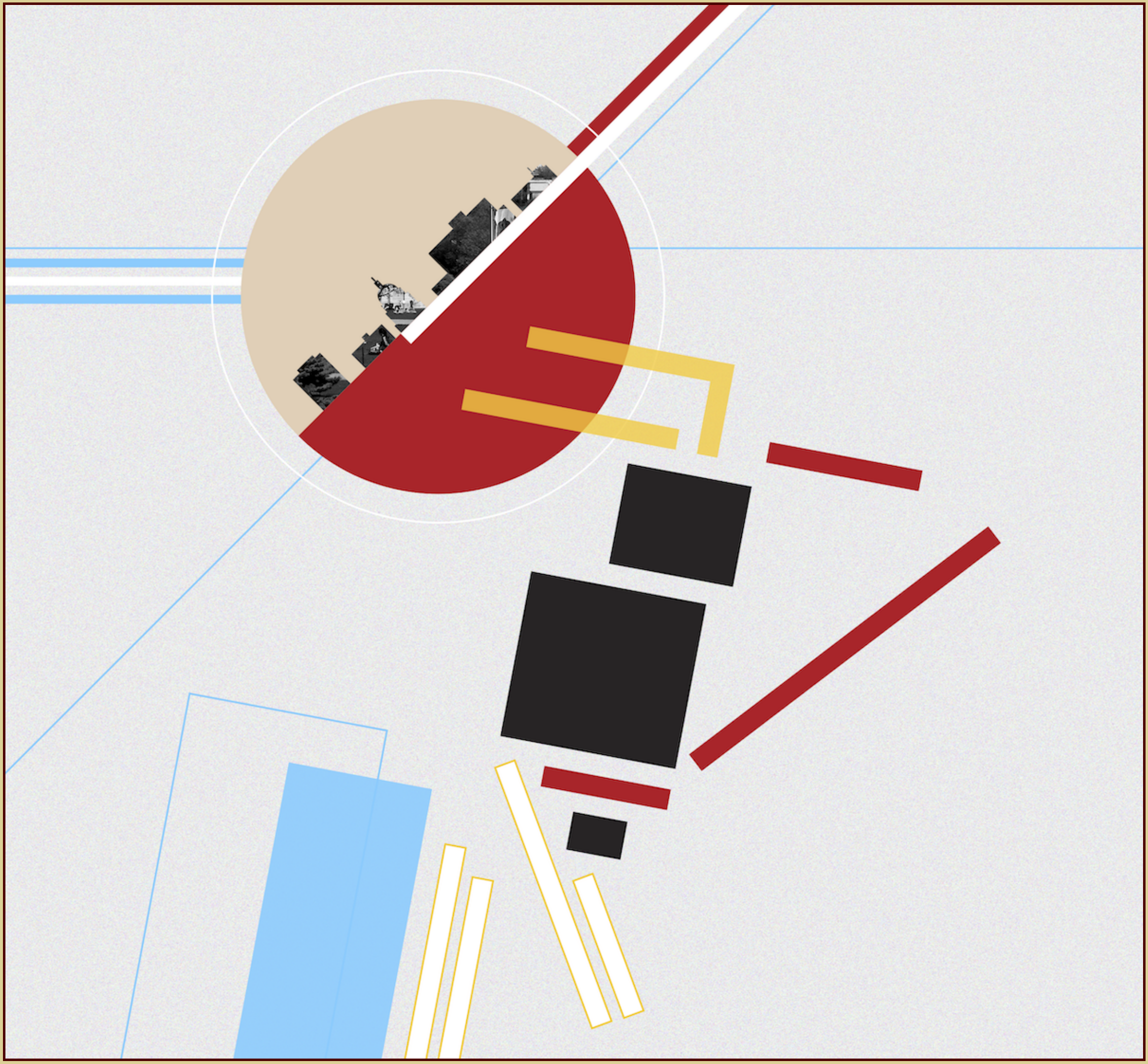
THE OPEN BOOK SERIES 2

ANTS XIII
Proceedings of the Thirteenth
Algorithmic Number Theory Symposium

Computation of triangular integral bases

Jens-Dietrich Bauch and Ha Thanh Nguyen Tran



msp

THE OPEN BOOK SERIES **2** (2019)
Thirteenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2019.2.69

Computation of triangular integral bases

Jens-Dietrich Bauch and Ha Thanh Nguyen Tran

Let A be a Dedekind domain, K the fraction field of A, and $f \in A[x]$ a monic irreducible separable polynomial. For a given nonzero prime ideal $\mathfrak{p}$ of A we present in this paper a new algorithm to compute a triangular $\mathfrak{p}$-integral basis of the extension L of K determined by f. This approach can be easily adapted to compute a triangular $\mathfrak{p}$-integral basis of fractional ideals I of the integral closure of A in L. Along this process one can compute $\mathfrak{p}$-integral bases for a family of ideals contained in I as a by-product.

Introduction

In computational number theory one of the most important examples for a Dedekind domain is the ring of integers $\mathcal{O}$ of a number field $L = \mathbb{Q}(\theta)$, where θ is the root of a monic irreducible polynomial f over $\mathbb{Z}$ of degree n. In that context a set $(b_0, \dots, b_{n-1})$ is called a triangular basis of $\mathcal{O}$ if it generates $\mathcal{O}$ as a $\mathbb{Z}$-module and

$$b_0 = 1 \quad \text{and} \quad b_i = \frac{\theta^i + \sum_{j<i} \lambda_{i,j}\theta^j}{h_i},$$

where $\lambda_{i,j}, h_i \in \mathbb{Z}$ and $1 \le i \le n-1$. For a module over a PID, a triangular basis always exists. For instance, in the case $L = \mathbb{Q}(\sqrt{5})$ we have

$$\mathcal{O} = \left\langle 1, \frac{\sqrt{5}+1}{2} \right\rangle_{\mathbb{Z}}.$$

Let p be a prime and let $\mathfrak{p} = p\mathbb{Z}$ be the prime ideal generated by p. A triangular $\mathfrak{p}$-integral basis of $\mathcal{O}$ is a triangular basis of $\mathcal{O}$ considered as module over the localization of $\mathbb{Z}$ at $\mathfrak{p}$. In the latter example we see a $\mathfrak{p}$-integral triangular basis of $\mathcal{O}$ with $\mathfrak{p} = 2\mathbb{Z}$, which is already an integral basis.

In [5, p. 217] the computation of an integral basis of a number field L is considered one of the five main computational problems in number theory. Let $\operatorname{Disc}(f) = \mathcal{L} \cdot \mathcal{S}^2$ be the discriminant of f with $\mathcal{L}, \mathcal{S} \in \mathbb{Z}$ and let $\mathcal{L}$ be square-free. Denote by p a prime dividing $\mathcal{S}$ and set $\mathfrak{p} = p\mathbb{Z}$. One can distinguish in general two approaches for the computation of an integral basis. The first approach is based on the idea

MSC2010: 11Y16, 13B22.
Keywords: $\mathfrak{p}$-integral bases, maximal order, Montes algorithm, Dedekind domain.

of computing kernels of linear maps in order to compute a $\mathfrak{p}$-radical of the order $\mathcal{O}$ and is known as the round two algorithm due to Pohst and Zassenhaus [12]. The second approach is based on constructing certain elements in $\mathcal{O}$ of maximal valuation at the prime ideals lying over $\mathfrak{p}$. The most famous algorithms are the round four algorithm [6; 12], those which are based on the OM-representation [8; 16; 1], and in the context of the computation of integral bases of algebraic function fields those using Puiseux expansion [17; 4]. In general, the second approach needs a prime factor of $\mathcal{S}$ as input. However, Guàrdia and Nart found in [9] a $\mathfrak{p}$-adic algorithm, which does not require a prefactorization of $\mathcal{S}$.

Our algorithm follows the approach from [16] and is based on simple linear algebra after a $\mathfrak{p}$-adic initialization step.

Let A be a Dedekind domain, K the fraction field of A, and $\mathfrak{p}$ a nonzero prime ideal of A. By $A_\mathfrak{p}$ we denote the localization of A at $\mathfrak{p}$ and we set $k_\mathfrak{p} = A/\mathfrak{p}$. Let $\pi \in \mathfrak{p}$ be a prime element of $\mathfrak{p}$.

Denote by $\theta \in K^{\mathrm{sep}}$ a root of a monic irreducible separable polynomial $f \in A[x]$ of degree n and $L = K(\theta)$ the finite separable extension of K generated by θ. Let $\mathcal{O}$ be the integral closure of A in L and $\mathcal{O}_\mathfrak{p}$ be the integral closure of $A_\mathfrak{p}$ in L. A $\mathfrak{p}$-*integral basis of* $\mathcal{O}$ is an $A_\mathfrak{p}$-basis of $\mathcal{O}_\mathfrak{p}$. In order to determine a $\mathfrak{p}$-integral basis, we compute, for $0 \le i \le n-1$, monic polynomials $g_i(x) \in A[x]$ of degree i such that $g_i(\theta)$ has maximal value with respect to a pseudovaluation ω on L (see equation (1) below). Then a triangular $\mathfrak{p}$-integral basis is obtained by $(g_i(\theta)/\pi^{w(g_i(\theta))} \mid 0 \le i \le n-1)$. The computation of the g_i's can be deduced by straightforward linear algebra, which results in a simple algorithm. The theoretical complexity (counted in the operations in $k_\mathfrak{p}$, see Section 2D) is slower than the current state-of-the-art methods presented in [8; 16; 1]. The running time of the current methods is asymptotically $n^{2+\epsilon}$, whereas the one of our method is cubic in n. However, after an initialization step the running time drops to n^2. One advantage of our algorithm is that it can be adapted to compute integral bases of families of fractional ideals. That is, for calling once our algorithm for a fractional ideal I of $\mathcal{O}$ with $I \supset \mathcal{O}$ we can determine with no extra time $\mathfrak{p}$-integral bases for certain fractional ideals I' contained in I (see Section 3).

In Section 1 we introduce the notation which is needed to explain the main idea of our algorithm in Section 2. Further on we describe the details of our new methods, give an example, and analyze the running time. Finally an application of our algorithm for the computation of $\mathfrak{p}$-integral bases of families of fractional ideals is presented in Section 3.

1. Notation

We keep the notation from the Introduction. Every prime ideal $\mathfrak{p}$ induces a discrete valuation $v_\mathfrak{p} : A \to \mathbb{Z} \cup \{\infty\}$. We denote the completion of K at $\mathfrak{p}$ by $K_\mathfrak{p}$. The valuation $v_\mathfrak{p}$ extends in an obvious way to $K_\mathfrak{p}$. Denote by $\hat{A}_\mathfrak{p}$ the valuation ring of $v_\mathfrak{p}$. Let $S = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ be the set of all prime ideals of $\mathcal{O}$ lying over $\mathfrak{p}$. For each $\mathfrak{P}_i \in S$ we define $L_{\mathfrak{P}_i}$ to be the completion of L at $\mathfrak{P}_i$ and $\mathcal{O}_{\mathfrak{P}_i}$ to be the integral closure of $\hat{A}_\mathfrak{p}$ in $L_{\mathfrak{P}_i}$.

By the classical theorem of Hensel [11] the prime ideals $\mathfrak{P}_i$ are in one-to-one correspondence with the monic irreducible factors $f_{\mathfrak{P}_i}$ of f in $\hat{A}_\mathfrak{p}[x]$. For each $i \in \{1, \dots, s\}$ denote by θ_i a root and by n_i

the degree of $f_{\mathfrak{P}_i}$. Then we can represent $L_{\mathfrak{P}_i}$ as $L_{\mathfrak{P}_i} = K_{\mathfrak{p}}(\theta_i)$ and define the injection $\iota_i : L \to L_{\mathfrak{P}_i}$ via $\theta \mapsto \theta_i$. In particular, $\sum_{1\le i\le s} n_i = n$ since $f = \prod_{1\le i\le s} f_{\mathfrak{P}_i} \in \hat{A}_{\mathfrak{p}}[x]$.

Denote by $\operatorname{Max}(\mathcal{O})$ the set of all maximal ideals of $\mathcal{O}$. As $\mathcal{O}$ is a Dedekind domain every nonzero fractional ideal I of $\mathcal{O}$ can be factored into a finite product of prime ideals,

$$I = \prod_{\mathfrak{P}\in\operatorname{Max}(\mathcal{O})} \mathfrak{P}^{a_{\mathfrak{P}}},$$

with integer exponents $a_{\mathfrak{P}}$. Any fractional ideal can be considered as a free A-module of rank n.

Definition 1.1 (index). Let M and M' be two free A-modules of rank n. The *index* $[M : M']$ is defined to be the nonzero fractional ideal generated by the determinant of the transition matrix from an A-basis of M' to one of M.

2. Computation of $\mathfrak{p}$-integral bases

The goal of this section is to describe an algorithm that computes a triangular $\mathfrak{p}$-integral basis of $\mathcal{O}$ for a fixed nonzero prime ideal $\mathfrak{p}$ of A. In particular, we compute $b_0, \dots, b_{n-1}$ in L such that $\mathcal{O}_{\mathfrak{p}} = \langle b_0, \dots, b_{n-1}\rangle_{A_{\mathfrak{p}}}$ and

$$b_i = \frac{g_i(\theta)}{\pi^{m_i}}$$

for some monic polynomial $g_i \in A[x]$ of degree i and $m_i \in \mathbb{Z}_{\ge 0}$.

2A. ***The algorithm.*** For $\mathfrak{P}_i \in S$, let $e_{\mathfrak{P}_i}$ be the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$ and $v_{\mathfrak{P}_i}$ be the induced discrete valuation on L. Then we define a pseudovaluation on L as

$$\omega = \left\lfloor \min_{1\le i\le s} \left\{ \frac{v_{\mathfrak{P}_i}}{e_{\mathfrak{P}_i}} \right\} \right\rfloor. \tag{1}$$

Definition 2.1. The monic polynomial $g(x) \in A[x]$ of degree $i < n$ is called *i-maximal* if $\omega(g(\theta)) \ge \omega(h(\theta))$ for all monic polynomials $h \in A[x]$ having the same degree as g.

Our algorithm is based on the following theorem [16, Theorem 1.4]:

Theorem 2.2. *Let* $b_0, \dots, b_{n-1} \in L$, *where*

$$b_i = \frac{g_i(\theta)}{\pi^{\omega(g_i(\theta))}}, \quad g_i \text{ is } i\text{-maximal}. \tag{2}$$

Then $(b_0, \dots, b_{n-1})$ *is a triangular* $\mathfrak{p}$*-integral basis.*

In particular the theorem guarantees the existence of a triangular $\mathfrak{p}$-integral basis.

According to Theorem 2.2 we have to determine i-maximal polynomials $g_i(x) \in A[x]$ for $0 \le i \le n-1$. We start with $g_i = x^i$ and successively replace g_i by a monic polynomial g_i' having degree i with $\omega(g_i'(\theta)) > \omega(g_i(\theta))$. One can compute g_i' by applying an *augmentation-step* defined as follows. Let $\mathcal{R} \subset A$ be a fixed system of representatives of $k_{\mathfrak{p}} = A/\mathfrak{p}$.

Definition 2.3. Let $c_0, \dots, c_m$ be in L, ordered by nondecreasing ω-value, and $\lambda_1, \dots \lambda_m \in \mathcal{R}$ such that

$$\omega\left(c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j\right) > \omega(c_m).$$

Then we call $c_m^* = c_m + \sum_{j=0}^{m-1} \lambda_j \pi^{\omega(c_m)-\omega(c_j)} c_j$ an *augmentation-step*.

In particular an augmentation-step increases the module spanned by the vectors:

$$\left\langle \frac{c_0}{\pi^{\omega(c_0)}}, \dots, \frac{c_m^*}{\pi^{\omega(c_m^*)}} \right\rangle_{A_\mathfrak{p}} \supsetneq \left\langle \frac{c_0}{\pi^{\omega(c_0)}}, \dots, \frac{c_m}{\pi^{\omega(c_m)}} \right\rangle_{A_\mathfrak{p}}.$$

The process is as follows: As an initial step we set $b_0 = 1$ and consider the vectors b_0, θ. Next, we determine $\lambda_0 \in \mathcal{R}$ to perform an augmentation-step: $d_{1,0} = \theta + \lambda_0$. If $x + \lambda_0$ is not 1-maximal, one finds $\lambda_1 \in \mathcal{R}$ such that $d_{1,1} = d_{1,0} + \lambda_1$ realizes an augmentation-step. After finitely many steps, one can obtain some $d_1 = g_1(\theta)$ such that g_1 is 1-maximal. We set $b_1 = d_1/\pi^{\omega(d_1)}$.

Let $1 \le i \le n-1$ and assume we already have computed $b_0, \dots, b_{i-1}$ satisfying (2). After finitely many augmentation-steps we deduce $\lambda_{i,0}, \dots, \lambda_{i,i-1} \in \mathcal{R}$ such that $d_i = \theta^i + \sum_{j<i} \lambda_{i,j} b_j = g_i(\theta)$, where g_i is i-maximal. Let $b_i = d_i/\pi^{\omega(d_i)}$. Then $b_0, \dots, b_i$ are the first $i+1$ vectors in a triangular $\mathfrak{p}$-integral basis. After $n-1$ steps this leads to a triangular $\mathfrak{p}$-integral basis.

We summarize this idea with the pseudocode given in Algorithm 1.

Henceforth we explain how to perform an augmentation-step. We adopt the reduction algorithm from [13; 2] which is used for the computation of Riemann–Roch spaces in the context of algebraic function fields. Because the ω-value is strictly increased at any step, we prefer to use the word augmentation rather than reduction as in [2].

Denote by $\mathcal{B}_i$ an $\hat{A}_\mathfrak{p}$-basis for $\mathcal{O}_{\mathfrak{P}_i}$, which is in particular a $K_\mathfrak{p}$-basis for $L_{\mathfrak{P}_i}$. In addition, denote by v the $\mathfrak{p}$-adic valuation $v_\mathfrak{p}$ extended to a fixed algebraic closure of $K_\mathfrak{p}$ such that $v(x) = 1$ for all $x \in A_\mathfrak{p}^*$. Since $\mathfrak{P}_i$ lies over $\mathfrak{p}$ with ramification index $e_{\mathfrak{P}_i}$, the valuation $v_{\mathfrak{P}_i}$ is an extension of $v_\mathfrak{p}$ and relates to the extension v as follows: $v_{\mathfrak{P}_i}(z) = v(\iota_i(z))e_{\mathfrak{P}_i}$ for any $z \in L$. See [15] for more details.

Algorithm 1: Triangular $\mathfrak{p}$-integral basis

```
Input   : $(1, \theta, \dots, \theta^{n-1})$
Output : A triangular $\mathfrak{p}$-integral basis
$b_0 \leftarrow 1$,   $\mathcal{B} \leftarrow (b_0)$ for $i = 1, \dots, n-1$ do
    $b_i \leftarrow \theta^i$ while possible do
        $b_i \leftarrow b_i + \sum_{j<i} \lambda_j \pi^{\omega(b_i)-\omega(b_j)} b_j$ (augmentation-step)
    $\mathcal{B} \leftarrow$ Append($\mathcal{B}$, $b_i/\pi^{\omega(b_i)}$)
return $\mathcal{B}$
```

For $\alpha \in L_{\mathfrak{P}_i}$ we define by $\mathcal{C}_i(\alpha) \in K_{\mathfrak{p}}^{n_i}$ the coordinate vector of α with respect to the basis $\mathcal{B}_i$ and

$$\iota = (\mathcal{C}_i \circ \iota_i)_{1 \le i \le s} : L \to K_{\mathfrak{p}}^n.$$

Lemma 2.4. *For $z \in L$ it holds that*

$$\omega(z) = \min_{1 \le i \le n} \{v(\zeta_i) \mid \iota(z) = (\zeta_1, \dots, \zeta_n)\}.$$

Proof. For $1 \le i \le s$ we set $w_{\mathfrak{P}_i} = v_{\mathfrak{P}_i}/e_{\mathfrak{P}_i}$. By definition $\omega(z) = \min_{1 \le i \le s} \lfloor w_{\mathfrak{P}_i}(z) \rfloor$; thus it is sufficient to show that

$$\lfloor w_{\mathfrak{P}_i}(z) \rfloor = \min_{b \in \mathcal{B}_i} \{v(\zeta_b)\}, \quad \text{with } \iota_i(z) = \sum_{b \in \mathcal{B}_i} \zeta_b b,$$

for each $1 \le i \le s$. As $v_{\mathfrak{P}_i}(z) = v(\iota_i(z)) e_{\mathfrak{P}_i}$, one has $w_{\mathfrak{P}_i}(z) = v_{\mathfrak{P}_i}(z)/e_{\mathfrak{P}_i} = v(\iota_i(z))$. Since $\mathcal{B}_i$ is an integral basis of $\mathcal{O}_{\mathfrak{P}_i}$ by [1, Theorem 3.2] it holds that $\mathcal{B}_i$ is v-semiorthonormal; that is, $\lfloor v(\iota_i(z)) \rfloor = \lfloor v\big(\sum_{b \in \mathcal{B}_i} \zeta_b b\big) \rfloor = \min_{b \in \mathcal{B}_i} \{v(\zeta_b)\}$. □

Each $\lambda \in K_{\mathfrak{p}}$ can be written as $\lambda = \sum_{j=m}^{\infty} \lambda_j \pi^j$, where $m = v(\lambda)$ and $\lambda_j \in \mathcal{R}$. For an integer $r \ge m$, we set

$$\operatorname{lt}_r(\lambda) = \begin{cases} \lambda_m & \text{if } r = m, \\ 0 & \text{else} \end{cases}$$

and call it the *lower term* of λ at r.

Definition 2.5. Let ψ be a map from L to $K_{\mathfrak{p}}^n$. For $z \in L$ and $r \ge \omega(z)$ we define the *lower-term vector* of z at r (with respect to ψ) by

$$\operatorname{LT}_r(\psi(z)) = (\operatorname{lt}_r(z_i))_{1 \le i \le n} \in k_{\mathfrak{p}}^n,$$

where $\psi(z) = (z_1, \dots, z_n)$.

Recall that $\mathcal{R} \subset A$ is a set of representatives of $k_{\mathfrak{p}} = A/\mathfrak{p}$.

Lemma 2.6. *Let $c_0, \dots, c_m \in L$, ordered by nondecreasing ω-value, and $\alpha_0, \dots, \alpha_m \in \mathcal{R}$, with $\alpha_m \neq 0$, be such that*

$$\sum_{0 \le i \le m} \alpha_i \operatorname{LT}_{\omega(c_i)}(\iota(c_i)) = 0. \tag{3}$$

Then, $c_m^* = c_m + \sum_{j=0}^{m-1} (\alpha_j/\alpha_m) \pi^{\omega(c_m) - \omega(c_j)} c_j$ realizes an augmentation-step.

Moreover, if the $\operatorname{LT}_{\omega(c_i)}(\iota(c_i))$ are $k_{\mathfrak{p}}$-linearly independent, then no augmentation-step is applicable.

Proof. We write $\iota(c_j) = (c_{j,1}, \dots, c_{j,n})$, for $j = 0, \dots, m$. By Lemma 2.4 it holds that $\omega(c_j) = \min_{1 \le i \le n} \{v(c_{j,i})\}$. By construction, one can write

$$\iota(c_j) = \operatorname{LT}_{\omega(c_j)}(\iota(c_j)) \pi^{\omega(c_j)} + \sum_{i > \omega(c_j)} v_{i,j} \pi^i,$$

with $v_{i,j} \in k_\mathfrak{p}^n$. If we identify $k_\mathfrak{p}$ with $\mathcal{R}$, then ι becomes $k_\mathfrak{p}[\pi]$-linear. That is,

$$\iota(c_m^*) = \iota(c_m) + \sum_{j=0}^{m-1} \frac{\alpha_j}{\alpha_m} \pi^{\omega(c_m)-\omega(c_j)} \iota(c_j).$$

The fact that $\sum_{0 \le i \le m} \alpha_i \mathrm{LT}_{\omega(c_i)}(\iota(c_i)) = 0$ implies

$$\iota(c_m^*) = \sum_{i > \omega(c_m)} v_i \pi^i = (c_{m,1}^*, \dots, c_{m,n}^*),$$

with vectors $v_i \in k_\mathfrak{p}^n$. Accordingly, for $\iota(c_m^*) = (c_{m,1}^*, \dots, c_{m,n}^*)$ it holds that $v(c_{m,i}^*) > \omega(c_m)$ for $i = 1, \dots, n$. Therefore $\omega(c_m^*) > \omega(c_m)$ by Lemma 2.4.

On the other hand, any augmentation-step implies that $\{\mathrm{LT}_{\omega(c_i)}(\iota(c_i))\}_{i=0,\dots,m}$ are $k_\mathfrak{p}$-linearly dependent. □

Theorem 2.7. *Algorithm* 1 *terminates after a finite number of steps and computes a triangular* $\mathfrak{p}$*-integral basis.*

Proof. Any augmentation-step in Algorithm 1 is performed such that the resulting element b_i is of the form $g_i(\theta)/\pi^{m_i}$ with $g_i(x) \in A[x]$ monic of degree i and $m_i = \omega(g_i(\theta))$ for $0 \le i \le n-1$. After any augmentation-step, one of the m_i strictly increases. Every m_i is bounded by the $\mathfrak{p}$-valuation of the index $[\mathcal{O} : A[\theta]]$; hence after finitely many steps g_i is i-maximal for $0 \le i \le n-1$. Consequently, Algorithm 1 outputs $(g_i(\theta)/\pi^{m_i})_{0 \le i \le n-1}$, which is a triangular $\mathfrak{p}$-integral basis according to Theorem 2.2. □

2B. ***Algorithmic details.*** In this subsection we give a detailed realization of Algorithm 1. The bottleneck is the computation of $\iota(\theta^j) \in K_\mathfrak{p}^n$ for $j = 0, \dots, n-1$. The components of the vector $\iota(\theta^j)$ are in general infinite power series in π with coefficients in $k_\mathfrak{p}$ and cannot be exactly represented in the machine. It is however sufficient to work with approximations. In fact one can write

$$\iota(\theta^j) = \sum_{i=\omega(\theta^j)}^{\infty} v_i \pi^i,$$

where $v_i \in k_\mathfrak{p}^n$ and $v_{\omega(\theta^j)} = \mathrm{LT}_{\omega(\theta^j)}(\iota(\theta^j))$. In practice we work with $\iota(\theta^j) \pmod{\pi^\nu} \equiv \sum_{i=\omega(\theta^j)}^{\nu-1} v_i \pi^i$, where $\nu > \omega(\theta^j)$ has to be chosen such that Algorithm 1 still outputs a triangular $\mathfrak{p}$-integral basis.

First we consider a realization of the computation of $\iota(\theta^j) \pmod{\pi^\nu}$ and later we discuss how to choose ν.

Let $\Phi_i(x) \in A[x]$ be an approximation to $f_{\mathfrak{P}_i}(x)$ with precision $\nu \in \mathbb{Z}$; that is, Φ_i is monic and irreducible (over $\hat{A}_\mathfrak{p}$) such that

$$f_{\mathfrak{P}_i} \equiv \Phi_i \pmod{\pi^\nu}. \tag{4}$$

Moreover, every approximation Φ_i defines a finite extension L_{Φ_i} of K. We denote by $\tilde{\theta}_i$ a root of Φ_i such that $L_{\Phi_i} = K(\tilde{\theta}_i)$ and define the map $\iota_{i,\nu}$ via $\theta \mapsto \tilde{\theta}_i$.

Recall that $\mathcal{B}_i$ denotes an integral basis for the completion $L_{\mathfrak{P}_i}$. Every $b \in \mathcal{B}_i$ can be written as $b = g(\theta_i)/\pi^{l_b}$, with $g(x) \in \hat{A}_{\mathfrak{p}}[x]$ and $l_b \in \mathbb{Z}$ minimal. Let $g_\nu(x) \in A[x]$ be the polynomial obtained by reducing the coefficients of g modulo π^ν. This allows us to define $b_\nu = g_\nu(\tilde{\theta_i})/\pi^{l_b} \in L_{\Phi_i}$.

Lemma 2.8. *For* $\nu > \max\{l_b \mid b \in \mathcal{B}_i\}$, *the set* $\mathcal{B}_{i,\nu} = \{b_\nu \mid b \in \mathcal{B}_i\}$ *is a* $\mathfrak{p}$*-integral basis of* L_{Φ_i}.

Proof. Denote by $\mathcal{O}_i$ the integral closure of A in L_{Φ_i}. Since Φ_i is irreducible over $\hat{A}_{\mathfrak{p}}$ there exists only one prime ideal $\widetilde{\mathfrak{P}}_i$ of $\mathcal{O}_i$ over $\mathfrak{p}$. Here $b = g(\theta_i)/\pi^{l_b}$ for all $b \in \mathcal{B}_i$ as above. By the choice of ν we have $v_{\widetilde{\mathfrak{P}}_i}(g_\nu(\tilde{\theta_i})/\pi^{l_b}) \geq 0$ and b_ν is integral. As a consequence $\mathcal{B}_{i,\nu} \subset \mathcal{O}_i$. Now it is enough to show that $\mathcal{B}_{i,\nu}$ generates $\mathcal{O}_i$ but this is directly inherited from $\mathcal{B}_i$. □

For $z \in L_{\Phi_i}$ we denote by $C_{\mathcal{B}_{i,\nu}}(z) \in K^{n_i}$ the coordinate vector of z with respect to the basis $\mathcal{B}_{i,\nu}$. Then we can define the map

$$\tilde{\iota}_\nu : L \to K^n, \quad z \mapsto (C_{\mathcal{B}_{i,\nu}}(\iota_{i,\nu}(z)))_{1 \leq i \leq s}.$$

Lemma 2.9. *For* $z \in L$ *and a positive integer* ν *it holds*

$$\iota(z) \pmod{\pi^\nu} \equiv \tilde{\iota}_\nu(z).$$

Proof. The elements b_ν in $\mathcal{B}_{i,\nu}$ are obtained by taking the coefficients of $b \in \mathcal{B}_i$ modulo π^ν. Therefore, it is sufficient to show that $\iota_i(z)$ and $\iota_{i,\nu}(z)$ are the same modulo π^ν for all $z \in L$, for all $1 \leq i \leq s$. Any element $z \in L$ can be written as $z = g(\theta)/h$ with $g(x) \in A[x]$ and $h \in A$. Thus, we may restrict our consideration to elements $g(\theta)$.

Given an index i and a polynomial $g(x) \in A[x]$, we will show that $\iota_i(g(\theta)) = g(\theta_i)$ and $\iota_{i,\nu}(g(\theta)) = g(\tilde{\theta_i})$ coincide modulo π^ν. We consider $g(\theta_i)$ to be the class of g in $A_{\mathfrak{p}}[x]/f_{\mathfrak{P}_i}A_{\mathfrak{p}}[x]$ and $g(\tilde{\theta_i})$ to be the one of g in $A_{\mathfrak{p}}[x]/\Phi_i A_{\mathfrak{p}}[x]$. Then the statement follows immediately by the fact that

$$f_{\mathfrak{P}_i} \pmod{\pi^\nu} \equiv \Phi_i$$

by the definition of the approximation Φ_i. □

Theorem 2.10. *Let* ν *be an integer with* $\nu \geq v_{\mathfrak{p}}([\mathcal{O} : A[\theta]])$. *If we replace in the augmentation-steps along Algorithm* 1 *the map* ι *by* $\tilde{\iota}_\nu$ *then the algorithm outputs a triangular* $\mathfrak{p}$*-integral basis and needs at most* $v_{\mathfrak{p}}([\mathcal{O} : A[\theta]])$ *augmentation-steps.*

Proof. For a triangular $\mathfrak{p}$-integral basis $(b_0, \ldots, b_{n-1})$ with $b_i = g_i(\theta)/\pi^{\omega(g_i(\theta))}$ we have

$$\sum_{0 \leq i \leq n-1} \omega(g_i(\theta)) = v_{\mathfrak{p}}([\mathcal{O} : A[\theta]]).$$

Algorithm 1 produces b_i with g_i being i-maximal by applying augmentations-steps. Note that any of these steps increases the ω-value by at least 1. Consequently, after maximally $v_{\mathfrak{p}}([\mathcal{O} : A[\theta]])$ steps, the algorithm outputs a $\mathfrak{p}$-integral basis.

For the first statement we assume that the precision $\nu \geq v_{\mathfrak{p}}([\mathcal{O} : A[\theta]])$ is not sufficient. That is Algorithm 1 outputs $b_0, \ldots, b_{n-1}$, which is not a $\mathfrak{p}$-integral basis, at precision $\nu \geq v_{\mathfrak{p}}([\mathcal{O} : A[\theta]])$. Hence there are still augmentation-steps applicable to $b_0, \dots, b_{n-1}$, which have not been detected because of the too-low precision. This implies that the lower-term vectors

$$\mathrm{LT}_{\omega(b_0)}(\tilde{\iota}_\nu(b_0)), \dots, \mathrm{LT}_{\omega(b_{n-1})}(\tilde{\iota}_\nu(b_{n-1}))$$

are linearly dependent by Lemma 2.6. In particular, for at least one $0 \le i \le n-1$ the lower-term vector $\mathrm{LT}_{w(b_i)}(\tilde{\iota}_\nu(b_i))$ is zero. Then $b_i = g_i(\theta)/\pi^{w(g_i(\theta))}$ satisfies

$$\iota(g_i(\theta)) = \sum_{j \ge \nu} v_{i,j}\pi^j, \qquad v_{i,j} \in k_{\mathfrak{p}}^n.$$

In particular we have $\omega(g_i(\theta)) \ge \nu$, which leads to the contradiction

$$\nu \ge v_{\mathfrak{p}}([\mathcal{O} : A[\theta]]) > v_{\mathfrak{p}}([\langle b_0, \dots, b_{n-1}\rangle_A : A[\theta]]) = \sum_{0 \le i \le n-1} w(g_i(\theta)) \ge \nu. \qquad \square$$

2C. ***Example.*** Let $f = x^4 + 4x^3 + (4t^2+4)x^2 + 8t^2x + 2t^8 + 4t^4 + 8t^2 \in A[x]$ with $A = \mathbb{F}_{13}[t]$ and let L be the function field defined by f. Then $\mathrm{Disc}(f) = \mathcal{L} \cdot \mathcal{S}^2$ with $\mathcal{S} = t^2(t^3+3)(t^3+10)$. Let $\pi = t$ and $\mathfrak{p} = \pi \cdot A$. Then we want to compute a $\mathfrak{p}$-integral basis. Here $\mathfrak{p}\mathcal{O} = \mathfrak{P}_1 \cdot \mathfrak{P}_2$, and the ramification indices satisfy $e_{\mathfrak{P}_1} = e_{\mathfrak{P}_2} = 1$. Moreover f splits into $f = f_{\mathfrak{P}_1} \cdot f_{\mathfrak{P}_2}$ over $\hat{A}_{\mathfrak{p}} = \mathbb{F}_{13}[\![t]\!]$ with $\deg f_{\mathfrak{P}_1} = \deg f_{\mathfrak{P}_2} = 2$. First, one can compute approximations $\Phi_1 = x^2 + 2t^2$ and $\Phi_2 = x^2 + 4x + 2t^2 + 4$ of $f_{\mathfrak{P}_1}$ and $f_{\mathfrak{P}_2}$ with precision $\nu = 8$ using the Montes algorithm [10]. This precision is sufficient according to Theorem 2.10 because $\nu = 8 > v_{\mathfrak{p}}(\mathrm{Disc}(f)) = 4 \ge v_{\mathfrak{p}}([\mathcal{O} : A[\theta]])$. Let θ_i be a root of $f_{\mathfrak{P}_i}$ and $\tilde{\theta}_i$ be one root of Φ_i for $i = 1, 2$ respectively.

Next, we compute

$$\mathcal{B}_1 = (1, \tilde{\theta}_1/t), \quad \mathcal{B}_2 = (1, (\tilde{\theta}_2+2)/t),$$

$\mathfrak{p}$-integral bases for L_{Φ_1} and L_{Φ_2}, respectively, as explained in [7]. Note that $(1, \theta_1/t)$ and $(1, (\theta_2+2)/t)$ are integral bases for $L_{\mathfrak{P}_1}$ and $L_{\mathfrak{P}_2}$. We compute $\tilde{\iota}_\nu(\theta^j)$ for $0 \le j \le 3$ as follows. First, we obtain $\iota_{i,\nu}(\theta^j)$ by computing $x^j \pmod{\Phi_i}$. Second, we evaluate it in $\tilde{\theta}_i$ and take its coefficients with respect to $\mathcal{B}_i$ for $i = 1, 2$. This process leads to the following matrix:

$$\begin{array}{c|cc:cc|c}
 & \multicolumn{2}{c:}{\mathcal{B}_1} & \multicolumn{2}{c|}{\mathcal{B}_2} & \omega \\
\hline
\tilde{\iota}_\nu(1) & \underline{1} & 0 & \underline{1} & 0 & 0 \\
\tilde{\iota}_\nu(\theta) & 0 & t & \underline{11} & t & 0 \\
\tilde{\iota}_\nu(\theta^2) & 11t^2 & 0 & 11t^2+\underline{4} & 9t & 0 \\
\tilde{\iota}_\nu(\theta^3) & 0 & 11t^3 & 12t^2+\underline{5} & 11t^3+12t & 0
\end{array}$$

The rows of the 4×4 submatrix represent the vectors $\tilde{\iota}_\nu(\theta^j)$ for $j = 0, \dots, 3$. The last column shows the value $\omega(\theta^j)$. The underlined entries of the submatrix are those which attain the minimum; that is, their v_t-valuation coincides with the ω-value of the corresponding row.

We consider the lower-term vectors in order to perform augmentation-steps:

$$M=\begin{bmatrix}\mathrm{LT}_0(\tilde{\iota}_\nu(1))\\ \vdots\\ \mathrm{LT}_0(\tilde{\iota}_\nu(\theta^3))\end{bmatrix}=\begin{bmatrix}\underline{1}&0&\underline{1}&0\\ 0&0&\underline{11}&0\\ 0&0&\underline{4}&0\\ 0&0&\underline{5}&0\end{bmatrix}\in\mathbb{F}_{13}^{4\times 4}.$$

Since $\operatorname{rank}(M)=2<4$, one can apply augmentation-steps. We have $\mathrm{LT}_0(\tilde{\iota}_\nu(\theta^2))+2\mathrm{LT}_0(\tilde{\iota}_\nu(\theta))=0\in\mathbb{F}_{13}^4$ and $\mathrm{LT}_0(\tilde{\iota}_\nu(\theta^3))+9\mathrm{LT}_0(\tilde{\iota}_\nu(\theta))=0\in\mathbb{F}_{13}^4$. By Lemma 2.6 we can read out the augmentation-steps from M and deduce $b_2^*=\theta^2+2\theta$ and $b_3^*=\theta^3+9\theta$. This results in

	$\mathcal{B}_1$		$\mathcal{B}_2$		ω
$\tilde{\iota}_\nu(1)$	$\underline{1}$	0	$\underline{1}$	0	0
$\tilde{\iota}_\nu(\theta)$	0	t	$\underline{11}$	t	0
$\tilde{\iota}_\nu(b_2^*)$	$11t^2$	$\underline{2}t$	$11t^2$	$\underline{11}t$	1
$\tilde{\iota}_\nu(b_3^*)$	0	$11t^3+\underline{9}t$	$12t^2$	$11t^3+\underline{8}t$	1

(5)

with $\omega(b_2^*)=\omega(b_3^*)=1$. We again check the lower-term vectors in order to see if another augmentation-step can be applied:

$$M=\begin{bmatrix}\mathrm{LT}_0(\tilde{\iota}_\nu(1))\\ \mathrm{LT}_0(\tilde{\iota}_\nu(\theta))\\ \mathrm{LT}_1(\tilde{\iota}_\nu(b_2^*))\\ \mathrm{LT}_1(\tilde{\iota}_\nu(b_3^*))\end{bmatrix}=\begin{bmatrix}\underline{1}&0&\underline{1}&0\\ 0&0&\underline{11}&0\\ 0&\underline{2}&0&\underline{11}\\ 0&\underline{9}&0&\underline{8}\end{bmatrix}.$$

Now $\operatorname{rank}(M)=4$, so no further augmentation is applicable. That is,

$$\left(1,\theta,\frac{\theta^2+2\theta}{t},\frac{\theta^3+9\theta}{t}\right)$$

is a $\mathfrak{p}$-integral basis.

2D. *Complexity.* For the subsequent complexity analysis we define $\delta:=v_{\mathfrak{p}}(\operatorname{Disc} f)$, the $\mathfrak{p}$-valuation of the discriminant of f. Furthermore we admit fast multiplication techniques of Schönhage and Strassen [14]. Let R be a ring and $g_1,g_2\in R[x]$ be two polynomials whose degrees are bounded by d_1 and d_2, respectively. Then, the multiplication $g_1\cdot g_2$ requires $O(\max\{d_1,d_2\}^{1+\epsilon})$ operations in R. Algorithm 1 works well with precision $\nu=\delta$ by Theorem 2.10. Thus, one may consider the elements in A to be finite π-adic developments whose length is equal to $O(\delta)$. We fix a system of representatives $\mathcal{R}$ of $k_{\mathfrak{p}}=A/\mathfrak{p}$ and call an operation in A $\mathfrak{p}$-*small* if it involves two elements belonging to $\mathcal{R}$. Hence, any multiplication in A can be performed with $O(\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations. We assume the residue field $A/\mathfrak{p}$ is finite with q elements.

The total cost of Algorithm 1 is obtained by adding all the costs from Lemma 2.14 and 2.15 as below.

Theorem 2.11. *Algorithm* 1 *requires*

$$O(n^3\delta+n^2\delta^2+n^{1+\epsilon}\delta\log q+n^{1+\epsilon}\delta^{2+\epsilon})$$

$\mathfrak{p}$-*small operations. In particular, the running time after the initialization is equal to* $O(n^2\delta^2)$ $\mathfrak{p}$-*small operations.*

Although the complexity depends asymptotically on n^3, in practice the running time is less pessimistic. The factor n^3 is due to the Gaussian elimination process in the initialization step (1b). We have to invert an $n \times n$ matrix T' with entries in A (see Lemma 2.13 for more details). If $\mathfrak{p}\mathcal{O}$ is a prime ideal then T' is a triangular matrix. In fact the less factors $\mathfrak{p}\mathcal{O}$ has, the more T' looks like a triangular matrix. In that case inverting T' can be performed quickly and the algorithm is practical for large n.

The following steps dominate the running time of Algorithm 1:

(1) Initialization:

- (a) Computation of approximations Φ_i and local bases $\mathcal{B}_i$ for $1 \le i \le s$.
- (b) Computing the vectors $(C_{\mathcal{B}_i}(\iota_{i,\nu}(\theta^j)))_{1 \le i \le s}$ for $0 \le j \le n-1$.

(2) Realization of augmentation-steps:

- (a) Determining the coefficients in the linear relation from (3).
- (b) Performing the augmentation-step.

For the initialization step we use the Montes algorithm [3; 7] to compute approximations Φ_i and the $\mathfrak{p}$-integral basis $\mathcal{B}_i$ of L_{Φ_i}. Details can be found in [10; 1].

2D1. *Initialization.* (a) The Montes algorithm has a cost of $O(n^{2+\epsilon} + n^{1+\epsilon}\delta \log q + n^{1+\epsilon}\delta^{2+\epsilon})$ operations [3]. Once we have called the Montes algorithm we determine the bases $\mathcal{B}_i$ as explained in [1]. The complexity of computing all bases is equal to $O(n^{2+\epsilon}\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations.

According to [3, Theorem 5.16], the cost of the computation of an approximation Φ_i of $f_{\mathfrak{P}_i}$ with precision ν is given by

$$O(nn_i\nu^{1+\epsilon} + n\delta^{1+\epsilon})$$

$\mathfrak{p}$-small operations, where $n_i = \deg \Phi_i$. As a result of Theorem 2.10 a sufficient precision is equal to $O(\delta)$. Since $\sum_{i=1}^{s} n_i = n$, the cost of computing all approximations is equal to $O(n^2\delta^{1+\epsilon})$.

(b) Let T be the matrix with rows given by $\tilde{\iota}_\nu(\theta^i)$. We analyze the cost of determining T. First we consider $\iota_{i,\nu}(\theta^j)$ for $1 \le i \le s$ and $0 \le j \le n-1$, and then $C_{\mathcal{B}_i}(\iota_{i,\nu}(\theta^j))$. Recall that $\tilde{\theta}_i$ is a root of Φ_i such that $L_{\Phi_i} = K(\tilde{\theta}_i)$ for $1 \le i \le s$.

Lemma 2.12. *The cost of computing $\iota_{i,\nu}(\theta^j)$ for $1 \le i \le s$ and $0 \le j \le n-1$ is equal to $O(n^2\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations.*

Proof. Clearly, $\iota_{i,\nu}(\theta^j)$ is equal to $x^j \pmod{\Phi_i}$ evaluated in $\tilde{\theta}_i$. For $j < n_i = \deg \Phi_i$ we have $\iota_{i,\nu}(\theta^j) = \tilde{\theta}_i^j$.

When $j = n_i$, let $\psi_{n_i} = x^{n_i} - \Phi_i$. Then $x^{n_i} = \psi_{n_i} + \Phi_i$. Therefore $\iota_{i,\nu}(\theta^{n_i}) = \psi_n(\tilde{\theta}_i)$, which can be computed at no cost.

Assume $j \ge n_i$ and that we have computed $\psi_j = \alpha_{n_i-1}x^{n_i-1} + \cdots + \alpha_0 \in A[x]$, where $\psi_j \equiv x^j \pmod{\Phi_i}$. In particular, $x^j = \psi_j + r_j\Phi_i$ with $r_j \in A[x]$. Then it holds

$$\begin{aligned} x^{j+1} = x(\psi_j + r_j\Phi_i) &= \alpha_{n_i-1}x^{n_i} + \cdots + \alpha_0 x + xr_j\Phi_i \\ &= \alpha_{n_i-1}(\psi_{n_i} + \Phi_i) + \alpha_{n_i-2}x^{n_i-1} + \cdots + \alpha_0 x + xr_j\Phi_i \\ &= \psi_{j+1} + r_{j+1}\Phi_i, \end{aligned}$$

where $\psi_{j+1} = \alpha_{n_i-1}\psi_{n_i} + \alpha_{n_i-2}x^{n_i-1} + \cdots + \alpha_0 x$ and $r_{j+1} = (\alpha_{n_i-1} + xr_j)\Phi_i$. As a consequence, one can compute ψ_{j+1} with at most n_i multiplications and additions in A. Then $\iota_{i,\nu}(\theta^{j+1}) = \psi_{j+1}(\tilde{\theta}_i)$. Since the precision is $\nu = O(\delta)$, it is enough to perform this computation modulo π^ν. For this reason, the computation of $\iota_{i,\nu}(\theta^j)$ for $j = 0, \dots, n-1$ can be performed in $O(nn_i\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations. Because i runs from 1 to s and $n_i = \deg(\Phi_i)$ satisfies $\sum_{i=1}^{s} n_i = n$, computing $\iota_{i,\nu}(\theta^j)$ for $1 \le i \le s$ and $0 \le j \le n-1$ can be done in $O(n^2\delta^{1+\epsilon})$ $\mathfrak{p}$-small operations. □

Lemma 2.13. *The cost of computing the coordinates of the vectors $\iota_{i,\nu}(\theta^j)$ with respect to the basis $\mathcal{B}_i$ is equal to $O(n^3\delta)$ $\mathfrak{p}$-small operations.*

Proof. Let $W = \prod_{i=1}^{s} L_{\Phi_i}$ and $\kappa_i : L_{\Phi_i} \to W$ be the canonical embedding of L_{Φ_i} into W:

$$z \mapsto (0, \dots, 0, \underbrace{z}_{i\text{-th}}, 0, \dots, 0).$$

Then $\mathcal{B} = \bigcup_{i=1,\dots,s} \kappa_i(\mathcal{B}_i)$ and $\mathcal{B}' = \{\kappa_i(\tilde{\theta}_i^j) \mid 1 \le i \le s,\ 0 \le j \le n_i\}$ are both K-bases of W. In particular, T is the basis change matrix from $\mathcal{B}'$ to $\mathcal{B}$. Since $n_i = \deg \Phi_i$ and $\sum_i n_i = n$, the bases $\mathcal{B}$ and $\mathcal{B}'$ both have n elements. In particular T is an $n \times n$ matrix. One computes T by inverting T', the matrix whose rows are the coefficients of the vectors in $\mathcal{B}$ with respect to $\mathcal{B}'$. Clearly T' can be computed at zero cost since it can be read off from the coefficients of the elements in $\mathcal{B}_i$.

As we work with precision $\nu = O(\delta)$ we may assume that the coefficients of $\iota_{i,\nu}(\theta^j) \in A[\hat{\theta}_i]$ are polynomials in $k_{\mathfrak{p}}[\pi]$ of degree $O(\delta)$ for $0 \le j \le n-1$. Accordingly inverting T' can be done by $O(n^3\delta)$ $\mathfrak{p}$-small operations by Gaussian elimination. □

Adding all the costs leads to the following result.

Lemma 2.14. *The cost for the initialization step is*

$$O(n^3\delta + n^2\delta^{1+\epsilon} + n^{1+\epsilon}\delta \log q + n^{1+\epsilon}\delta^{2+\epsilon}) \tag{6}$$

$\mathfrak{p}$-*small operations.*

2D2. *Augmentation-steps.*

Lemma 2.15. *The cost of the augmentation-steps is $O(n^2\delta^2)$ $\mathfrak{p}$-small operations.*

Proof. Let $\mathcal{B}$ be the set manipulated along Algorithm 1. We determine the coefficients α_b for $b \in \mathcal{B}$ from (3) by solving a system of linear equations over $k_{\mathfrak{p}}$ represented by the lower-term matrix M whose rows are given by $\mathrm{LT}_{\omega(b)}(\tilde{\iota}_\nu(b))$ for $b \in \mathcal{B}$. Note that one can obtain M by taking the lower-term matrix M' from the previous augmentation-step and refreshing or replacing the last row. Both matrices have at most n rows and n columns with entries in $k_{\mathfrak{p}}$. If we have stored M' in row echelon form we can transform M into row echelon form and read out the coefficients for the augmentation-steps in $O(n^2)$ operations. After determining the coefficients α_b for $b \in \mathcal{B}$ from (3), one will apply the augmentation-steps to $\mathcal{B}$ and T; that is, one computes a linear combination of the form $\sum_{b\in\mathcal{B}} \alpha_b \pi^{r_b} b$ with $r_b \in \mathbb{Z}_{\ge 0}$ and then applies the same combinations to the corresponding rows of T. We assume that the coefficients of the elements in $\mathcal{B}$ and the entries in T are represented π-adicly. Then, the multiplication by a π-power is just a shift of the coefficients and its cost can be neglected. Consequently, an augmentation-step can be seen as a $k_\mathfrak{p}$-linear combination of the vectors in $\mathcal{B}$ or the rows of T, respectively.

By Theorem 2.10 we can work out all computations with precision $\nu = O(\delta)$. Thus the entries in T can be considered modulo π^ν and therefore as polynomials in $k_\mathfrak{p}[\pi]$ of degree bounded by δ. Moreover the elements $b \in \mathcal{B}$ are given by $b = g(\theta)/\pi^{\omega(g(\theta))}$ with $g(x) \in (A/\pi^\delta A)[x]$. Therefore any augmentation-step can be performed by $O(n^2\delta)$ $\mathfrak{p}$-small operations. By Theorem 2.10 the number of all augmentation-steps is bounded by δ. As the result, the total cost of all augmentation-steps is equal to $O(n^2\delta^2)$ $\mathfrak{p}$-small operations. □

3. Computing $\mathfrak{p}$-integral bases of families of fractional ideals

Let I be a fractional ideal of $\mathcal{O}$. Since $\mathcal{O}$ is a Dedekind domain, I can be factored into a finite product of prime ideals $I = \prod_{\mathfrak{P}\in\mathrm{Max}(\mathcal{O})} \mathfrak{P}^{a_\mathfrak{P}}$ with integer exponents $a_\mathfrak{P}$. We denote by $I_\mathfrak{p} = \prod_{1\le i\le s} \mathfrak{P}_i^{a_{\mathfrak{P}_i}}$ the $\mathfrak{p}$-part of I. Clearly I and $I_\mathfrak{p}$ are rank-n modules over A. The set $\{b_0, \dots, b_{n-1}\} \subset I$ is called a $\mathfrak{p}$-integral basis of I if $\{b_0, \dots, b_{n-1}\}$ forms an $A_\mathfrak{p}$-basis of $I_\mathfrak{p}$.

In this section we generalize the idea of the computation of a $\mathfrak{p}$-integral basis of $\mathcal{O}$ to the computation of a $\mathfrak{p}$-integral basis of fractional ideals. For any fractional ideal I there exists a maximal integer $a_I \le 0$ such that the ideal $(\mathfrak{p}^{a_I} I_\mathfrak{p})^{-1}$ is integral. We call $I_\mathfrak{p}^* = \mathfrak{p}^{a_I} I_\mathfrak{p}$ the *normalization* of $I_\mathfrak{p}$ and I $\mathfrak{p}$-*normalized* if $I_\mathfrak{p}^* = I_\mathfrak{p}$. Clearly if $\{b_0, \dots, b_{n-1}\}$ is an $A_\mathfrak{p}$-basis of $I_\mathfrak{p}^*$ then $\{\pi^{-a_I} b_0, \dots, \pi^{-a_I} b_{n-1}\}$ is a $\mathfrak{p}$-integral basis of I. Hence it is sufficient to consider only $\mathfrak{p}$-normalized fractional ideals.

3A. *Basis computation of fractional ideals.* Let $I = \prod_{\mathfrak{P}\in\mathrm{Max}(\mathcal{O})} \mathfrak{P}^{a_\mathfrak{P}}$ be a $\mathfrak{p}$-normalized fractional ideal. We define for $z \in L$

$$\omega_I(z) = \left\lfloor \min_{1\le i\le s} \left\{ \frac{v_{\mathfrak{P}_i}(z) - a_{\mathfrak{P}_i}}{e_{\mathfrak{P}_i}} \right\} \right\rfloor.$$

Let $g(x) \in A[x]$ be a monic polynomial of degree $i < n$. Then g is called *i-maximal* in I (or just i-maximal) if $\omega_I(g(\theta)) \ge \omega_I(h(\theta))$ for all monic $h \in A[x]$ having the same degree as g.

One can generalize Theorem 2.2 to the following.

Theorem 3.1. *Let $b_0, \dots, b_{n-1} \in L$ with*

$$b_i = \frac{g_i(\theta)}{\pi^{\omega_I(g_i(\theta))}}, \quad g_i \text{ is } i\text{-maximal in } I;$$

then $(b_0, \dots, b_{n-1})$ is a triangular $\mathfrak{p}$-integral basis of I.

Analogous to Definition 2.3, one can generalize an augmentation-step by replacing ω by ω_I. Then Algorithm 1 can be adapted to compute a $\mathfrak{p}$-integral basis of I with a minor adjustment of the realization of an augmentation-step. Let $I_\mathfrak{p} = \prod_{1\le i\le s} \mathfrak{P}_i^{a_{\mathfrak{P}_i}}$. For $1 \le i \le s$ denote by $\mathcal{B}_i$ an $\hat{A}_\mathfrak{p}$-basis of $\iota_i(\mathfrak{P}_i^{a_{\mathfrak{P}_i}}) \subset L_{\mathfrak{P}_i}$. In particular $\mathcal{B}_i$ is a $K_\mathfrak{p}$-basis of $L_{\mathfrak{P}_i}$. We define by $C_{\mathcal{B}_i}(\alpha) \in K_\mathfrak{p}^{n_i}$ the coordinate vector of $\alpha \in L_{\mathfrak{P}_i}$ with respect to $\mathcal{B}_i$ and

$$\iota_I = (C_{\mathcal{B}_i} \circ \iota_i)_{1\le i\le s} : L \to K_\mathfrak{p}^n.$$

Then Lemma 2.6 and Theorem 2.7 can be stated by replacing ι by ι_I. Similar to Section 2B, one should work with approximations $\Phi_i \in A[x]$ of the irreducible $\mathfrak{p}$-adic factors $f_{\mathfrak{P}_i}$ of f of precision $\nu \in \mathbb{Z}_{>0}$. Analogously we define

$$\iota_{I,\nu} : L \to K^n, \quad z \mapsto (C_{\mathcal{B}_{i,\nu}}(\iota_{i,\nu}(z)))_{1\leq i\leq s}, \tag{7}$$

where $\mathcal{B}_{i,\nu}$ denotes a $\mathfrak{p}$-integral basis of the fractional ideal $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$. One can prove analogously to Lemma 2.9 that $\iota_I(z) \pmod{\pi^\nu} \equiv \iota_{I,\nu}(z)$ for all $z \in L$. Let $1 \leq i \leq s$ and denote by $\mathcal{B}'_{i,\nu}$ a $\mathfrak{p}$-integral basis of L_{Φ_i} the finite extension of K defined by the approximation Φ_i. Then one can easily derive $\mathcal{B}_{i,\nu}$ from $\mathcal{B}'_{i,\nu}$: We consider the fractional ideal $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$ and write

$$a_{\mathfrak{P}_i} = \tilde{a}_{\mathfrak{P}_i} + l_i(-e_{\mathfrak{P}_i}) \quad \text{with } l_i \in \mathbb{Z}_{\geq 0} \text{ and } -e_{\mathfrak{P}_i} < \tilde{a}_{\mathfrak{P}_i} \leq 0. \tag{8}$$

Define $\widetilde{\mathfrak{P}}_i = \iota_{i,\nu}(\mathfrak{P}_i)$. Let $\gamma_i \in L_{\Phi_i}$ be such that $v_{\widetilde{\mathfrak{P}}_i}(\gamma_i) = \tilde{a}_{\mathfrak{P}_i}$. Then, $\mathcal{B}_{i,\nu} = \gamma_i \pi^{-l_i} \cdot \mathcal{B}'_{i,\nu}$ is a $\mathfrak{p}$-integral basis of $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$. Note that one can choose $\gamma_i = \iota_{i,\nu}(\pi_i)^{\tilde{a}_{\mathfrak{P}_i}}$ for a uniformizer π_i of $\mathfrak{P}_i$, which can be computed along the Montes algorithm as a by-product.

Theorem 3.2. *Let $\delta_I = v_{\mathfrak{p}}([I : A[\theta]])$ and ν be an integer with $\nu \geq \delta_I$. If we replace the map ι by $\iota_{I,\nu}$ in the augmentation-steps along Algorithm* 1, *then the algorithm outputs a triangular $\mathfrak{p}$-integral basis of I and needs at most δ_I augmentation-steps. In particular this basis can be computed in*

$$O(n^3\delta_I + n^2\delta_I^2 + n^{1+\epsilon}\delta_I \log q + n^{1+\epsilon}\delta_I^{2+\epsilon})$$

$\mathfrak{p}$-*small operations.*

Proof. Analogous to the proof of Theorem 2.10 one proves the first statement by replacing δ by δ_I. For the complexity statement one proceeds exactly as in Section 2D taking into account that the cost for the computation of $\mathcal{B}_{i,\nu}$ can be neglected as mentioned above. □

3B. ***Computation of bases of families of fractional ideals.*** Let I and I' be two $\mathfrak{p}$-normalized fractional ideals of L with $I'_{\mathfrak{p}} \subset I_{\mathfrak{p}}$. In particular, let $I_{\mathfrak{p}} = \prod_{1\leq i\leq s} \mathfrak{P}^{a_{\mathfrak{P}_i}}$ and $I'_{\mathfrak{p}} = \prod_{1\leq i\leq s} \mathfrak{P}^{a'_{\mathfrak{P}_i}}$ with

$$a_{\mathfrak{P}_i} \equiv a'_{\mathfrak{P}_i} \pmod{e_{\mathfrak{P}_i}}, \quad 1 \leq i \leq s. \tag{9}$$

We explain how to determine a $\mathfrak{p}$-integral basis $\mathcal{B}_{I'}$ of I' along the process of computing a $\mathfrak{p}$-integral basis $\mathcal{B}_I$ of *I*. The basic idea is to run Algorithm 1 with precision δ_I to compute first $\mathcal{B}_{I'}$. Then one just keeps on running the algorithm until $\mathcal{B}_I$ is obtained as below.

Assume that approximations Φ_i with precision $\nu = \delta_I$ have been computed. Then we determine $\mathfrak{p}$-integral bases $\mathcal{B}'_{i,\nu}$ for $\iota_{i,\nu}(\mathfrak{P}^{a'_{\mathfrak{P}_i}})$ as explained above. Let $\iota_{I',\nu}$ be defined as in (7) with respect to the bases $\mathcal{B}'_{i,\nu}$. Now we can compute the vectors $\iota_{I',\nu}(\theta^j)$ for $1 \leq j \leq n-1$ and apply maximally $\delta_{I'} = v_{\mathfrak{p}}([I' : \mathcal{O}])$ augmentation-steps until obtaining $\mathcal{B}_{I'}$. That is we run Algorithm 1 to compute $\mathcal{B}_{I'}$ with precision $\delta_I \geq \delta_{I'}$. Now one has to calculate $\iota_{I,\nu}(b)$ for $b \in \mathcal{B}_{I'}$ and apply further augmentation-steps until receiving $\mathcal{B}_I$. By (9), any basis $\mathcal{B}_{i,\nu}$ for $\iota_{i,\nu}(\mathfrak{P}_i^{a_{\mathfrak{P}_i}})$ can be deduced by

$$\mathcal{B}_{i,\nu} = \pi^{l_i} \cdot \mathcal{B}'_{i,\nu},$$

with l_i such that $a_{\mathfrak{P}_i} = a'_{\mathfrak{P}_i} + l_i e_{\mathfrak{P}_i}$. In other words the basis $\mathcal{B}_{i,\nu}$ is up to a π-power equal to the basis $\mathcal{B}'_{i,\nu}$. Denote by T the matrix with rows given by $\iota_{I,\nu}(b)$ for $b \in \mathcal{B}_{I'}$ and let T' be the matrix with rows given by $\iota_{I',\nu}(b)$ for $b \in \mathcal{B}_{I'}$. Then T is obtained from T' by multiplying it with a diagonal matrix whose diagonal entries are of the form π^{l_i}. Because we represent the entries in T and T' as polynomials in $k_{\mathfrak{p}}[\pi]$, computing T can be done at no cost by shifting the coefficients of the elements in T' adequately. Thus, $\mathcal{B}_I$ can be determined after maximally $\delta_I - \delta_{I'}$ augmentation-steps.

Clearly, the computation of both, a $\mathfrak{p}$-integral basis $\mathcal{B}_{I'}$ for I' and $\mathcal{B}_I$ for I, has the same complexity as computing just $\mathcal{B}_I$.

Lemma 3.3. *Let $I_{\mathfrak{p}} = \prod_{1 \le i \le s} \mathfrak{P}_i^{a_{\mathfrak{P}_i}}$ with $r_i = \lfloor -a_{\mathfrak{P}_i} / e_{\mathfrak{P}_i} \rfloor$. One can compute at the cost of*

$$O(n^3 \delta_I + n^2 \delta_I^2 + n^{1+\epsilon} \delta_I \log q + n^{1+\epsilon} \delta_I^{2+\epsilon})$$

$\mathfrak{p}$-*small operations triangular* $\mathfrak{p}$-*integral bases of* $\sum_{1 \le i \le s} r_i + 1$ *fractional ideals I' contained in I satisfying* (9).

Proof. Let us show that there are $\sum_{1 \le i \le s} r_i + 1$ many ideals contained in I satisfying (9). Define $I_0 = \prod_{1 \le i \le s} \mathfrak{P}_i^{\tilde{a}_{\mathfrak{P}_i}}$, where the $\tilde{a}_{\mathfrak{P}_i}$ satisfy (8). We define $I_{1,l} = I_0 \cdot \mathfrak{P}_1^{-l e_{\mathfrak{P}_1}}$ with $l = 1, \dots, r_1$. Additionally, we set $I_1 = I_{1,r_1}$ and

$$I_{2,l} = I_1 \cdot \mathfrak{P}_2^{-l e_{\mathfrak{P}_2}},$$

with $l = 1, \dots, r_2$. Inductively, let $I_{s-1} = I_{s-1,r_{s-1}}$ and

$$I_{s,l} = I_{s-1} \cdot \mathfrak{P}_s^{-l e_{\mathfrak{P}_s}},$$

with $l = 1, \dots, r_s$. Thus, for each $1 \le i \le s$ there are exactly r_i ideals contained in I satisfying (9) and I_0, which can be computed as a by-product while computing a $\mathfrak{p}$-integral basis of I with Algorithm 1. □

3C. ***Example.*** We go back to Section 2C, where we computed the $\mathfrak{p}$-integral basis $\mathcal{B}_{I'} = (1, \theta, b_2^*/t, b_3^*/t)$ for $I' = \mathcal{O}$, with $b_2^* = \theta^2 + 2\theta$ and $b_3^* = \theta^3 + 9\theta$. Using that data, one can compute a $\mathfrak{p}$-integral basis $\mathcal{B}_I$ for the fractional ideal $I = \mathfrak{P}_1^{-1}$. Clearly, $[I : A[\theta]] = [I : \mathcal{O}] \cdot [\mathcal{O} : A[\theta]] = \mathrm{N}_{L/K}(\mathfrak{P}_1) \cdot [\mathcal{O} : A[\theta]]$. The residual degree of $\mathfrak{P}_1$ is 2 and $v_{\mathfrak{p}}([\mathcal{O} : A[\theta]]) = 2$. It follows that

$$v_{\mathfrak{p}}([I : A[\theta]]) = 4.$$

The approximations Φ_1 and Φ_2 are computed with precision $\nu = 8$, which is sufficient for the computation of $\mathcal{B}_I$ by Theorem 3.2. The ramification index of $\mathfrak{P}_1$ satisfies $e_{\mathfrak{P}_1} = 1$, so we are now in the situation of (8). Therefore a $\mathfrak{p}$-integral basis $\mathcal{B}_{1,\nu}$ for $\iota_{1,\nu}(\mathfrak{P}_1)$ is given by $\pi^{-1}\mathcal{B}_1 = (1/t, \tilde{\theta}_1/t^2)$. Clearly $\mathcal{B}_{2,\nu} = \mathcal{B}_2$. Then one can compute the matrix T, whose rows represent $\iota_{I,\nu}(b)$ for $b \in \mathcal{B}_{I'}$, by manipulating the matrix from (5). Since we obtained $\mathcal{B}_{1,\nu}$ by dividing the elements in $\mathcal{B}_1$ by t, the matrix T is given by

	$\mathcal{B}_{1,\nu}$		$\mathcal{B}_{2,\nu}$		ω
$\iota_{I,\nu}(1)$	t	0	$\underline{1}$	0	0
$\iota_{I,\nu}(\theta)$	0	t^2	$\underline{11}$	t	0
$\iota_{I,\nu}(b_2^*/t)$	$11t^2$	$2t$	$11t$	$\underline{11}$	0
$\iota_{I,\nu}(b_3^*/t)$	0	$11t^3{+}9t$	$12t$	$11t^2{+}\underline{8}$	0

(10)

We consider the lower-term vectors in order to check if augmentation-steps are applicable:

$$M = \begin{bmatrix} \mathrm{LT}_0(\iota_{I,\nu}(1)) \\ \mathrm{LT}_0(\iota_{I,\nu}(\theta)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_2^*/t)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_3^*/t)) \end{bmatrix} = \begin{bmatrix} 0 & 0 & \underline{1} & 0 \\ 0 & 0 & \underline{11} & 0 \\ 0 & 0 & 0 & \underline{11} \\ 0 & 0 & 0 & \underline{8} \end{bmatrix}.$$

As $\mathrm{rank}(M) = 2$, once can still apply augmentation-steps. According to Lemma 2.6 we can read out the augmentation-steps from M and deduce $b_1' = \theta + 2$ and $b_3' = b_3^*/t + 4b_2^*/t$. This results in

	$\mathcal{B}_{1,\nu}$		$\mathcal{B}_{2,\nu}$		ω
$\iota_{I,\nu}(1)$	t	0	$\underline{1}$	0	0
$\iota_{I,\nu}(b_1')$	$\underline{2}$t	t^2	0	$\underline{1}\,t$	1
$\iota_{I,\nu}(b_2^*/t)$	$11t^2$	$2t$	$11t$	$\underline{11}$	0
$\iota_{I,\nu}(b_3')$	$5t^2$	$11t^3{+}\underline{4}t$	$\underline{4}t$	$11t^2$	1

(11)

with the lower-term matrix

$$M = \begin{bmatrix} \mathrm{LT}_0(\iota_{I,\nu}(1)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_1')) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_2^*/t)) \\ \mathrm{LT}_0(\iota_{I,\nu}(b_3')) \end{bmatrix} = \begin{bmatrix} 0 & 0 & \underline{1} & 0 \\ \underline{2} & 0 & 0 & \underline{1} \\ 0 & 0 & 0 & \underline{11} \\ 0 & \underline{4} & \underline{4} & 0 \end{bmatrix}.$$

Since $\mathrm{rank}(M) = 4$ no further augmentation-steps are applicable and

$$\mathcal{B}_I = \left(1, \frac{b_1'}{t}, \frac{b_2^*}{t}, \frac{b_3'}{t}\right) = \left(1, \frac{\theta+2}{t}, \frac{\theta^2+2\theta}{t}, \frac{\theta^3+4\theta^2+4\theta}{t^2}\right)$$

is a $\mathfrak{p}$-integral basis of I. Thus we computed $\mathcal{B}_I$ from computing $\mathcal{B}_{I'}$. In other words we first computed $\mathcal{B}_I$ and $\mathcal{B}_{I'}$ is implied as a by-product.

Acknowledgment

The authors would like to thank the Pacific Institute for the Mathematical Sciences (PIMS) for its financial support.

References

[1] Jens-Dietrich Bauch, *Computation of integral bases*, J. Number Theory **165** (2016), 382–407. MR 3479230

[2] ______, *Lattices over polynomial rings and applications to function fields*, preprint, 2016. arXiv 1601.01361v1

[3] 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

[4] Janko Boehm, Wolfram Decker, Santiago Laplagne, and Gerhard Pfister, *Computing integral bases via localization and Hensel lifting*, preprint, 2015. arXiv 1505.05054v1

[5] Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, no. 138, Springer, 1993. MR 1228206

[6] David Ford and Pascal Letard, *Implementing the round four maximal order algorithm*, J. Théor. Nombres Bordeaux **6** (1994), no. 1, 39–80. MR 1305287

[7] Jordi Guàrdia, Jesús Montes, and Enric Nart, *A new computational approach to ideal theory in number fields*, Found. Comput. Math. **13** (2013), no. 5, 729–762. MR 3105943

[8] ———, *Higher Newton polygons and integral bases*, J. Number Theory **147** (2015), 549–589. MR 3276340

[9] Jordi Guàrdia and Enric Nart, *Local-to-global computation of integral bases without a previous factorization of the discriminant*, preprint, 2015. arXiv 1510.01995v1

[10] 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

[11] K. Hensel, *Theorie der algebraischen Zahlen*, Teubner, Leipzig, 1908.

[12] Michael E. Pohst, *Computational algebraic number theory*, DMV Seminar, no. 21, Birkhäuser, Basel, 1993. MR 1243639

[13] Wolfgang M. Schmidt, *Construction and estimation of bases in function fields*, J. Number Theory **39** (1991), no. 2, 181–224. MR 1129568

[14] A. Schönhage and V. Strassen, *Schnelle Multiplikation grosser Zahlen*, Computing (Arch. Elektron. Rechnen) **7** (1971), 281–292. MR 0292344

[15] Jean-Pierre Serre, *Corps locaux*, 4th ed., Hermann, Paris, 2004.

[16] Hayden D. Stainsby, *Triangular bases of integral closures*, J. Symbolic Comput. **87** (2018), 140–175. MR 3744344

[17] Mark van Hoeij, *An algorithm for computing an integral basis in an algebraic function field*, J. Symbolic Comput. **18** (1994), no. 4, 353–363. MR 1324494

Received 1 Mar 2018. Revised 20 Jun 2018.

JENS-DIETRICH BAUCH: jbauch@sfu.ca
Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada

HA THANH NGUYEN TRAN: hatran1104@gmail.com
Department of Mathematics and Statistics, University of Calgary, Calgary, AB, Canada

VOLUME EDITORS

Renate Scheidler
University of Calgary
Calgary, AB T2N 1N4
Canada

Jonathan Sorenson
Butler University
Indianapolis, IN 46208
United States

The cover image is based on a design by Linh Chi Bui.

Electronic copies can be obtained free of charge from http://msp.org/obs/2 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-02-6 (print), 978-1-935107-03-3 (electronic)

First published 2019.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org http://msp.org

THE OPEN BOOK SERIES 2

Thirteenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the thirteenth ANTS meeting, held July 16-20, 2018, at the University of Wisconsin-Madison. It includes revised and edited versions of 28 refereed papers presented at the conference.

Edited by Renate Scheidler and Jonathan Sorenson

CONTRIBUTORS

Simon Abelard
Sonny Arora
Vishal Arul
Angelica Babei
Jens-Dietrich Bauch
Alex J. Best
Jean-François Biasse
Alin Bostan
Reinier Bröker
Nils Bruin
Xavier Caruso
Stephanie Chan
Qi Cheng
Gilles Christol
Owen Colman
Edgar Costa
Philippe Dumas
Kirsten Eisenträger
Claus Fieker
Shuhong Gao
Pierrick Gaudry
Alexandre Gélin
Alexandru Ghitza
Laurent Grémy
Jeroen Hanselman
David Harvey
Tommy Hofmann
Everett W. Howe
David Hubbard
Kiran S. Kedlaya
Thorsten Kleinjung
David Kohel
Wanlin Li
Richard Magner
Anna Medvedovsky
Michael Musty
Ha Thanh Nguyen Tran
Christophe Ritzenthaler
David Roe
J. Maurice Rojas
Nathan C. Ryan
Renate Scheidler
Sam Schiavone
Andrew Shallue
Jeroen Sijsling
Carlo Sircana
Jonathan Sorenson
Pierre-Jean Spaenlehauer
Andrew V. Sutherland
Nicholas Triantafillou
Joris van der Hoeven
Christine Van Vredendaal
John Voight
Daqing Wan
Lawrence C. Washington
Jonathan Webster
Benjamin Wesolowski
Yinan Zhang
Alexandre Zotine