach rests on work of Krasner [Kra37] as modernized by Monge [Mon14]. In the case where $L/\mathbb{Q}_p$ is totally ramified, this theory gives a collection of *near-canonical* Eisenstein polynomials, each of which defines L. We generalize this approach to the case that the inertia degree is larger than 1, replacing Eisenstein polynomials with Øystein polynomials (see Section 3), and give a process to pick a *distinguished polynomial* among them (see Condition 6.14).

The name `polredpadic` is inspired by the PARI-GP [Pg25] function `polredabs` which computes a (pseudo) canonical defining polynomial of a number field and enables searching the LMFDB's number field database given an arbitrary irreducible polynomial over $\mathbb{Q}$.

Date: June 5, 2026.

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

The paper is structured as follows. In Section 2 we set up notation and describe how we select polynomials defining unramified extensions. In Section 3 we define ν-Øystein polynomials for an unramified polynomial $\nu(x)$, give Algorithm 3.5 for finding an Øystein polynomial generating an arbitrary extension, and connect Øystein polynomials to Eisenstein polynomials over the maximal unramified subextension. In Section 4 we recall the theory of ramification polygons and generalize them from their original context of Eisenstein polynomials to Øystein polynomials. In Section 5 we recall the theory of residual polynomials, which are attached to the segments of the ramification polygon and provide an invariant allowing for the division of families into subfamilies (Definition 5.4). We also define distinguished residual polynomials, which provide one part of the recipe for selecting a distinguished polynomial for $L/\mathbb{Q}_p$.

Section 6 forms the core of the paper, describing how to reduce an Øystein polynomial to a set of near-canonical options and then how to pick a distinguished polynomial from among them. We first give the process for Eisenstein polynomials from [Mon14], with modifications to ensure compatibility with the generic polynomial of the family [GJK+26, §3.3]. As part of this process, we recall additive residual polynomials and generalize them to Øystein polynomials. The main theorem underpinning the reduction process is Theorem 6.8, which describes how the minimal polynomial of a root α of a ν-Øystein polynomial ψ changes when making a substitution of the form $\alpha \mapsto \alpha + \gamma\nu(\alpha)^m$. This theorem enables setting many p-adic digits of the coefficients of ψ to 0 without changing the extension (see Corollary 6.10), and also provides a reduction algorithm for the remaining coefficients (Algorithm 6.12). Section 6 ends by defining a total order on Øystein polynomials, allowing for the selection of a distinguished defining polynomial. We close with a complexity analysis of our algorithms in Section 7.

Our implementation in Magma [BCP97] of the algorithms in this paper is available on GitHub at `https://github.com/roed314/padic_db` and data is available on the LMFDB at `https://www.lmfdb.org/padicField/`.

We thank the American Institute of Mathematics for supporting this work through an AIM SQuaRE and the three anonymous referees whose comments have improved the quality of the paper. Roe was supported by SFI-MPS-SSRFA-00005427.

2. Setup and notation

Let K be a finite extension of $\mathbb{Q}_p$ with inertia degree f_K, ramification index e_K, and degree $n_K = f_K e_K$. Let π_K be a uniformizer for K and let $v_K : K \to \mathbb{Z} \cup \{\infty\}$ be the valuation on K normalized so that $v_K(\pi_K) = 1$. Let $\mathcal{O}_K = \{\alpha \in K : v_K(\alpha) \geq 0\}$ be the ring of integers of K and let $(\pi_K) = \{\alpha \in K : v_K(\alpha) > 0\}$ be the maximal ideal of $\mathcal{O}_K$. For $\alpha, \beta \in K$, we write $\alpha \sim \beta$ when $v_K(\alpha - \beta) > v_K(\alpha)$.

We denote the residue class field of K by $\kappa = \mathcal{O}_K/(\pi_K)$ and by $q = \#\kappa$ its cardinality. For a generator $\overline{\xi}_K$ of the cyclic group $\kappa^\times$ and $\overline{\gamma} \in \kappa^\times$ we let $\log_{\overline{\xi}_K} \overline{\gamma}$ be the smallest $n \in \mathbb{Z}_{\geq 0}$ with $\overline{\xi}_K^n = \overline{\gamma}$.

Let $\mathcal{R}_K$ be a fixed set of representatives of κ in $\mathcal{O}_K$ with $\{0, 1\} \subseteq \mathcal{R}_K$.

Let $\varphi \in \mathcal{O}_K[x]$ have degree n. We write $\varphi(x) = \sum_{i=0}^n \varphi_i x^i$, and for each coefficient we write $\varphi_i = \sum_{i=0}^\infty \varphi_{i,k}\pi_K^i$, where $\varphi_{i,k} \in \mathcal{R}_K$.

Let K^{sep} be a separable closure of K and let L/K be a finite subextension of K^{sep}/K, with inertia degree f, ramification index $e = \epsilon p^w$ with $p \nmid \epsilon$, and degree $n = ef = \epsilon p^w f$. We denote by L_{ur}/K the maximal unramified subextension of

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

L/K, by L_0/K its maximal tame subextension and by λ the residue class field of L. Then $[L_{\mathrm{ur}} : K] = [\lambda : \kappa] = f$, $[L_0 : L_{\mathrm{ur}}] = \epsilon$, and we get the standard tower of subextensions

$$K \overset{f}{\subseteq} L_{\mathrm{ur}} \overset{\epsilon}{\subseteq} L_0 \overset{p^w}{\subseteq} L. \tag{2.1}$$

Let ψ be a defining polynomial for L/K and let β be a root of ψ such that $L = K(\beta)$. For $\gamma \in K[x]$ we denote the characteristic polynomial of $\gamma(\beta)$ by $\chi_{L/K}(\gamma(\beta)) = \chi_\psi(\gamma) = \mathrm{Res}_t\,(\psi(t), x - \gamma(t))$.

For $\rho(x) = \sum_{i=0}^{n} \rho_i x^i \in \mathcal{O}_L[x]$ we call the lower convex hull $\mathcal{N}$ of

$$\{(-i, v_L(\rho_i)) : 0 \le i \le n\}$$

the *Newton polygon* of ρ. Its slopes yield the multiset of valuations of the roots of ρ. We denote the π_L-content of ρ by

$$\mathrm{cont}_{\pi_L}(\rho) = \pi_L^{\min_{0\le i\le n} v_L(\rho_i)}.$$

Unramified extensions. The standard choice for defining these extensions are Conway polynomials, which were introduced by Parker [HEO05, Section 2.8.3] and are the default in Magma [BCP97], SageMath [S+26] and other systems. Unfortunately Conway polynomials have not been computed for all primes and extension degrees considered in the p-adic field database of the LMFDB. See [Lüb23, Section 7] for the Conway polynomials known in 2023.

For the database, when no Conway polynomial is known we follow the procedure from [JR06] which is in the same spirit, but with fewer restrictions. We pick the polynomial whose roots over $\mathbb{F}_p$ are primitive of multiplicative order $p^f - 1$ which is smallest according to the lexicographic ordering used in the definition of Conway polynomials: for $\nu(x) = x^n + \sum_{i=0}^{n-1}(-1)^{n-i}\nu_i x^i \in \mathbb{Z}[x]$ and $\mu(x) = x^n + \sum_{i=0}^{n-1}(-1)^{n-i}\mu_i x^i \in \mathbb{Z}[x]$ with $0 \le \nu_i, \mu_i < p$ we define $\overline{\nu} < \overline{\mu}$ when there exists k with $\nu_i = \mu_i$ for all $i > k$ and $\nu_k < \mu_k$. The code allows users to make a different choice if desired.

In our complexity analysis in Section 7, we assume that a table that includes all such polynomials needed in our algorithms has been precomputed, since the computation of these polynomials is not a focus of this paper.

LMFDB. Following the choice made in Magma and Sage, in the LMFDB we define unramified extensions using polynomials with coefficients in $\{0, 1, \ldots, p-1\}$ that are congruent to the coefficients of the polynomials described above. By construction a root $\overline{\xi}$ over $\mathbb{F}_p$ of such a polynomial $\overline{\nu}$ is a primitive element and is used as the base of discrete logarithms. For a p-adic field K with residue field $\mathbb{F}_{p^{f_K}}$ we choose the set of representatives

$$\mathcal{R}_K = \{c_{f_K-1}\xi^{f_K-1} + \cdots + c_1\xi + c_0 : c_i \in \{0, 1, \ldots, p-1\}\}.$$

In particular, if $f_K = 1$ we get $\mathcal{R}_K = \{0, 1, \ldots, p-1\}$.

3. Øystein polynomials

Every totally ramified extension L/K of degree e is generated by a root of an Eisenstein polynomial $\varphi(x) = x^e + \sum_{i=0}^{e-1}\varphi_i x^i \in \mathcal{O}_K[x]$, where $v_K(\varphi_i) \ge 1$ for $1 \le i \le e-1$ and $v_K(\varphi_0) = 1$. In the following we consider a generalization of Eisenstein polynomials that can be used to define any finite extension of a local field.

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

Definition 3.1. Let $\nu(x) \in \mathcal{O}_K[x]$ be monic and irreducible modulo π_K. A monic polynomial $\varphi \in \mathcal{O}_K[x]$ is ν-Øystein when

$$\varphi(x) = \nu(x)^e + \sum_{i=1}^{e-1} \varphi_i^*(x)\nu(x)^i + \varphi_0^*(x) \tag{3.2}$$

for some $e \in \mathbb{Z}_{>0}$, where $\pi_K \mid \varphi_i^*(x)$ and $\deg \varphi_i^* < \deg \nu$ for $0 \le i \le e-1$, and $\operatorname{cont}_{\pi_K}(\varphi_0^*) = \pi_K$. We call (3.2) the ν-expansion of φ.

We chose the name Øystein to honor Øystein Ore and to avoid confusion with Ore polynomials which are elements of Ore extensions in ring theory. Øystein polynomials are called *regular* polynomials in [Ore28] and polynomials in *Eisenstein form* in [FPR02].

Let $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ be a ν-Øystein polynomial with $\overline{\nu}(x) \ne x$ and set $f = \deg \nu$. Let $\alpha \in K^{\mathrm{sep}}$ be a root of $\varphi(x)$ and set $L = K(\alpha)$. Because $\overline{\nu}$ is irreducible we have $f_{L/K} \ge f$ and because $\overline{\nu}(\overline{\alpha}) = 0$ we have $v_L(\alpha) = 0$. The polynomial $\varphi^*(y) = y^e + \sum_{i=0}^{e-1} \varphi_i^*(\alpha) y^i \in \mathcal{O}_L[y]$ has the root $\nu(\alpha)$. Since $v_K(\varphi_0^*(\alpha)) = 1$ and $v_K(\varphi_i^*(\alpha)) \ge 1$ the lower convex hull of

$$\left\{(-e, 0), (-e+1, v_K(\varphi_{e-1}^*(\alpha))), \dots, (0, v_K(\varphi_0^*(\alpha)))\right\}$$

consists of a single segment of slope $\frac{1}{e}$. Thus, for the root $\nu(\alpha)$ of φ^* we have $v_K(\nu(\alpha)) = \frac{1}{e}$ which yields a lower bound for the ramification index of L/K, namely $e_{L/K} \ge e$. Now, since $e_{L/K} f_{L/K} \le ef = \deg \varphi$ we have $e_{L/K} = e$ and $f_{L/K} = f$. Furthermore, $\nu(\alpha)$ is a uniformizer of L, $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, and $v_K(\operatorname{disc}(L/K)) = v_K(\operatorname{disc}(\varphi))$. Over the unramified subextension $L_{\mathrm{ur}} = K[x]/(\nu)$ of L/K the polynomial φ factors into $f = \deg \nu$ polynomials of degree e.

Every finite extension of a local field can be generated by an Øystein polynomial:

Lemma 3.3. *Let L/K be finite with inertia degree f and ramification index e and let π_L a uniformizer of L. Let $\nu \in \mathcal{O}_K[x]$ be monic of degree f such that $\overline{\nu} \in \kappa[x]$ is irreducible and let $\alpha \in \mathcal{O}_L$ be a root of $\nu(x) - \pi_L$. Then the minimal polynomial of α over K is a ν-Øystein polynomial.*

Proof. We have $\nu(\alpha) = \pi_L$, and $\kappa(\overline{\alpha})$ is the residue class field of L/K by construction. Hence the result follows from [FPR02, Proposition 4.5]. □

The constant coefficient.

Lemma 3.4. *Let $L/L_{\mathrm{ur}}/K$ as in (2.1) and let $\alpha \in L$ be a root of $\nu(x) - \pi_L$. Write $\psi(x) = x^e + \sum_{i=0}^{e-1} \psi_i x^i \in L_{\mathrm{ur}}[x]$ for the minimal polynomial of π_L over L_{ur} and $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i$ for the minimal polynomial of α over K. Then $\varphi_0^*(\alpha) \sim \psi_0$.*

Proof. By Lemma 3.3 φ is a ν-Øystein polynomial. Since $\nu(\alpha) = \pi_L$ and $\psi(\pi_L) = 0$ we have $-\psi_0 = \nu(\alpha)^e + \sum_{i=1}^{e-1} \psi_i \nu(\alpha)^i \sim \nu(\alpha)^e$. Also $-\varphi_0^*(\alpha) = \nu(\alpha)^e + \sum_{i=1}^{e-1} \varphi_i^*(\alpha)\nu(\alpha)^i \sim \nu(\alpha)^e$. □

The OM-algorithm and Øystein polynomials. The OM-algorithm[1] [GMN12] determines the essential p-local invariants of a square-free integral polynomial, facilitating both a number of important computations for global fields [GMN13] and the

[1]Other similar algorithms, such as Round 4 [FPR02], can also be used.

p-adic factorization of the polynomial [GNP12]. The 'O' in OM-algorithm stands for Okutsu and Ore, and the 'M' for Mac Lane and Montes.

It is well known that Øystein polynomials are irreducible. In addition, they have the property that their Okutsu invariants are found after only one step of the OM-algorithm. Ore [Ore28] asserts that every finite extension of $\mathbb{Q}_p$ admits a *regular* defining polynomial, which we call an Øystein polynomial. Unfortunately, Ore's result is only theoretical, and does not provide a practical method to find a regular defining polynomial for a given extension. Lemma 3.3 gives this construction.

With the OM-Algorithm and Lemma 3.3 we find a defining Øystein polynomial $\varphi \in \mathcal{O}_K[x]$ of a finite extension L/K. We assume that for each $f \in \mathbb{Z}_{>0}$ we can look up a monic polynomial $\nu(x) \in \mathcal{O}_K[x]$ of degree f such that $\overline{\nu}$ is irreducible over κ.

Algorithm 3.5 (`Øystein`)**.**

Input: $\psi \in \mathcal{O}_K[x]$ irreducible
Output: $\nu \in \mathcal{O}_K[x]$ monic irreducible over κ and
$\varphi \in \mathcal{O}_K[x]$ ν-Øystein such that $K[x]/(\varphi) \cong K[x]/(\psi)$

Denote by β a root of ψ and write $L = K(\beta)$
(1) with the OM-algorithm find:
- the ramification index e of L/K and $\Pi \in K[x]$ with $v_K(\Pi(\beta)) = 1/e$
- the inertia degree f of L/K

(2) let $\nu \in \mathcal{O}_K[x]$ be monic of degree f with $\overline{\nu} \in \kappa[z]$ irreducible and let $\overline{\gamma} \in \lambda$ be a root of ν
(3) use the output of the OM-algorithm to find $\Gamma \in K[x]$ with $\overline{\Gamma(\beta)} = \overline{\gamma}$
(4) $\alpha \leftarrow \Gamma(\beta) - \frac{\nu(\Gamma(\beta)) - \Pi(\beta)}{\nu'(\Gamma(\beta))}$
(5) return ν and the characteristic polynomial $\varphi = \chi_{K(\beta)/K}(\alpha)$ of α

After step (3) we have $v_K\left(\nu(\Gamma(\beta)) - \Pi(\beta)\right) \geq \frac{1}{e}$. One iteration of Newton lifting in step (4) is sufficient to obtain $\alpha \in K(\beta)$ with $v_K\left(\nu(\alpha) - \Pi(\beta)\right) > \frac{1}{e}$. Hence $v_L(\nu(\alpha)) = 1$, so $\chi_\psi(\alpha)$ is Øystein.

In the LMFDB we choose the polynomials in step (2) to be Conway polynomials or the polynomials from [JR06] described in Section 2.

Given a ν-Øystein polynomial $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ we can find an Eisenstein polynomial ψ over $L_{\mathrm{ur}} = K[x]/(\nu)$ such that $L_{\mathrm{ur}}[x]/(\psi) = K[x]/(\varphi)$ as follows. Because the polynomial $\nu(x)$ splits into linear factors over λ, say $\overline{\nu}(x) = (z - \overline{\xi}_1)\cdots(z - \overline{\xi}_f)$, we have

$$\varphi(x) \equiv \nu(x)^e \equiv (x - \xi_1)^e \cdots (x - \xi_f)^e \pmod{\pi_K}$$

where $\xi_i \in L_{\mathrm{ur}}$ is a lifting of $\overline{\xi}_i$. So Hensel lifting yields $f = \deg \nu$ coprime factors of φ of degree e over L_{ur}. Let $\psi^* \in \mathcal{O}_{L_{\mathrm{ur}}}[x]$ be the factor of φ that corresponds to the factor $(x - \xi_1)^e$ of ν^e. Then $\psi(x) = \psi^*(x + \xi_1)$ is Eisenstein and $L_{\mathrm{ur}}[x]/(\psi) = K[x]/(\varphi)$.

4. Ramification polygons

Ramification polygons of Eisenstein polynomials were introduced by Krasner [Kra37], and can be found with slightly varying definitions in later work [Sch03, GP12, Mon14, PS17]. They are a formulation of the Herbrand invariant of an

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

extension of local fields; see [GJK+26, Section 2] for various perspectives on these. Here we generalize the notion of ramification polygons to Øystein polynomials.

Definition 4.1. Let $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ be ν-Øystein and let $\alpha \in K^{\text{sep}}$ be one of its roots. We say that

$$\rho(x) = \frac{\varphi\left(\nu(\alpha)x + \alpha\right)}{\nu(\alpha)^e}$$

is the *ν-ramification polynomial* of φ. We say that the Newton polygon $\mathcal{N}(\varphi)$ of ρ is the *ramification polygon* of φ; note that $\mathcal{N}(\varphi)$ does not depend on ν.

If we write $\rho(x) = \sum_{i=0}^{n} \rho_i x^i$ we have

$$\rho_i = \nu(\alpha)^{i-e} \sum_{j=i}^{n} \binom{j}{i} \varphi_j \alpha^{j-i}. \tag{4.2}$$

Denote the roots of φ by $\alpha = \alpha_1, \dots, \alpha_n \in \overline{K}$. Then the roots of ρ are $\frac{\alpha_i - \alpha}{\nu(\alpha)}$ for $1 \le i \le n$ and thus the slopes of the ramification polygon $\mathcal{N}(\varphi)$ determine the valuations of the differences of the roots of φ.

Lemma 4.3. *Let $\varphi \in \mathcal{O}_K[x]$ be a ν-Øystein polynomial of degree $n = fe = f\epsilon p^w$ and set $L = K[x]/(\varphi)$. Then the ramification polygon $\mathcal{N}(\varphi)$ of φ is obtained from the ramification polygon $\mathcal{N}_{L/L_{\text{ur}}}$ of the totally ramified extension L/L_{ur} by adding a segment with endpoints $(-n, n-e)$, $(-e, 0)$.*

Proof. There are $n - e$ roots $\widetilde{\alpha}$ of $\varphi(x)$ such that $\widetilde{\alpha} \not\sim \alpha$; these all give roots of $\rho(x)$ with L-valuation -1. Let $\psi(x)$ be the minimal polynomial over L_{ur} of the uniformizer $\pi_L = \nu(\alpha)$ of L. Then the roots of ψ have the form $\widetilde{\pi}_L = \nu(\widetilde{\alpha})$, where $\widetilde{\alpha}$ is a root of φ such that $\widetilde{\alpha} \sim \alpha$. Since $\nu(x) \in \mathcal{O}_K[x]$ and $\overline{\nu}(x)$ is separable, we have $v_L(\widetilde{\pi}_L - \pi_L) = v_L(\widetilde{\alpha} - \alpha)$. Hence the multisets $\{v_L(\frac{\widetilde{\alpha}-\alpha}{\nu(\alpha)}) : \varphi(\widetilde{\alpha}) = 0,\ \widetilde{\alpha} \sim \alpha\}$ and $\{v_L(\frac{\widetilde{\pi}_L - \pi_L}{\pi_L}) : \psi(\widetilde{\pi}_L) = 0\}$ are equal. The lemma now follows from the relation between the slopes of the Newton polygon of $\rho(x)$ and the valuations of its roots. $\square$

It follows from the lemma that $\mathcal{N}(\varphi)$ is determined by the extension L/K, so we may denote it by $\mathcal{N}_{L/K}$. Using the description of the ramification polygon for the totally ramified case (see [Sch03, Lemma 1] or [PS17, Lemma 3.2]) we obtain the ramification polygon of a general extension L/K of degree $fe = f\epsilon p^w$

$$\begin{aligned} \mathcal{N}_{L/K} = \Big\{ &\big(-ef, (f-1)e\big), (-e, 0), \big(-p^w, 0\big), \big(-p^{w_1}, v_L(\rho_{w_1})\big), \dots \\ &\dots, \big(-p^{w_{u-1}}, v_L(\rho_{w_{u-1}})\big), \big(-1, v_L(\rho_1)\big) \Big\} \end{aligned} \tag{4.4}$$

for some $w = w_0 > w_1 > \cdots > w_{u-1} > w_u = 0$.

We have $v_K(\operatorname{disc}(L/K)) = v_K(\operatorname{disc}(\varphi)) = f \cdot (e + v_L(\rho_1) - 1)$, and each of the segments of $\mathcal{N}$ corresponds to a subextension of L/K (see [Gre10, Algorithmus 4.4] or [Mil17, Section 3.4] for an algorithm).

Hasse-Herbrand function. Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein of degree e and let α be a root of φ. Set $L = K(\alpha)$ and let $\rho(x) = \frac{\varphi(\alpha x + \alpha)}{\alpha^e}$ be the ramification polynomial of φ. Denote the endpoints of the segments with positive slope of the ramification polygon of φ by $(-p^{w_i}, v_L(\rho_{p^{w_i}}))$ where $0 = w_u < \cdots < w_0 = w$. Let $\Phi_{L/K} : [0, \infty) \to [0, \infty)$ be the Hasse-Herbrand function of L/K, which is defined

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

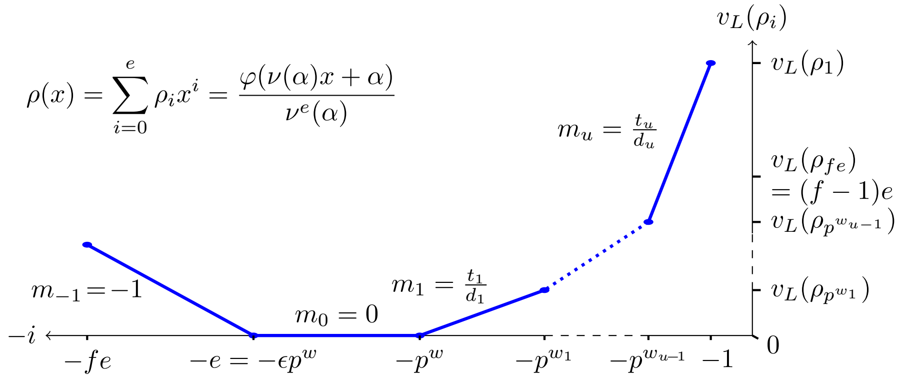

FIGURE 4.1. General form of the ramification polygon of a ν-Øystein polynomial $\varphi = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ of degree $n = f \cdot e = f \cdot \epsilon p^w$. The segment of slope -1 only exists when $f > 1$ and a segment of slope 0 indicates $\epsilon > 1$.

in [Ser79, IV §3] and discussed in [GJK+26, Section 2.2]. Then we have (compare [Mon14, Section 2] and [PS17, Section 3])
(4.5)
$$e\Phi_{L/K}(m) = \min_{0\le i\le u}\{v_L(\rho_{p^{w_i}}) + mp^{w_i}\} = \min_{1\le i\le e}\{v_L(\rho_i) + i\cdot m\} = \mathrm{cont}_{\pi_L}(\rho(\pi_L^m x))$$

for $m \ge 0$. Now suppose, $\varphi \in \mathcal{O}_K[x]$ is ν-Øystein of degree fe, $L_{\mathrm{ur}} = K[x]/(\nu)$, $L = K[x]/(\varphi)$ with ν-ramification polynomial ρ and ramification polygon $\mathcal{N}$. Then $\Phi_{L_{\mathrm{ur}}/K}(x) = x$ and thus $\Phi_{L/K} = \Phi_{L_{\mathrm{ur}}/K} \circ \Phi_{L/L_{\mathrm{ur}}} = \Phi_{L/L_{\mathrm{ur}}}$. Using (4.5) and Lemma 4.3 we get

$$e\Phi_{L/K}(m) = \min_{1\le i\le n}\{v_L(\rho_i) + i\cdot m\} = \mathrm{cont}_{\nu(\alpha)}(\rho(\nu(\alpha)^m x)). \tag{4.6}$$

Because $\Phi_{L/K}$ only depends on the ramification polygon $\mathcal{N}$ of L/K, we can set $\Phi_{\mathcal{N}} = \Phi_{L/K}$.

5. Residual polynomials

Let $\mathcal{N}$ be the Newton polygon of a polynomial $\rho \in \mathcal{O}_L[x]$. To each segment $\mathcal{S}$ of $\mathcal{N}$ we attach a polynomial $\overline{A} \in \lambda[x]$. These polynomials were first introduced as *zugeordnete* (associated) polynomials by Ore [Ore28, MN92] and have been called residual polynomials in more recent work. The residual polynomials of the segments of the Newton polygon of a polynomial yield information about the unramified part of the extensions generated by the factors of the polynomial.

Let $\rho(x) = \sum_{i=0}^{n} \rho_i x^i \in \mathcal{O}_L[x]$ with roots $\beta_1, \ldots, \beta_n$ and denote by $\mathcal{N}$ its Newton polygon. Let $(-i, v_L(\rho_i))$ and $(-j, v_L(\rho_j))$ be the endpoints of a segment of $\mathcal{N}$ of slope $m = \frac{t}{d}$ and let $\beta \in \overline{L}$ be a root of ρ with $v_L(\beta) = m$. We divide the polynomial $\rho(\beta x)$ whose roots are $\frac{\beta_1}{\beta}, \ldots, \frac{\beta_n}{\beta}$ by its content $\pi_L^{v_L(\rho_j)}\beta^j$ and get

$$\frac{\rho(\beta x)}{\pi_L^{v_L(\rho_j)}\beta^j} = \sum_{l=0}^{n} \frac{\rho_l \beta^l x^l}{\pi_L^{v_L(\rho_j)}\beta^j} \equiv \sum_{l=j}^{i} \frac{\rho_l \beta^{l-j}}{\pi_L^{v_L(\rho_j)}} x^l \equiv \sum_{k=0}^{(i-j)/d} \frac{\rho_{j+kd}\beta^{kd}}{\pi_L^{v_L(\rho_j)}} x^{j+kd} \bmod \pi_L.$$

Let $\theta = \frac{\beta^d}{\pi_L^t}$. Dividing the above by x^j, replacing β^d with $\theta\pi_L^t$ and replacing $\theta \cdot x^d$ with z yields the residual polynomial of the segment of slope m of $\mathcal{N}$:

Definition 5.1. Let $\rho(x) = \sum_{i=0}^n \rho_i x^i \in \mathcal{O}_L[x]$ and suppose the Newton polygon of ρ has a segment $\mathcal{S}$ with endpoints $(-i, v_L(\rho_i))$ and $(-j, v_L(\rho_j))$ of slope $m = \frac{t}{d}$. Then the *residual polynomial* of $\mathcal{S}$ is

$$\overline{A}_m(z) := \sum_{k=0}^{(i-j)/d} \overline{\rho_{j+kd}\pi_L^{kt-v_L(\rho_j)}} z^k \in \lambda[z].$$

Each root of $\overline{A}_m$ has the form $\overline{\theta \cdot \left(\frac{\beta_i}{\beta}\right)^d} = \overline{\left(\frac{\beta_i^d}{\pi_L^t}\right)}$, where β_i is a root of ρ with $v_L(\beta_i) = m = \frac{t}{d}$.

Denote the slopes of $\mathcal{N}$ by $m_1 < m_2 < \cdots < m_u$ and the residual polynomials by $\overline{A}_{m_i}$. It follows directly from Definition 5.1 that the constant coefficient of $\overline{A}_{m_i}$ is equal to the leading coefficient of $\overline{A}_{m_{i+1}}$. The nonzero terms of $\overline{A}_m$ correspond to the points of the form $(-h, v_L(\rho_h))$ on the segment of slope m.

The residual invariant. We now consider the residual polynomials attached to the segments of the ramification polygon $\mathcal{N}(\varphi)$ of an Eisenstein polynomial φ. If $m_1, \ldots, m_u$ are the slopes of $\mathcal{N}(\varphi)$ and $\overline{A}_{m_1}$ is the residual polynomial of the segment of slope m_i we write $\mathcal{A}_\varphi = (\overline{A}_{m_1}, \ldots, \overline{A}_{m_u})$.

Let $\alpha = \alpha_1, \ldots, \alpha_e \in K^{\mathrm{sep}}$ be the roots of φ. Then the roots of the ramification polynomial $\rho(x) = \frac{\varphi(\alpha x+\alpha)}{\alpha^e}$ are of the form $\frac{\alpha_i - \alpha}{\alpha}$, and if $v_L\left(\frac{\alpha_i-\alpha}{\alpha}\right) = m = \frac{t}{d}$ we have $\overline{A}_m\left(\frac{(\alpha_i-\alpha)^d}{\alpha^{d+t}}\right) = 0$.

Let $\delta \in \mathcal{O}_L^\times$ and $\beta = \delta\alpha$. Then the minimal polynomial $\psi \in \mathcal{O}_K[x]$ of β is Eisenstein and has the same ramification polygon $\mathcal{N}$ as φ. Let $\overline{\left(\frac{(-1+\alpha_i/\alpha)^d}{\alpha^t}\right)}$ be a root of the residual polynomial $\overline{A}_m$ of the ramification polynomial ρ of φ for the segment of $\mathcal{N}$ with slope $m = \frac{t}{d}$. Then by the proof of [GP12, Proposition 4.4], the corresponding residual polynomial $\overline{B}_m(z)$ of the ramification polynomial σ of ψ has a root $\overline{\left(\frac{(-1+\beta_i/\beta)^d}{\beta^t}\right)}$ with

$$\frac{(-1+\beta_i/\beta)^d}{\beta^t} \sim \frac{1}{\delta^t}\frac{(-1+\alpha_i/\alpha)^d}{\alpha^t}.$$

Thus $\overline{B}_m(z) = \overline{\gamma}\overline{A}_m(\overline{\delta}^t z)$ for some $\overline{\gamma} \in \kappa^\times$.

Since the ramification polynomials ρ and σ are monic the respective residual polynomials $\overline{A}_{m_1}$ and $\overline{B}_{m_1}$ of the first segment (with slope $m_1 = \frac{t_1}{d_1}$) are also monic. Therefore we get

$$\overline{B}_{m_1}(z) = \overline{\delta}^{(-t_1)\deg A_{m_1}} \overline{A}_{m_1}(\overline{\delta}^{t_1} z).$$

Because all uniformizers of L/K are of the form $\beta = \delta\alpha$ where $v_L(\delta) = 0$ and because the residual polynomials are only affected by $\overline{\delta} \in \kappa^\times$ as described above we obtain an invariant of L/K. Note that our formulation of the invariant $\mathcal{A}$ differs in the ordering of the polynomials from [PS17, Theorem 4.7], because of the different ordering of the segments in the ramification polygon.

Theorem 5.2. *Let $\varphi \in \mathcal{O}_K[x]$ be an Eisenstein polynomial with ramification polygon $\mathcal{N}$. Denote by $m_1 = \frac{t_1}{d_1}, \ldots, m_u = \frac{t_u}{d_u}$ the slopes of the segments of $\mathcal{N}$ and*

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

let $\overline{A}_{m_i}$ be the residual polynomial of the segment of slope m_i. Let $L = K[x]/(\varphi)$. Then the following is an invariant of L/K:

$$\mathcal{A}_{L/K} = \left\{ \left(\overline{\gamma}_1 \overline{A}_{m_1}(\overline{\delta}^{t_1} z), \overline{\gamma}_2 \overline{A}_{m_2}(\overline{\delta}^{t_2} z), \ldots, \overline{\gamma}_u \overline{A}_{m_u}(\overline{\delta}^{t_u} z) \right) : \overline{\delta} \in \kappa^\times \right\} \tag{5.3}$$

where $\overline{\gamma}_1 = \overline{\delta}^{(-t_1)\deg A_{m_1}}$ and $\overline{\gamma}_i = \overline{\gamma}_{i-1} \overline{\delta}^{(-t_i)\deg A_{m_i}}$ for $i = 2, \ldots, u$. We write

$$\mathcal{A}_{L/K} = [\overline{A}_{m_1}, \ldots, \overline{A}_{m_u}].$$

We say that $\mathcal{A}_{L/K}$ is the *residual invariant* of the extension L/K. This invariant is an important tool in the enumeration of generating polynomials for extensions of local fields [PS17]. Together with the ramification polygon and the constant coefficient modulo π_K^2 the residual invariant determines a subextension T of the splitting field N of an Eisenstein polynomial such that N/T is a p-extension [GP12, Theorem 9.1]. This data also determines the Galois groups of Eisenstein polynomials whose ramification polygon consists of a single segment [GP12, Section 8].

The residual invariant for general extensions. It is natural to extend the definition of the residual invariant to include extensions L/K generated by a root α of an Øystein polynomial $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i$ by setting

$$\overline{B}_m(z) = \sum_{k=0}^{(i-j)/d} \overline{\rho_{j+kd}\nu(\alpha)^{kt-v_L(\rho_j)}} z^k \in \lambda[z].$$

Unfortunately, in this setting there may exist $\delta_1, \delta_2 \in \mathcal{O}_K^\times$ with $\delta_1 \equiv \delta_2 \pmod{\pi_K}$ for which the residual polynomials of the minimal polynomials of $\delta_1\alpha$ and $\delta_2\alpha$ differ for some slope m, which means that the equivalence relation used to define $\mathcal{A}_{L/K}$ in the Eisenstein case may not be well-defined. To avoid this difficulty we base the residual invariant of $L/L_{\mathrm{ur}}/K$ on $\mathcal{A}_{L/L_{\mathrm{ur}}}$. Therefore we need to consider the action of $\mathrm{Gal}(L_{\mathrm{ur}}/K) \cong \mathrm{Gal}(\lambda/\kappa)$ on $\mathcal{A}_{L/L_{\mathrm{ur}}}$:

Definition 5.4. Let $L/L_{\mathrm{ur}}/K$ and let $(\overline{A}_{m_1}, \ldots, \overline{A}_{m_u})$ be a representative of the residual invariant $\mathcal{A}_{L/L_{\mathrm{ur}}}$ of the totally ramified extension L/L_{ur}. Let γ_i $(1 \le i \le u)$ be as in Theorem 5.2. We call

$$\mathcal{A}_{L/K} = \left\{ \left(\sigma\big(\overline{\gamma}_1 \overline{A}_{m_1}(\overline{\delta}^{t_1} z)\big), \ldots, \sigma\big(\overline{\gamma}_u \overline{A}_{m_u}(\overline{\delta}^{t_u} z)\big) \right) : \overline{\delta} \in \lambda^\times,\ \sigma \in \mathrm{Aut}(\lambda/\kappa) \right\}$$

the *residual invariant* of L/K.

Distinguished residual polynomials. We choose a distinguished representative of each residual invariant $\mathcal{A}_{L/K}$ defined in Theorem 5.2 using the following ordering:

Definition 5.5. Let $\langle \overline{\xi} \rangle = \mathbb{F}_q^\times$, $g(z) = \sum_{i=0}^n g_i z^i \in \mathbb{F}_q[z]$ and $h(z) = \sum_{i=0}^n h_i z^i \in \mathbb{F}_q[z]$. We write $g >_{\overline{\xi}} h$ when $g_i = h_i$ for $i > j$ and $\log_{\overline{\xi}} g_j > \log_{\overline{\xi}} h_j$ for some $0 \le j \le n$. With lexicographic ordering, we extend this ordering to the tuples of polynomials in the residual invariant of an Eisenstein polynomial. We call the smallest tuple in the residual invariant distinguished.

To find the distinguished representative of $\mathcal{A}$, we find $\overline{\delta} \in \kappa^\times$ such that

$$\left(\overline{\gamma}_1 \overline{A}_{m_1}(\overline{\delta}^{t_1} z), \overline{\gamma}_2 \overline{A}_{m_2}(\overline{\delta}^{t_2} z), \ldots, \overline{\gamma}_u \overline{A}_{m_u}(\overline{\delta}^{t_u} z) \right) \tag{5.6}$$

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

is minimal with respect to $>_{\overline{\xi}_K}$ where $\overline{\gamma}_1 = \overline{\delta}^{(-t_1)\deg A_{m_1}}$ and $\overline{\gamma}_i = \overline{\gamma}_{i-1}\overline{\delta}^{(-t_i)\deg A_{m_i}}$ for $i = 2, \ldots, u$. Repeated applications of Lemma 5.7 below yield $l = b + c\Delta$ such that (5.6) is minimal for $\overline{\delta} = \overline{\xi}_K^l$.

When $a = bq + r$ for $a, q \in \mathbb{Z}$, $b \in \mathbb{Z}_{>0}$, and $0 \le r < b$ we write $r = a \bmod b$ and $q = a \operatorname{div} b$. The following elementary lemma will be useful:

Lemma 5.7. *Let $Q, e \in \mathbb{Z}_{>0}$ and $a \in \mathbb{Z}_{\ge 0}$. Set $g = \gcd(e, Q) = se + tQ$, $d = a \operatorname{div} g$, $\Delta = Q \operatorname{div} g$, $b = (-s \cdot d) \bmod Q$, and*

$$m = \min\left\{(a + k \cdot e) \bmod Q : k \in \mathbb{Z}\right\}.$$

Then $m = a \bmod g$, and $m = (a + k \cdot e) \bmod Q$ if and only if $k = b + c\Delta$ for some $c \in \mathbb{Z}$.

Definition 5.8. The *distinguished residual polynomial tuple* of $L/L_{\mathrm{ur}}/K$ is the tuple that is distinguished among the conjugates of the residual invariant of L/L_{ur} under the automorphisms of L_{ur}/K.

Families and subfamilies. Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein and set $L = K[x]/(\varphi)$. Then the first π_K-adic digit of the constant coefficient of all defining Eisenstein polynomials of L/K is in $\mathcal{C}_{L/K} = \{\overline{\varphi}_{0,1}\delta^n : \delta \in \kappa^\times\}$, which is an invariant of L/K.

For an Øystein polynomial $\varphi \in \mathcal{O}_K[x]$ we can choose $\varphi_{0,1}^*$ such $\overline{\psi}_{0,1} = \overline{\varphi}_{0,1}^*(\overline{\alpha})$ where $\psi \in L_{\mathrm{ur}}[x]$ is a defining Eisenstein polynomial of $L = K[x]/(\varphi)$ over L_{ur}. Since the $\mathrm{Aut}(L_{\mathrm{ur}}/K)$-conjugates of ψ yield the same extension over K, in this setting the invariant becomes $\mathcal{C}_{L/K} = \{\sigma(\overline{\varphi}_{0,1})\delta^n : \sigma \in \mathrm{Aut}(\lambda/\kappa),\, \delta \in \lambda^\times\}$. To combine $\mathcal{C}_{L/K}$ with the residual invariant $\mathcal{A}_{L/K}$ we restrict the transformations of the residual polynomials to those that fix a representative of $\mathcal{C}_{L/K}$. We set (compare [PS17, (4.2)] for the totally ramified case):

$$\mathcal{A}_{L/K}^* = \left\{ \left(\sigma\big(\overline{\gamma}_1 \overline{A}_{m_1}(\overline{\delta}^{t_1} z)\big), \ldots, \sigma\big(\overline{\gamma}_u \overline{A}_{m_u}(\overline{\delta}^{t_u} z)\big)\right) : \overline{\delta} \in \lambda^\times,\, \delta^n = 1,\, \sigma \in \mathrm{Aut}(\lambda/\kappa) \right\}$$

with γ_i as in Theorem 5.2. With the above we refine the definition of family from [Mon14] and [GJK+26, Section 1.2] and obtain:

Definition 5.9. A *family* $\mathcal{F}$ of extensions of K is the set of all extensions of K that have the same ramification polygon. We call the subset of all extensions L/K in $\mathcal{F}$ that have the same $\mathcal{C}_{L/K}$ and the same $\mathcal{A}_{L/K}^*$ a *subfamily*.

This notion of subfamily is used in defining labels for p-adic fields in the LMFDB, but does not reappear in the remainder of this article.

6. Reduction

Reduced Eisenstein polynomials were introduced by Krasner [Kra37] and their theory was brought into modern form by Monge [Mon14]. We recall their construction and generalize it to Øystein polynomials.

Zeroth reduction step for Eisenstein polynomials. We refine the first reduction step [Mon14, Algorithm 1] for an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$, in which the leading coefficient $\varphi_{0,1}$ of the constant term φ_0 is reduced. Because transforming $\varphi_{0,1}$ also impacts the residual polynomials, out of all the transformations that lead to a reduced value for $\varphi_{0,1}$, we choose those that yield the smallest residual polynomials with respect to $>_{\overline{\xi}_K}$ (see Definition 5.5).

Fix $\overline{\xi}_K \in \kappa$ such that $\langle \overline{\xi}_K \rangle = \kappa^\times$ and let $\xi_K \in \mathcal{O}_K$ be a lift of $\overline{\xi}_K$. We first find all $s \in \mathbb{Z}_{\geq 0}$ such that the transformation $x \mapsto x\xi_K^{-s}$ yields polynomials

$$\psi(x) = \xi_K^{es}\varphi(x\xi_K^{-s}) = x^e + \cdots + \varphi_{0,1}\xi_K^{es}$$

with $\log_{\overline{\xi}_K}(\overline{\varphi}_{0,1}\overline{\xi}_K^{es})$ minimal. That is, with Lemma 5.7 we find all s for which

$$(a + s \cdot e) \bmod (q-1) = \min\{(a + k \cdot e) \bmod (q-1) : 0 \leq k \leq q-2\}$$

where $a = \log_{\overline{\xi}_K} \overline{\varphi}_{0,1}$. Among these polynomials we find those whose residual polynomials are minimal given the constraints above. This choice assures compatibility with the generic defining polynomials [GJK+26] but also means that the residual polynomials of distinguished polynomials in general do not match their distinguished representatives.

The definition of being a *distinguished* ν-Øystein polynomial is given in Definition 6.14 below. We build up the definition through a series of conditions.

Condition 6.1. For an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$ to be distinguished we require that for all Eisenstein polynomials ψ with $K[x]/(\psi) \cong K[x]/(\varphi)$ we have

1. $\log_{\overline{\xi}_K}(\overline{\varphi_{0,1}}) \leq \log_{\overline{\xi}_K}(\overline{\psi_{0,1}})$ and
2. $\mathcal{A}_\varphi \leq \mathcal{A}_\psi$ when $\log_{\overline{\xi}_K}(\overline{\varphi_{0,1}}) = \log_{\overline{\xi}_K}(\overline{\psi_{0,1}})$.

When $e = p^w$ exactly one representative of $\mathcal{A}_{L/K}$ satisfies Condition 6.1. Reducing $\varphi_{0,1}$ is the first step in our reduction algorithm for Eisenstein polynomials.

Algorithm 6.2 (`polred0ram`).

Input: Eisenstein $\varphi \in \mathcal{O}_K[x]$ of degree e with ramification polynomial ρ
Output: $\left\{\psi(x) = \delta^e\varphi(\frac{1}{\delta}x) : \delta \in \mathcal{R}_K \text{ and } \psi \text{ satisfies Condition 6.1}\right\}$ and a distinguished representative of $\mathcal{A}_{L/K}$

Write $\langle \overline{\xi}_K \rangle = \kappa^\times$.

(1) compute the residual polynomials $(A_{m_1}, \ldots A_{m_u})$ of ρ.
(2) find the set E of all $\overline{\delta} \in \kappa^\times$ such that $\log_{\overline{\xi}_K}(\overline{\varphi}_{0,1}\overline{\delta}^e) \bmod (\#\kappa - 1)$ is minimal.
(3) find the set D of all $\overline{\delta} \in E$ such that

$$(\overline{B}_{m_1}, \ldots, \overline{B}_{m_u}) = \left(\overline{\gamma}_1\overline{A}_{m_1}(\overline{\delta}^{t_1}z), \ldots, \overline{\gamma}_u\overline{A}_{m_u}(\overline{\delta}^{t_u}z)\right)$$

is minimal with respect to $\geq_{\overline{\xi}_K}$ (see Theorem 5.2 and Definition 5.5).
(4) return $\left\{\delta^e\varphi(\frac{1}{\delta}x) : \overline{\delta} \in D\right\}$ where $\delta \in \mathcal{R}_K$ is a lift of $\overline{\delta}$ and $(\overline{B}_{m_1}, \ldots, \overline{B}_{m_u})$

Constant coefficient of Øystein polynomials. Because for Øystein polynomials we do not have a straightforward connection between constant coefficient and residual polynomial transformations, the following is simpler than Condition 6.1.

Let $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1}\varphi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ be ν-Øystein. In the following we will be concerned with the reduction of the φ_i^*. We write $\varphi_i^*(x) = \sum_{k=0}^{\infty}\varphi_{i,k}^*\pi_K^k$ where $\varphi_{i,k}^* = \sum_{j=0}^{f-1}\varphi_{i,k,j}^*x^j$ with $\varphi_{i,k,j}^* \in \mathcal{R}_K$.

Condition 6.3. Let $\varphi \in \mathcal{O}_K[x]$ be ν-Øystein. For φ to be distinguished we require that for all ν-Øystein polynomials $\psi \in \mathcal{O}_K[x]$ with $K[x]/(\psi) \cong K[x]/(\varphi)$ we have

$$\log_{\overline{\xi}_L}(\overline{\varphi}_{0,1}^*(\overline{\xi}_L)) \leq \log_{\overline{\xi}_L}(\overline{\psi}_{0,1}^*(\overline{\xi}_L)).$$

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

Additive residual polynomials. In [PS17] additive residual polynomials are called residual polynomials of components; in [Mon14] they are denoted by S_m; and in [Kra37] they are denoted by U_m.

Definition 6.4. Let $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ be ν-Øystein, α a root of φ, and $\rho(x) = \varphi(\nu(\alpha)x + \alpha)/\nu(\alpha)^e$ the ramification polynomial of φ. For $m \in \mathbb{Z}_{\geq 0}$ we call

$$\overline{A}_m^+(x) = \overline{\left(\frac{\rho(\nu(\alpha)^m x)}{\mathrm{cont}_{\nu(\alpha)}(\rho(\nu(\alpha)^m x))}\right)}$$

the *additive residual polynomial* of φ attached to the slope m.

Lemma 6.5. *For $m \in \mathbb{Z}_{>0}$, $\overline{A}_m^+(x)$ is additive. Suppose the ramification polygon $\mathcal{N}$ of φ has a segment of slope m whose endpoints have abscissas $-p^u, -p^v$, with $0 \leq v < u \leq w$. Then $\overline{A}_m^+(x)$ has top degree p^u and bottom degree p^v.*

Proof. Set $\pi_L = \nu(\alpha)$, $\varphi_m(x) = \varphi(\pi_L^{m+1}x + \alpha)$, and $\theta_m(x) = \frac{\varphi_m(x)}{\mathrm{cont}_{\pi_L}(\varphi_m)}$. Then $\theta_m(x) \in \mathcal{O}_L[x]$ is a primitive polynomial whose image in $\lambda[x]$ is $\overline{A}_m^+(x)$. The roots of $\theta_m(x)$ have the form $\frac{\widetilde{\alpha}-\alpha}{\pi_L^{m+1}}$, where $\widetilde{\alpha}$ is a root of $\varphi(x)$. It follows from Lemma 4.3 and (4.4) that there are $n - p^u$ roots $\widetilde{\alpha}$ of $\varphi(x)$ such that $v_L\left(\frac{\widetilde{\alpha}-\alpha}{\pi_L^{m+1}}\right) < 0$. These correspond to primitive factors of $\theta_m(x)$ of the form $-\frac{\pi_L^{m+1}}{\widetilde{\alpha}-\alpha}x + 1$. The remaining roots $\widetilde{\alpha}$ of $\varphi(x)$ satisfy $v_L\left(\frac{\widetilde{\alpha}-\alpha}{\pi_L^{m+1}}\right) \geq 0$, and give primitive factors of the form $x - \frac{\widetilde{\alpha}-\alpha}{\pi_L^{m+1}}$. Hence there is $\zeta \in \lambda^\times$ such that $\zeta^{-1}\overline{A}_m^+(x)$ is the product of the factors $x - \overline{\left(\frac{\widetilde{\alpha}-\alpha}{\pi_L^{m+1}}\right)} \in \lambda[x]$ such that $v_L\left(\frac{\widetilde{\alpha}-\alpha}{\pi_L^{m+1}}\right) \geq 0$.

As in the proof of Lemma 4.3 we let $\psi(x)$ be the minimal polynomial over L_{ur} of the uniformizer $\pi_L = \nu(\alpha)$ for L. Set $\delta = \nu'(\alpha) \in \mathcal{O}_L^\times$. Corresponding to each root $\widetilde{\alpha}$ of $\varphi(x)$ such that $\widetilde{\alpha} \sim \alpha$ there is a root $\widetilde{\pi}_L = \nu(\widetilde{\alpha})$ of $\psi(x)$ such that $\widetilde{\pi}_L - \pi_L \sim \delta \cdot (\widetilde{\alpha} - \alpha)$. Hence there is $\gamma \in \lambda^\times$ such that $\gamma\overline{A}_m^+(\delta^{-1}x)$ is the mth additive residual polynomial of $\psi(x)$. Since the conclusions of the lemma hold for the Eisenstein polynomial $\psi(x)$ [Sch03, Lemma 1], they hold for $\varphi(x)$ as well. □

When φ is Eisenstein the residual polynomials of segments of the ramification polygon $\mathcal{N}$ of φ with positive integral slopes correspond to additive residual polynomials. Namely, when $\mathcal{N}$ has a segment $\mathcal{S}$ of slope $m \in \mathbb{Z}_{>0}$ then $\overline{A}_m^+(z) = z^j\overline{A}_m(z)$ where $-j$ is the abscissa of the right endpoint of $\mathcal{S}$. When $\mathcal{N}$ has no segment of slope m then $\overline{A}_m^+$ is a monomial.

Although the additive residual polynomials do not carry new information beyond the residual polynomials, they are a useful tool for the reduction of Eisenstein and Øystein polynomials as we will see in Proposition 6.6 and Theorem 6.8.

As we have seen in (4.6), the content of $\rho(\nu(\alpha)^m x)$ is equal to $e\Phi_{\mathcal{N}}(m)$, which only depends on the ramification polygon.

Reduction of Eisenstein polynomials. We recall the method used in [Mon14] for reducing an Eisenstein polynomial $\varphi \in \mathcal{O}_K[x]$ and introduce our choice of representatives of the cokernel of the additive residual polynomials $\overline{A}^+ \in \kappa[x]$. Let $m \in \mathbb{Z}_{>0}$ and let $\rho(x) = \frac{\varphi(\pi_L x + \pi_L)}{\pi_L^e}$ be the ramification polynomial of φ. Because φ

is Eisenstein the additive residual polynomial to the slope m is $\overline{A}_m^+(x) = \overline{\frac{\rho(\pi_L^m x)}{\pi_L^{e\Phi_{L/K}(m)}}}$. The reduction is based on the following result, which describes how a change in the uniformizer of L changes the coefficients of the defining polynomials in terms of the additive residual polynomials, compare [Kra37, pp. 156–7], [Mon14, Lemma 2.5], or [PS17, Proposition 5.5]:

Proposition 6.6. *Let $\varphi \in \mathcal{O}_K[x]$ be Eisenstein, let π_L be a root of $\varphi(x)$, and set $L = K(\pi_L)$. Let $\gamma \in \mathcal{O}_L^\times$ and $m \in \mathbb{Z}_{>0}$; then $\beta = \pi_L + \gamma\pi_L^{m+1}$ is another uniformizer of L. Let $\psi(x) \in \mathcal{O}_K[x]$ be the minimal polynomial of β over K. Let $\overline{A}_m^+(z)$ be the additive residual polynomial of φ for the slope m and set $\eta = \pi_K/\pi_L^e$. Then*

1. *$\varphi_{i,k} = \psi_{i,k}$ for all i, k such that $i + ek < e(\Phi_{L/K}(m) + 1)$.*
2. *Set $h = e\Phi_{L/K}(m)$, $i = h \bmod e$ and $k = (h \operatorname{div} e) + 1$. Then*
$$(\varphi_{i,k} - \psi_{i,k})\eta^k \equiv \overline{A}_m^+(\gamma) \pmod{\pi_L}.$$

This proposition leads to a reduction algorithm (see [Mon14, Algorithm 2]), in which starting at slope $m = 1$ the coefficients of φ are reduced iteratively. If $\overline{A}_m^+ : \kappa \to \kappa$ is surjective we can choose $\gamma \in \mathcal{O}_L$ so that the transformation $\pi_L \mapsto \alpha + \gamma\pi_L^{m+1}$ gives $\psi_{i,k} = 0$ where i, k are defined in statement (2). Otherwise, we can still alter $\overline{\varphi}_{i,k}$ by an element of the image of the additive polynomial $\overline{A}_m^+$:

Definition 6.7. Let $\overline{\xi}$ be a generator for λ over $\mathbb{F}_p$ and set $d = [\lambda : \mathbb{F}_p] = f \cdot [\kappa : \mathbb{F}_p]$; then $B = \{1, \overline{\xi}, \ldots, \overline{\xi}^{d-1}\}$ is an $\mathbb{F}_p$-basis for λ. Let $\overline{A}^+ \in \kappa[x]$ be additive and let T be the $d \times d$ matrix whose ith row is the coordinate vector of $\overline{A}^+(\overline{\xi}^{i-1})$ with respect to B. Let E be the reduced row echelon form of T and set $r = \operatorname{rank}(E) = \operatorname{rank}(T)$. Let $\beta(x) \in \kappa[x]$ and let $\vec{v}$ be the coordinate vector of $\beta(\overline{\xi})$ with respect to B. For $1 \le i \le r$ let E_i be the ith row of E and assume that the leftmost nonzero entry of E_i is in column j_i. Set $\vec{w} = \vec{v} - \sum_{i=1}^r v_{j_i} E_i$, where v_{j_i} is the j_i entry of $\vec{v}$, and let η be the element of λ whose coordinate vector with respect to B is $\vec{w}$. We define the reduction of $\beta(x)$ by $\overline{A}^+$ to be the unique $\gamma(x) \in \kappa[x]$ such that $\deg(\gamma) < f$ and $\gamma(\overline{\xi}) = \eta$.

Reduction of Øystein polynomials. We now generalize the reduction algorithm for Eisenstein polynomials to Øystein polynomials. Let $\varphi \in K[x]$ be a ν-Øystein polynomial, let α be a root of φ, and set $L = K(\alpha)$. We investigate the effect of the transformation $\alpha \mapsto \alpha + \gamma\nu(\alpha)^m$ on the coefficients of the respective minimal polynomials. Generalizing Proposition 6.6 to Øystein polynomials we obtain:

Theorem 6.8. *Let $\varphi \in \mathcal{O}_K[x]$ be a ν-Øystein polynomial written as*
$$\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i \text{ with } \varphi_i^*(x) = \sum_{j=0}^{f-1} x^j \sum_{k=1}^{\infty} \varphi_{i,j,k}^* \pi_K^k \text{ and } \varphi_{i,j,k}^* \in \mathcal{R}_K.$$
Let α be a root of φ and set $L = K(\alpha)$. Let $\beta = \alpha + \gamma(\alpha)\nu(\alpha)^{m+1}$ for some $m \in \mathbb{Z}_{\ge 0}$ and $\gamma \in \mathcal{O}_K[x]$ such that $\deg(\gamma) < f$, $v_L(\gamma(\alpha)) = 0$, and $v_L(\nu(\beta)) = 1$. Then the minimal polynomial $\psi \in \mathcal{O}_K[x]$ of β over K is of the form
$$\psi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \psi_i^*(x)\nu(x)^i \text{ with } \psi_i^*(x) = \sum_{j=0}^{f-1} x^j \sum_{k=1}^{\infty} \psi_{i,j,k}^* \pi_K^k \text{ and } \psi_{i,j,k}^* \in \mathcal{R}_K.$$

Let $\rho(x) = \frac{\varphi(\nu(\alpha)x+\alpha)}{\nu(\alpha)^e}$ be the ν-ramification polynomial of φ, and for $m \in \mathbb{N}_0$ set $A_m^+(x) = \frac{\rho(\nu(\alpha)^m x)}{\nu(\alpha)^{e\Phi_{L/K}(m)}}$. Then

(1) *$\varphi^*_{i,j,k} = \psi^*_{i,j,k}$ for all i, k such that $i + ek < e(\Phi_{L/K}(m) + 1)$.*

(2) *Set $h = e\Phi_{L/K}(m)$, $\widetilde{\imath} = h \bmod e$ and $\widetilde{k} = (h \operatorname{div} e) + 1$. Let $\eta \in \mathcal{O}_K[x]$ satisfy $\eta(\alpha) = \pi_K/\nu(\alpha)^e$. Then*

$$\sum_{j=0}^{f-1} \left(\overline{\varphi^*_{\widetilde{\imath},j,\widetilde{k}}} - \overline{\psi^*_{\widetilde{\imath},j,\widetilde{k}}}\right) \overline{\alpha}^j = \overline{\eta}(\overline{\alpha})^{-k} \overline{A}_m^+(\overline{\gamma}(\overline{\alpha})).$$

Note that the condition $v_L(\nu(\beta)) = 1$ is always satisfied for $m > 0$, since in this case $\nu(\beta) = \nu(\alpha + \gamma(\alpha)\nu(\alpha)^{m+1}) = \nu(\alpha) + \nu(\alpha)^2\delta$ for some $\delta \in L$ with $v_L(\delta) \geq 0$.

Proof. We have $\varphi(\beta) - \psi(\beta) = \varphi(\beta) = \varphi(\alpha + \gamma(\alpha)\nu(\alpha)^{m+1}) = \rho(\gamma(\alpha)\nu(\alpha)^m)\nu(\alpha)^e$. and also

$$\varphi(\beta) - \psi(\beta) = \sum_{i=0}^{e-1} \left(\varphi^*_i(\beta) - \psi^*_i(\beta)\right) \nu(\beta)^i = \sum_{i=0}^{e-1}\sum_{j=0}^{f-1} \beta^j \sum_{k=1}^{\infty} \left(\varphi^*_{i,j,k} - \psi^*_{i,j,k}\right) \nu(\beta)^i \pi_K^k.$$

Combine the two expressions for $\varphi(\beta) - \psi(\beta)$ and divide by $\nu(\alpha)^{e+e\Phi_{L/K}(m)}$ to get

$$\sum_{i=0}^{e-1}\sum_{j=0}^{f-1} \beta^j \sum_{k=1}^{\infty} \left(\varphi^*_{i,j,k} - \psi^*_{i,j,k}\right) \frac{\nu(\beta)^i \pi_K^k}{\nu(\alpha)^{e+e\Phi_{L/K}(m)}} = \frac{\rho(\gamma(\alpha)\nu(\alpha)^m)}{\nu(\alpha)^{e\Phi_{L/K}(m)}}. \tag{6.9}$$

Note that we have $\beta \sim \alpha$ and that since $v_L(\pi_K) = e$ there exists $\eta \in \mathcal{O}_K[x]$ with $\eta(\alpha) = \pi_K/\nu(\alpha)^e$.

Suppose $m = 0$. Since $\Phi_{L/K}(0) = 0$, statement (1) holds vacuously. Furthermore, we have $\widetilde{k} = 1, \widetilde{\imath} = 0$, so (6.9) gives

$$\sum_{j=0}^{f-1} \alpha^j \left(\varphi^*_{0,j,1} - \psi^*_{0,j,1}\right) \eta(\alpha) \equiv \rho(\gamma(\alpha)) \equiv A_0^+(\gamma(\alpha)) \pmod{\nu(\alpha)},$$

which implies statement (2) for this case.

For $m > 0$ we have $\nu(\beta) = \nu(\alpha + \gamma(\alpha)\nu(\alpha)^{m+1}) \sim \nu(\alpha)$. Therefore by (6.9)

$$\sum_{i=0}^{e-1}\sum_{j=0}^{f-1} \alpha^j \sum_{k=1}^{\infty} \left(\varphi^*_{i,j,k} - \psi^*_{i,j,k}\right) \eta(\alpha)^k \frac{\nu(\alpha)^{i+ek}}{\nu(\alpha)^{e+e\Phi_{L/k}(m)}} \equiv A_m^+(\gamma(\alpha)) \pmod{\nu(\alpha)}.$$

If $i + ek < e(\Phi_{L/K}(m) + 1)$ then $\varphi^*_{i,j,k} = \psi^*_{i,j,k}$ since $A_m^+(\gamma(\alpha)) \in \mathcal{O}_L$. This gives statement (1). All the terms on the left with $i+ek > e(\Phi_{L/K}(m)+1)$ are congruent to $0 \pmod{\nu(\alpha)}$. By considering the remaining terms (those with $i = \widetilde{\imath}$ and $k = \widetilde{k}$) we get statement (2). □

Let $\varphi \in \mathcal{O}_K[x]$ be a ν-Øystein polynomial with root α and set $L = K(\alpha)$. Then every ν-Øystein polynomial that defines L/K can be obtained from φ by a sequence of transformations of the type described in Theorem 6.8.

Most of the coefficients of an Øystein polynomial can be easily reduced. We write $(-p^{w_1}, v_L(\rho_{p^{w_1}}))$ and $(-1, v_L(\rho_1))$ for the endpoints of the segment of $\mathcal{N}(\varphi)$ with steepest slope $\widetilde{m} = \frac{v_L(\rho_1)-v_L(\rho_{p^{w_1}})}{p^{w_1}-1}$. Let $m \geq \widetilde{m}$ be an integer and suppose the minimum in (4.6) is not attained for $i = 1$. Then there is $2 \leq j \leq n$ such that $v_L(\rho_j) + m \cdot j < v_L(\rho_1) + m$. Thus $\frac{v_L(\rho_1)-v_L(\rho_j)}{j-1} > m \geq \widetilde{m}$, which contradicts the assumption that $\widetilde{m}$ is the steepest slope in $\mathcal{N}(\varphi)$. Hence for $m \geq \widetilde{m}$ we have $e\Phi_{\mathcal{N}(\varphi)}(m) = v_L(\rho_1) + m$. We get the following version of the Krasner bound (see, for instance, [PS17, Lemma 2.3]):

Corollary 6.10. *Let $\psi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \psi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ and $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i$ be ν-Øystein polynomials in $\mathcal{O}_K[x]$. Assume that $\varphi_{i,k}^*(x) = 0$ for all i, k such that $i + ek > e(\Phi_{L/K}(\widetilde{m}) + 1)$ and $\varphi_{i,k}^*(x) = \psi_{i,k}^*(x)$ for all other i, k. Then $K[x]/(\psi) \cong K[x]/(\varphi)$.*

Since the transformation used in Algorithm 6.2 (3) is not directly applicable for Øystein polynomials, we apply Theorem 6.8 for the horizontal segment.

Algorithm 6.11 (`polred0`)**.**

Input: ν-Øystein $\varphi(x) \in \mathcal{O}_K[x]$ with ν-ramification polynomial $\rho \in \mathcal{O}_L[x]$
Output: $\{\psi \in \mathcal{O}_K[x] : \psi = \chi_{L/K}(\alpha + \theta\nu(\alpha))$ with $\theta \in \mathcal{R}_{L_{\mathrm{ur}}}$, $\log_{\overline{\xi}} \overline{\psi}_{0,1}$ minimal$\}$

Denote by $\overline{\xi_L} \in \lambda$ a root of $\overline{\nu}$.
(1) $\eta \leftarrow \frac{\pi_K}{\nu(\alpha)^e}$
(2) $\overline{A}_0^+(x) \leftarrow \overline{\left(\frac{\varphi(\nu(\alpha)z+\alpha)}{\mathrm{cont}_{\nu(\alpha)}(\varphi(\nu(\alpha)x+\alpha))}\right)}$
(3) $r \leftarrow \min\left\{\log_{\overline{\xi}_L}\left(\sigma\left(\overline{\varphi}_{0,1}(\overline{\xi}_L)\right) \cdot \overline{\xi}_L^{e\cdot l}\right) : 0 \leq l < \#\lambda - 1, \sigma \in \mathrm{Aut}(\lambda/\kappa)\right\}$
(4) $\overline{B}(x) \leftarrow \overline{\eta}^{-1}\overline{A}_0^+(x) - \overline{(\varphi_{0,1} - \xi_L^r)}$
(5) $\Theta \leftarrow \{\theta \in \mathcal{R}_{L_{\mathrm{ur}}} : \overline{B}(\overline{\theta}) = 0\}$
(6) return $\{\chi_{L/K}(\alpha + \theta\nu(\alpha)) : \theta \in \Theta\}$

For $m \in \mathbb{Z}_{>0}$ not covered by Corollary 6.10 we apply the following algorithm. It can be used for all Øystein polynomials, including Eisenstein polynomials, which are obtained by taking $\nu(x) = x$.

Algorithm 6.12 (`polredslope`)**.**

Input: $\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1} \varphi_i^*(x)\nu(x)^i$ with root α and $m \in \mathbb{Z}_{>0}$
Output: The set M of reduced polynomials obtained by substitutions of the form $\alpha \mapsto \alpha + \theta \cdot \nu(\alpha)^{m+1}$, for $\theta \in \mathcal{R}_{L_{\mathrm{ur}}}$

(1) $\eta \leftarrow \pi_K/\nu(\alpha)^e$
(2) $\overline{A}_m^+ \leftarrow \overline{\frac{\varphi(\alpha+\nu(\alpha)^{m+1}x)}{\nu(\alpha)^{e\Phi_{L/K}(m)}}}$
(3) $i \leftarrow e\Phi_{L/K}(m) \bmod e$, $k \leftarrow (e\Phi_{L/K}(m) \operatorname{div} e) + 1$
(4) let $\overline{\delta}$ be the reduction of $\overline{\varphi_{i,k}^*(\alpha)}$ by $\overline{A}_m^+$, see Definition 6.7
(5) $\Theta \leftarrow \left\{\theta \in \mathcal{R}_{L_{\mathrm{ur}}} : \overline{\varphi_{i,k}^*(\alpha)} - \overline{\delta} = \overline{\eta}^{-k} \cdot \overline{A}_m^+(\overline{\theta})\right\}$
(6) $M \leftarrow \left\{\chi_{L/\mathbb{Q}_p}(\alpha + \theta \cdot \nu(\alpha)^{m+1}) : \theta \in \Theta\right\}$

Tamely ramified extensions. Let $\varphi(x) = \nu(x)^\epsilon + \sum_{i=0}^{\epsilon-1} \varphi_i^*(x)\nu(x)^i \in \mathcal{O}_K[x]$ be ν-Øystein with $p \nmid \epsilon$ and $L_0 = K[x]/(\varphi)$. Because $\epsilon\Phi_{L_0/K}(m) = m$ and the steepest slope is $\widetilde{m} = 0$, by Corollary 6.10 for $\widetilde{\varphi}(x) = \nu(x)^\epsilon + \varphi_{0,1}(x)\pi_K$ we have $L_0 \cong K[x]/(\widetilde{\varphi})$.

By Lemma 3.4, for $\psi(x) = x^\epsilon + \psi_{0,1}\pi_K \in L_{\mathrm{ur}}[x]$ with $\psi_0^* \sim \varphi_0^*(\xi_L)$ and $\psi(\beta) = 0$ we have $L_{\mathrm{ur}}(\beta) = K(\xi_L, \beta) \cong L_0$. Let $\sigma : L_{\mathrm{ur}} \to L_{\mathrm{ur}}$ with $\sigma : \xi_L \to \xi_L^{q^u}$ for some $0 \leq u < f$ and let $\beta^{(\sigma)}$ be a root of $\psi^{(\sigma)}(x) = x^\epsilon + \psi_{0,1}^{(\sigma)}\pi_K \in L_{\mathrm{ur}}[x]$.

Then $K(\xi_L, \beta^{(\sigma)}) \cong K(\xi_L, \beta)$. Substitution of x by $\xi_L^{-l}x$ in $\psi^{(\sigma)}$ and multiplication by $\xi_L^{l\epsilon}$ yields $x^\epsilon + \psi_{0,1}^{(\sigma)}\xi_L^{l\epsilon}\pi_K$. To satisfy Condition 6.3, we find l and σ such that

$$\log_{\overline{\xi}_L}\left(\overline{\psi}_{0,1}^{(\sigma)}\xi_L^{l\epsilon}\right) = (aq^u + l\epsilon) \bmod (q^f - 1)$$

is minimal, where $a = \log_{\overline{\xi}_L}\overline{\psi}_{0,1}$. As in Lemma 5.7 set $g = \gcd(\epsilon, q^f - 1)$. We now find $0 \le u < f$ such that $r = aq^u \bmod g$ is minimal. Then the distinguished defining Eisenstein polynomial of L_0/L_{ur} is $\psi(x) = x^\epsilon + \xi_L^r\pi_K$ and the distinguished defining Øystein polynomial of L_0/K is

$$\varphi(x) = \nu(x)^\epsilon + \varphi_{0,1}^*(x)\pi_K \text{ with } \deg\varphi_{0,1}^* < e \text{ and } \overline{\varphi}_{0,1}^*(\overline{\xi}_L) = \overline{\xi}_L^r.$$

Final Distinction. Since the reduction algorithm yields a set of reduced polynomials rather than a unique reduced polynomial, we need to distinguish one of these. We choose the polynomial that is minimal with respect to the following ordering.

Definition 6.13. Let $\nu \in \mathcal{O}_K[x]$ be monic and irreducible modulo π_K and write

$$\varphi(x) = \nu(x)^e + \sum_{i=0}^{e-1}\left(\sum_{k=1}^{\infty}\varphi_{ik}^*(x)\pi_K^k\nu(x)^i\right) \in \mathcal{O}_K[x] \text{ where } \varphi_{ik}^* \in \mathcal{R}_K[x],\ \deg\varphi_{ik}^* < f$$

Given $\overline{\gamma}, \overline{\delta} \in \lambda$ we write $\overline{\gamma} >_{\overline{\xi}_L} \overline{\delta}$ when $\log_{\overline{\xi}_L}\overline{\gamma} > \log_{\overline{\xi}_L}\overline{\delta}$ (compare Definition 5.5). For two ν-Øystein polynomials $\varphi, \psi \in \mathcal{O}_K[x]$ we write $\varphi >_{\overline{\xi}_L} \psi$ when $\overline{\varphi}_{ik}^*(\overline{\xi}_L) = \overline{\psi}_{ik}^*(\overline{\xi}_L)$ for all $k < k_0$ and all $0 \le i < e$, $\overline{\varphi}_{ik_0}^* = \overline{\psi}_{ik_0}^*$ for $i < i_0$, and $\overline{\varphi}_{i_0k_0}^*(\overline{\xi}_L) >_{\overline{\xi}_L} \overline{\psi}_{i_0k_0}^*(\overline{\xi}_L)$.

Main Algorithm.

Definition 6.14. A ν-Øystein polynomial $\varphi \in \mathcal{O}_K[x]$ is *distinguished* if it satisfies the following, given in order of precedence.

(1) φ satisfies Condition 6.1 or 6.3.
(2) The tuple of residual polynomials of φ is minimal (Definitions 5.5 and 5.8, considering the constraint imposed by (1)).
(3) The coefficients of φ are reduced with Algorithm 6.11 for slope $m = 0$ and Algorithm 6.12 for integral slopes $m > 0$.
(4) Among the polynomials that satisfy all of the above, φ is smallest according to Definition 6.13.

We summarize all of this in the algorithm `polredpadic`.

Algorithm 6.15 (`polredpadic`)**.**

Input: ν-Øystein polynomial $\varphi(x) \in \mathcal{O}_K[x]$ of degree $f\epsilon p^w$ with $v_K(\mathrm{disc}(\varphi)) = f(n + J - 1)$
Output: the distinguished ν-Øystein polynomial ψ with $\mathcal{O}_K[x]/(\varphi) \cong \mathcal{O}_K[x]/(\psi)$

(1) compute the ν-ramification polynomial ρ and ramification polygon $\mathcal{N}$ of φ. where $\widetilde{m}$ is the steepest slope of $\mathcal{N}$
(2) $M_0 \leftarrow \begin{cases} \texttt{polred0ram}(\varphi, \rho) & \text{if } \varphi \text{ is Eisenstein} \\ \texttt{polred0}(\varphi, \rho) & \text{otherwise} \end{cases}$
(3) for $m \in \{1, \dots, \lceil\widetilde{m}\rceil\}$:
- $M_m \leftarrow \emptyset$
- for $\psi \in M_{m-1}$: $M_m \leftarrow M_m \cup$ `polredslope`(ψ, m)

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

(4) for $\psi \in M_{\lceil \widetilde{m} \rceil}$ and $m > \widetilde{m}$:
   - $\psi^*_{i,k} \leftarrow 0$ where $i = e\Phi_{L/K}(m) \bmod e$, $k = (e\Phi_{L/K}(m) \operatorname{div} e) + 1$

(5) return the distinguished polynomial in $M_{\lceil \widetilde{m} \rceil}$ according to Definition 6.13

7. Complexity

We denote by $\mathsf{M}(R)$ the cost in bit operations of multiplication in a ring R and by $\mathsf{M}(R, n)$ the cost of multiplying two polynomials of degree up to n over R. When we compute in $\mathcal{O}_K$ to an absolute π_K-adic precision of c then with fast Fourier transform [SS71] we get

$$\mathsf{M}(\mathcal{O}_K/(\pi_K^c)) = \mathsf{M}(\kappa, c) = O(c \cdot \log c \cdot \log\log c \cdot \mathsf{M}(\kappa)) = \widetilde{O}(c\mathsf{M}(\kappa))\,.$$

Also, if $[L : K] = f\epsilon p^w$, we have $\mathsf{M}(\lambda) = \mathsf{M}(\kappa, f) = \widetilde{O}(f\mathsf{M}(\kappa))$ and $\mathsf{M}\big(\mathcal{O}_L/\pi_L^d\big) = \mathsf{M}(\lambda, d) = \mathsf{M}(\kappa, fd)$. With the Cantor-Zassenhaus algorithm $\overline{B} \in \kappa[z]$ of degree n can be factored in expected $\mathsf{Z}(\kappa, n) = \widetilde{O}\big((n^2 + n\log(q))\mathsf{M}(\kappa)\big)$ bit operations where $q = \#\kappa$. The discrete logarithm $\log_{\overline{\xi}_L} \overline{\gamma}$ can be computed in $\mathsf{L}(\lambda) := O\big(\mathsf{M}(\lambda)\, q^{f/2}\big)$ bit operations with Shanks Baby-Step Giant-Step algorithm, where $q^f = \#\lambda$. See [JOP14] for a survey of the discrete logarithm problem including more efficient algorithms.

Øystein. For the computation of characteristic polynomials we use Newton relations:

Proposition 7.1 (compare [Coh93, Proposition 4.3.3])**.** *Let $\alpha_1, \ldots, \alpha_n$ be the roots of $\varphi(x) = x^n + \sum_{i=0}^{n-1} \varphi_i x^i \in \mathcal{O}_K[x]$. Write $S(\varphi) = (S_1, \ldots, S_n)$ with $S_k = \sum_{i=1}^{n} \alpha_i^k$ where we set $\varphi_i = 0$ for $i < 0$. Then*

1. *$S_k = -k\varphi_{n-k} - \sum_{i=1}^{k-1} \varphi_{n-i} S_{k-i}$ for $1 \le k \le n$ and*
2. *$\varphi_{n-k} = -S_k/k - \sum_{i=1}^{k-1} (\varphi_{n-i} S_{k-i})/k$ for $1 \le k \le n$*

Given $(S_1, \ldots, S_n)$ we write $\varphi = X(S_1, \ldots, S_n)$ such that $X(S(\varphi)) = \varphi$.

Let $\beta \in \mathcal{O}_K[x]$ and write $b_i^{(k)}$ for the i-th coefficient of $\beta^k \bmod \varphi$.

3. *$\chi_\varphi(\beta) = X(T_1, \ldots, T_n)$ where $T_k = nb_0^{(k)} + \sum_{i=1}^{n-1} S_i b_i^{(k)}$*
4. *$\chi_\varphi\left(\frac{\beta}{\pi_K^u}\right)(x) = \frac{\psi(x)}{\operatorname{cont}_{\pi_K}(\psi)}$ where $\psi(x) = \chi_\varphi(\beta)(\pi_K^u x)$.*

Lemma 7.2. *Let $\varphi \in \mathcal{O}_K[x]$ be monic and irreducible of degree n. Let $\gamma = \beta\pi_K^{-u} \in K[x]$ where $\beta \in \mathcal{O}_K[x]$. Following Proposition 7.1, $\chi_\varphi(\gamma)$ can be computed to a π_K-adic precision of b in $\mathsf{C}(\varphi, u, b) := O(\mathsf{M}(\mathcal{O}_K/(\pi_K^c), n)\log n)$ bit operations, where $c = b + \max\{n \cdot u, e_K\lceil \log_p n \rceil\}$.*

Proof. We go through the parts of Proposition 7.1 in the order in which they would be used in the computation of a characteristic polynomial.

(4) When the coefficients of γ are not integral, to allow for the factor $(\pi_K^u)^n$ we increase the precision by $n \cdot u$ to avoid precision loss.

(1) Let $E(t) = t^n\varphi(1/t)$ and $S(t) = \sum_{k=0}^{\infty} S_k t^k$. Then $S(-t) \equiv E'(t)E(t)^{-1} \pmod{t^{n+1}}$. Using Newton inversion we compute the inverse $E(t)^{-1}$ of $E(t)$ in $O(n \log n)$ and $E'(t) \cdot E(t)^{-1} \bmod t^{n+1}$ in $\mathsf{M}(\mathcal{O}_K/(\pi_K^c), n)$ bit operations.

(3) With fast multipoint evaluation, it takes $O(\mathsf{M}(\mathcal{O}_K/(\pi_K^c), n)\log n)$ bit operations to compute all of the T_k.

(2) Similarly as in (1) this takes $\mathsf{M}(\mathcal{O}_K/(\pi_K^c), n)$ bit operations. ∎

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

Our implementation of Proposition 7.1 uses $O(n^2)$ operations in $\mathcal{O}_K$, which is all that is needed for degrees of the polynomials that we are considering.

Proposition 7.3. *Given an irreducible polynomial $\psi \in \mathcal{O}_K[x]$ of degree n with discriminant exponent $b = v_K(\operatorname{disc}(\psi))$, Algorithm 3.5 returns a ν-Øystein polynomial $\varphi \in \mathcal{O}_K[x]$ such that $K[x]/(\psi) \cong K[x]/(\varphi)$ in $\widetilde{O}(nb^2\mathsf{M}(\kappa))$ bit operations.*

Proof. Let $c = \lfloor b/n \rfloor + 1$. The costs of the steps of the algorithm are:

(1,3) The Okutsu invariants of ψ can be computed in $\widetilde{O}((n^2 + nb^2)\mathsf{M}(\kappa))$ bit operations [BNS13]. This includes the computation of Π and Γ.
(2) By our assumption from Section 2 we can obtain ν by lookup.
(4) The precision c required in (1,3) is also an upper bound for the minimum of the valuations of the coefficients of Γ and Π. To avoid precision loss we increase the precision by cf, so α is computed in $O\Big(f\mathsf{M}\Big(\mathcal{O}_K/(\pi_K^{c+cf}), n\Big)\Big) = \widetilde{O}(f(c+cf)n\mathsf{M}(\kappa))$ bit operations.
(5) With the bound for the valuation of the denominator from (4) this takes $\mathsf{C}(\psi, c, c) = O\big(\mathsf{M}\big(\mathcal{O}_K/(\pi_K^{c+nc}), n\big)\log n\big) = \widetilde{O}(n(cn+c)\mathsf{M}(\kappa))$ bit operations.

As ψ is irreducible we have $b = v_K(\operatorname{disc}(\psi)) \geq v_K(\operatorname{disc}(K[x]/(\psi))) = f(e+j-1)$ for some $j \in \mathbb{Z}_{\geq 0}$ where e and f are the ramification index and inertia degree of $K[x]/(\psi)$. Thus in total we get $\widetilde{O}((nb^2)\mathsf{M}(\kappa))$ bit operations. □

Reduction. Let $\varphi \in \mathcal{O}_K[x]$ be ν-Øystein of degree $n = fe$ with inertia degree f and ramification index $e = \epsilon p^w$ with $\gcd(p, \epsilon) = 1$ and $v_K(\operatorname{disc}(\varphi)) = f(n + J - 1)$. Let $L = K[x]/(\varphi)$. Let ρ be the ν-ramification polynomial of φ, let $(-p^{w_u}, v_L(\rho_{p^{w_u}}))$ and $(-1, v_L(\rho_1)) = (-1, J)$ be the endpoints of the steepest segment of the ramification polygon $\mathcal{N}$, and let $\widehat{m}$ be the slope of this segment. It follows from Corollary 6.10 that it is sufficient to determine the reduced polynomials over $\mathcal{O}_K/\left(\pi_K^{\widehat{c}}\right)$ for any $\widehat{c} \in \mathbb{Z}_{>0}$ such that

$$\widehat{c} > \Phi_{\mathcal{N}}(\widehat{m}) + 1 = v_L(\rho_1) + \widehat{m} + 1 = J + \widehat{m} + 1. \tag{7.4}$$

We use the π_K-adic precision of $\widehat{c}$ throughout this section.

Lemma 7.5. *Let $\varphi \in \mathcal{O}_K[x]$ be an Eisenstein polynomial of degree $e = \epsilon p^w$. Algorithm 6.2 runs in $\widetilde{O}(eq\widehat{c}\mathsf{M}(\kappa))$ bit operations.*

Proof. The costs of the steps of the algorithm are:

(1) The coefficients of $A_{m_1}, \ldots, A_{m_u}$ can be read directly from ρ.
(2) We need to compute up to w discrete logarithms at $\mathsf{L}(\kappa) = O(\mathsf{M}(\kappa)\sqrt{q})$ bit operations each and apply Lemma 5.7 up to w times at $O(\log(e)\log(q^f))$ bit operations each.
(3) Because $\#D \leq q$, this can be completed in $O(eq\widehat{c}\mathsf{M}(\kappa))$ bit operations.
(4) There are at most q different ψ, each computed in $e\mathsf{M}(\kappa, \widehat{c})$ bit operations.

In total, this algorithm can be completed in $\widetilde{O}(eq\widehat{c}\mathsf{M}(\kappa))$ bit operations. □

Lemma 7.6. *Let $\varphi \in \mathcal{O}_K[x]$ be ν-Øystein of degree $n = f\epsilon p^w$. Algorithm 6.11 returns the set of slope 0 reduced polynomials in $\widetilde{O}\big((q^{f/2} + n^2(\widehat{c} + e_K))\mathsf{M}(\kappa)\big)$ bit operations.*

Proof. The costs of the steps of the algorithm are:

Algorithmic Number Theory Symposium XVII, Groningen, July 6-10, 2026

(1) Fast exponentiation computes η in $O(\log(e)\mathsf{M}(\lambda, n\widehat{c}))$ bit operations.
(2) With (4.2) the relevant coefficients of the ν-ramification polynomial can be computed in $O(n(p^w-1)\epsilon \cdot \mathsf{M}(\kappa, \widehat{c}))$ bit operations.
(3) Evaluating $\overline{\varphi}^*_{0,1}(\overline{\xi}_L)$ takes $O(f\mathsf{M}(\lambda))$ bit operations, and its discrete logarithm can be computed in $O\big(q^{f/2}\mathsf{M}(\lambda)\big)$ bit operations. Since $\operatorname{Aut}(\lambda/\kappa)$ is generated by the Frobenius automorphism $\overline{\xi}_L \mapsto \overline{\xi}_L^q$ the discrete logarithms of the conjugates only need additional $O\big(f\mathsf{M}\big(\mathbb{Z}/(q^f-1)\big)\big)$ bit operations. Computing the minimum for each of the f conjugates separately and then taking the minimum takes $O(f\log(e)\log(q))$ bit operations with Lemma 5.7. Since $f = O(\log(p^f))$, it can be omitted.
(4,5) We have $\deg \overline{A}_0^+ = \deg \overline{B} = (\epsilon-1)p^w$. We find the roots of $\overline{B}$ in expected $\mathsf{Z}(\lambda, (\epsilon-1)p^w) = \widetilde{O}\big((((\epsilon-1)p^w)^2 + (\epsilon-1)p^w f\log q)f\mathsf{M}(\kappa)\big)$ bit operations.
(6) Because $\overline{B}$ has $\#\Theta \le \deg \overline{B} = (\epsilon-1)p^w$ roots, this step takes up to $(\epsilon-1)p^w\,\mathsf{C}(K, 0, \widehat{c}) = \widetilde{O}\big(n^2(\widehat{c}+e_K)\,\mathsf{M}(\kappa)\big)$ bit operations.

Adding these yields the statement of the lemma. $\square$

Lemma 7.7. *Let $\varphi \in \mathcal{O}_K[x]$ be ν-Øystein of degree $n = f\epsilon p^w$ and let $m \in \mathbb{Z}_{>0}$. Denote by $-p^u$ and $-p^v$ be the abscissas of the endpoints of the segment of slope m on $\mathcal{N}(\varphi)$ (if there is no segment of slope m then $u = v$). Algorithm 6.12 runs in $\widetilde{O}\big((f^{\log_2 7} + p^{u-v}n(\widehat{c}+e_K))\,\mathsf{M}(\kappa)\big)$ bit operations.*

Proof. The costs of the steps of the algorithm are:

(1) Fast exponentiation computes η in $O(\log(e)\mathsf{M}(\lambda, n\widehat{c}))$ bit operations.
(2,3) With (4.2) this takes $O(n\mathsf{M}(\kappa, \widehat{c}))$ bit operations
(4) The ν-expansion of φ can be computed in $O(fn \cdot \mathsf{M}(\kappa, \widehat{c}))$ bit operations and the coefficient $\varphi^*_{i,k}$ is computed in at most $O(f\widehat{c} \cdot \mathsf{M}(\kappa))$ bit operations. By Lemma 6.5 $\overline{A}_m^+$ has at most $u - v + 1$ non-zero coefficients. An $f \times f$ matrix over κ representing $\overline{A}_m^+ : \lambda \to \lambda$ where $\overline{A}_m^+ \in \lambda$ and its row echelon form (using Strassen's algorithm) can be computed in $O\big(f(u-v+1)\mathsf{M}(\lambda, f) + f^{\log_2 7}\mathsf{M}(\kappa)\big)$ bit operations.
(5) We use linear algebra to find Θ. The system of linear equations can be solved in $f^{\log_2 7}\mathsf{M}(\kappa)$ bit operations.
(6) We have $\#\Theta \le p^{u-v}$. Thus, we need to compute at most p^{u-v} characteristic polynomials which can be done with $\widetilde{O}(p^{u-v}n(\widehat{c}+e_K)\mathsf{M}(\kappa))$ bit operations (compare Lemma 7.6 (6)).

Adding the above we obtain the statement of the Lemma. $\square$

Proposition 7.8. *Let $\varphi \in \mathcal{O}_K[x]$ of degree $n = f\epsilon p^w$ with $v_K(\operatorname{disc}(\varphi)) = f(n + J - 1)$ be ν-Øystein. Algorithm 6.15 returns the distinguished defining polynomial of $K[x]/(\varphi)$ in $\widetilde{O}\big((q^{f/2} + eq\widehat{c} + n^2(\widehat{c}+e_K) + n\widehat{c}^2)\mathsf{M}(\kappa)\big)$ bit operations where $\widehat{c} = J + \widehat{m} + 1$ as in (7.4).*

Proof. The costs of the steps of the algorithm are:

(1) By Lemma 6.5, the coefficients that contribute to the ramification polygon are ρ_i for $i \in \{1, p, \dots, p^w\}$. They can be computed using (4.2) and their valuations can be computed by repeated squaring of the uniformizer in a total of $O\big(w \cdot \log_2 J \cdot \mathsf{M}\big(\mathcal{O}_K/(\pi_K)^{J+1}\big)\big)$ bit operations.

(2) The slope 0 reduction step takes $\widetilde{O}\big((q^{f/2} + n^2(\widehat{c} + e_K))\mathsf{M}(\kappa)\big)$ bit operations by Lemma 7.6 if $f > 1$ or $\widetilde{O}(eq\widehat{c}\,\mathsf{M}(\kappa))$ by Lemma 7.5 if $f = 1$.
(3) For $m \in \{1, \ldots, \widehat{m}\}$ the slope m reduction step only results in additional polynomials when $\mathcal{N}$ has a segment of slope m. Write $(-p^{w_i}, v_L(\rho_{p^{w_i}}))$ and $(-p^{w_{i+1}}, v_L(\rho_{p^{w_{i+1}}}))$ for the endpoints of the i-th segment of $\mathcal{N}$. It follows from (6,7) in the proof of Lemma 7.7 that the number of reduced polynomials after this step is at most $\prod_{j=1}^{u-1}(p^{w_{j+1}}/p^{w_j}) = p^w$. Since the number of segments of $\mathcal{N}(\varphi)$ is at most w the number of bit operations for this step is less than $\widetilde{O}\big((wf^{\log_2 7} + p^w n(\widehat{c} + e_K))\,\mathsf{M}(\kappa)\big)$ by Lemma 7.7.
(4) In practice $\widehat{c}$ is chosen as the precision of these computations, so that at most $n-2$ coefficients need to be set to 0.
(5) To compare two polynomials $\varphi, \psi \in \mathcal{O}_K[x]$ with respect to the ordering from Definition 6.13 we compute their difference and compute the valuations of its coefficients in $O\big(n \log \widehat{c}\,\mathsf{M}\big(\mathcal{O}_K/(\pi_K^{\widehat{c}})\big)\big)$ bit operations. The lowest valuation determines which coefficient we need to consider. Its π_K-adic expansion is computed in at most $\widehat{c}\,\mathsf{M}\big(\mathcal{O}_K/(\pi_K^{\widehat{c}})\big)$ bit operations and the discrete logarithm of the relevant coefficient is found in $O\big(\sqrt{q}\big)\,\mathsf{M}(\kappa)$ bit operations. With merge sort, we find the smallest reduced polynomial with $O(\log(p^w)p^w)$ of these comparisons. Thus this step can be completed in $\widetilde{O}\big(p^w((n+\widehat{c})\widehat{c} + \sqrt{q})\mathsf{M}(\kappa)\big)$ bit operations.

In total these are $\widetilde{O}\big((q^{f/2} + eq\widehat{c} + n^2(\widehat{c} + e_K) + n\widehat{c}^2)\mathsf{M}(\kappa)\big)$ bit operations. □

For example, when $K = \mathbb{Q}_p$, taking the largest possible $\widehat{c}$ yields a maximum runtime of $\widetilde{O}\big(p^{1+f/2} + n^4 p\big)$.

Timings. In the table below we give minimum, maximum, and average running times for finding distinguished defining polynomials using our implementation of Algorithm 3.5 `oystein` and Algorithm 6.15 `polredpadic` in Magma. In each case, we considered a random defining polynomial (created using Pari's `poltschirnhaus` function) for each ramified extension of degree n over $\mathbb{Q}_p$. All times are in seconds.

p	n	$\#L$	min time	max time	avg time
2	6	46	0.03	0.31	0.11
3	6	74	0.03	0.53	0.15
2	8	1822	0.01	1.0	0.37
2	16	890110	0.04	25	12
2	18	2990	0.09	19	4.4
3	18	130646	0.05	98	19
2	20	314542	0.03	40	11
5	20	7586	0.11	360	69
7	21	3783	0.14	190	14

The computations were run single-threaded in Magma on a Linux computer with AMD 2.0 GHz processors and 2 terabytes of RAM. Note that, in the reduction steps, our current implementation does not use the method analyzed in Lemma 7.2 but uses Magma's `CharacteristicPolynomial`, which becomes the most expensive part of the computation. The runtime depends on the structure of the field extension; for Eisenstein polynomials chosen uniformly at random from a box, Algorithm 6.15 finishes in less than 90 seconds even for $p = 2$ and $n = 1024$.

For the task of looking up a field defined by an arbitrary polynomial against a list of N distinguished polynomials, one can either use `polredpadic` or an implementation of Panayi's root finding algorithm [Pan95, PR01]. The latter is generally faster when N is small. But when N is large (say, more than 100,000), `polredpadic` will be much faster since Panayi's algorithm is a pairwise isomorphism test.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993), vers. 2.29-7, https://magma.maths.usyd.edu.au. MR MR1484478

[BNS13] Jens-Dietrich Bauch, Enric Nart, and Hayden D. Stainsby, *Complexity of OM factorizations of polynomials over local fields*, LMS J. Comput. Math. **16** (2013), 139–171. MR 3081769

[Coh93] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993. MR 1228206

[FPR02] David Ford, Sebastian Pauli, and Xavier-François Roblot, *A fast algorithm for polynomial factorization over* $\mathbb{Q}_p$, J. Théor. Nombres Bordeaux **14** (2002), no. 1, 151–169. MR 1925995 (2003g:11134)

[GJK+26] Jordi Guàrdia, John W. Jones, Kevin Keating, Sebastian Pauli, David P. Roberts, and David Roe, *Families of p-adic fields*, LuCaNT: Databases, Algorithms, and Computational Number Theory, Contemporary Mathematics, vol. 840, AMS, 2026, pp. 1–28.

[GMN12] Jordi Guàrdia, Jesús Montes, and Enric Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. **364** (2012), no. 1, 361–416. MR 2833586 (2012k:11185)

[GMN13] ———, *A new computational approach to ideal theory in number fields*, Found. Comput. Math. **13** (2013), no. 5, 729–762. MR 3105943

[GNP12] Jordi Guàrdia, Enric Nart, and Sebastian Pauli, *Single-factor lifting and factorization of polynomials over local fields*, J. Symbolic Comput. **47** (2012), no. 11, 1318–1346. MR 2927133

[GP12] Christian Greve and Sebastian Pauli, *Ramification polygons, splitting fields, and Galois groups of Eisenstein polynomials*, International Journal of Number Theory **8** (2012), no. 6, 1401–1424. MR 2965757

[Gre10] Christian Greve, *Galoisgruppen von Eisensteinpolynomen über p-adischen Körpern*, 2010, Thesis (Ph.D.) Universität Paderborn.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien, *Handbook of computational group theory*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2005. MR 2129747

[JOP14] Antoine Joux, Andrew Odlyzko, and Cécile Pierrot, *The past, evolving present, and future of the discrete logarithm*, Open problems in mathematics and computational science. Based on the presentations at the conference, Istanbul, Turkey, September 18–20, 2013, Cham: Springer, 2014, pp. 5–36 (English).

[JR06] John W. Jones and David P. Roberts, *A database of local fields*, J. Symbolic Comput. **41** (2006), no. 1, 80–97. MR 2194887 (2006k:11230)

[Kra37] Marc Krasner, *Sur la primitivité des corps p-adiques*, Mathematica (Cluj) **13** (1937), 72–191.

[LMF25] The LMFDB Collaboration, *The L-functions and modular forms database*, https://www.lmfdb.org, 2025, [Online; accessed 17 January 2025].

[Lüb23] Frank Lübeck, *Standard generators of finite fields and their cyclic subgroups*, J. Symbolic Comput. **117** (2023), 51–67, https://www.math.rwth-aachen.de/~Frank.Luebeck/data/ConwayPol. MR 4518734

[Mil17] Jonathan Milstead, *Computing Galois groups of Eisenstein polynomials over p-adic fields*, Ph.D. thesis, University of North Carolina at Greensboro, 2017.

[MN92] Jesús Montes and Enric Nart, *On a theorem of Ore*, J. Algebra **146** (1992), no. 2, 318–334. MR 1152908 (93f:11077)

[Mon14] Maurizio Monge, *A family of Eisenstein polynomials generating totally ramified extensions, identification of extensions and construction of class fields*, Int. J. Number Theory **10** (2014), no. 7, 1699–1727. MR 3256847

[Ore28] Øystein Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. **99** (1928), no. 1, 84–117 (German). MR 1512440

[Pan95] Peter Panayi, *Computation of Leopoldt's p-adic regulator*, 1995, Thesis (Ph.D.)–University of East Anglia.

[Pg25] The PARI group, *PARI/GP documentation*, Bordeaux, 2025, vers. 2.16.1, https://pari.math.u-bordeaux.fr.

[PR01] Sebastian Pauli and Xavier-François Roblot, *On the computation of all extensions of a p-adic field of a given degree*, Math. Comp. **70** (2001), no. 236, 1641–1659 (electronic). MR 1836924 (2002e:11166)

[PS17] Sebastian Pauli and Brian Sinclair, *Enumerating extensions of* (π)*-adic fields with given invariants*, Int. J. Number Theory **13** (2017), no. 8, 2007–2038 (English).

[S+26] William A. Stein et al., *Sage Mathematics Software (Version 10.9)*, The Sage Development Team, 2026, http://www.sagemath.org.

[Sch03] John Scherk, *The ramification polygon for curves over a finite field*, Canad. Math. Bull. **46** (2003), no. 1, 149–156. MR 1955622 (2004c:11220)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237 (82e:12016)

[SS71] A. Schönhage and V. Strassen, *Schnelle Multiplikation großer Zahlen*, Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. MR 292344

Universitat Politècnica de Catalunya
Email address: jordi.guardia-rubies@upc.edu

Arizona State University
Email address: jj@asu.edu

University of Florida
Email address: keating@ufl.edu

University of North Carolina Greensboro
Email address: s_pauli@uncg.edu

University of Minnesota Morris
Email address: roberts@morris.umn.edu

Massachusetts Institute of Technology
Email address: roed@mit.edu