Unit Computation in Purely Cubic Function Fields of Unit Rank 1

Renate Scheidler*[1] and Andreas Stein[2]

[1] University of Delaware, Newark DE 19716, USA
scheidle@math.udel.edu
[2] University of Manitoba, Winnipeg MB R3T 2N2, CANADA
andreas@cs.umanitoba.ca

Abstract. This paper describes a method for computing the fundamental unit and regulator of a purely cubic congruence function field of unit rank 1. The technique is based on Voronoi's algorithm for generating a chain of successive minima in a multiplicative cubic lattice which is used for calculating the fundamental unit and regulator of a purely cubic number field.

1 Introduction

Voronoi's Algorithm [14, 7] computes a system of fundamental units of a cubic number field. The method is based on computing chains of successive minima in the maximal order $\mathcal{O}$ of the field K. An implementation in purely cubic number fields was given by Williams et al. [16, 17, 15]. Since then, the general method has been extended to fields of higher degree; see [1–6]. The first algorithm for computing fundamental units in cubic funcion fields was given by Mang [9]. His technique is based on the Pohst-Zassenhaus method for number fields [10, Chap. 5]. By Mang's own admission, his technique is slow and is infeasible for even modest size fields; an example that took 273 seconds of CPU time on a Siemens mainframe using Mang's method required only 0.04 seconds on a Silicon Graphics Challenge workstation with our algorithm. In this paper, we show how to adapt Voronoi's algorithm to purely cubic congruence function fields of unit rank 1. While the number field and function field situations are similar in many ways, there are also significant differences between the two settings; most notably, the different behavior of the valuation (which is non-archimedian in the function field case) and the lack of geometric lattice structure in function fields.

For an introduction to congruence function fields, see [13]; the purely cubic case is discussed in more detail in [9]. Let $k = \mathbb{F}_q$ be a finite field of order q and let t be a an element that is transcendental over k. As usual, we denote by $k(t)$ the

* Research supported by NSF grant DMS-9631647

rational function field and by $k[t]$ the ring of polynomials over k in the variable t. A *purely cubic (congruence) function field* K over the *field of constants* k is a cubic extension of $k(t)$ of the form $K = k(t, \rho)$ where $\rho^3 = D \in k[t]$ and $D = D(t)$ is cubefree in $k[t]$; write $D = GH^2$ where $G, H \in k[t]$ are relatively prime. The algebraic closure $\mathcal{O} = \overline{k[t]}$ of $k[t]$ in K is a $k[t]$-module of rank 3 with a *$(t-)$integral basis* $\{1, \rho = \sqrt[3]{GH^2}, \omega = \rho^2/H = \sqrt[3]{G^2H}\}$. Its unit group $\mathcal{O}^*$ is the *$(t-)$unit group* of K. $\mathcal{O}^* = k^* \times \mathcal{E}$ where $\mathcal{E}$ is the product of r infinite cyclic groups and $r \in \mathbb{N}_0$ is the *$(t-)$unit rank* of K. The units in k^* are the *trivial units*. If $r > 0$, an independent set of r generators of $\mathcal{E}$ is a system of *fundamental $(t-)$units* of K. Denote by $k((1/t))$ the field of *Puiseux series* $\sum_{i=m}^{\infty} a_i/t^i$ ($m \in \mathbb{Z}$, $a_i \in k$ for $i \geq m$) over k. Then the number of irreducible factors over $k((1/t))$ of the polynomial $F(t, y) = y^3 - D \in k[t, y]$ is $r + 1$.

Henceforth, we assume that $q \equiv -1 \pmod 3$ (so k does not contain any primitive cube roots of unity), the degree $\deg(D)$ of D is divisible by 3, and the leading coefficient $\operatorname{sgn}(D)$ of D is a cube in k. In this case, $\rho \in k((1/t))$, so $K \leq k((1/t))$, and $F(t, y)$ splits into two irreducibles over $k((1/t))$, namely $F(t, y) = (y-\rho)(y^2 + \rho y + \rho^2)$, so $r = 1$ and $\mathcal{O}^* = k^* \times \langle \epsilon \rangle$ with a fundamental unit ϵ (see [11]). If g denotes the *genus* of K, then we have

$$g = \deg(GH) - 2. \tag{1.1}$$

Let $\mathcal{D}$ be the *divisor group* of K over k, $\mathcal{D}^0$ the subgroup of $\mathcal{D}$ of *divisors of degree 0*, and $\mathcal{P} \leq \mathcal{D}^0$ the group of *principal divisors* of $K|k$. The *divisor class group (of degree 0)* of $K|k$ is the factor group $\mathcal{C}^0 = \mathcal{D}^0/\mathcal{P}$; its order $h = \#\mathcal{C}^0$ is finite and is the *divisor class number* of K. In analogy to $\mathcal{D}$ and $\mathcal{D}^0$, denote by $\mathcal{U}$ the subgroup of $\mathcal{D}$ generated by the infinite places (with respect to t) of K and by $\mathcal{U}^0$ the subgroup of divisors in $\mathcal{U}$ of degree 0. The *$(t-)$regulator* of K is the index $R = [\mathcal{U}^0 \ : \ \mathcal{P} \cap \mathcal{U}^0]$. If $\mathcal{I}$ is the group of *fractional $(t-)$ideals* of K and $\mathcal{H}$ the subgroup of fractional *principal $(t-)$ideals* of K, then the *$(t-)$ideal class group* of K is $\mathcal{C} = \mathcal{I}/\mathcal{H}$; its order $h' = \#\mathcal{C}$ is also finite and is the *$(t-)$ideal class number* of K. We have

$$h = Rh'. \tag{1.2}$$

For $\alpha = \sum_{i=m}^{\infty} a_i/t^i \in k((1/t))$ ($m \in \mathbb{Z}, a_i \in k$ for $i \geq m, a_m \neq 0$), we define

$$\begin{aligned}
\deg(\alpha) &= -m, \\
|\alpha| &= q^{-m} \ = \ q^{\deg(\alpha)}, \\
\operatorname{sgn}(\alpha) &= a_m, \\
\lfloor \alpha \rfloor &= \sum_{i=m}^{0} \frac{a_i}{t^i}.
\end{aligned}$$

We also set $\deg(0) = -\infty$ and $\lfloor 0 \rfloor = 0$. Note that $\lfloor \alpha \rfloor \in k[t]$ and $|\alpha - \lfloor \alpha \rfloor| < 1$.

If ϵ is a fundamental unit with $\deg(\epsilon) > 0$, then ϵ is unique up to a trivial unit factor. Then we have for the regulator $R = \deg(\epsilon)/2$.

Let ι be a primitive cube root of unity in some algebraic closure of k, so $\iota^2 + \iota + 1 = 0$ and $\iota^3 = 1$. Then $k((1/t))(\iota)$ is a quadratic extension of $k((1/t))$ whose nontrivial K-automorphism is "complex conjugation" $^- : k((1/t))(\iota) \to k((1/t))(\iota)$ via $\bar{\iota} = \iota^{-1}$. For $\phi \in k((1/t))(\iota)$, we define

$$\deg(\phi) = \frac{1}{2}\deg(\phi\bar{\phi}),$$
$$|\phi| = \sqrt{|\phi\bar{\phi}|} = q^{\frac{1}{2}\deg(\phi\bar{\phi})} = q^{\deg(\phi)}.$$

$K(\iota) = k(\iota, t, \rho)$ is a cyclic extension of $k(\iota, t)$ of degree 3 for which we fix the $k(\iota, t)$-automorphism $' : K(\iota) \to K(\iota)$ via $\rho' = \iota\rho$. Write γ'' for $(\gamma')'$ $(\gamma \in K(\iota))$. Note that $\overline{\alpha'} = \alpha''$ for $\alpha \in K$. For $\alpha \in K$, the *norm of* α *(over* $k(t)$*)* is $N(\alpha) = \alpha\alpha'\alpha''$. We have $N(\alpha) \in k(t)$, and if $\alpha \in \mathcal{O}$, then $N(\alpha) \in k[t]$.

2 Reduced Ideals and Minima

A subset $\mathcal{A}$ of $\mathcal{O}$ is an *integral ideal* if for any $\alpha, \beta \in \mathcal{A}$ and $\theta \in \mathcal{O}$, $\alpha + \beta \in \mathcal{A}$ and $\theta\alpha \in \mathcal{A}$. A subset $\mathcal{A}$ of K is a *fractional ideal* if there exists a nonzero $d \in k[t]$ such that $d\mathcal{A}$ is an integral ideal of $\mathcal{O}$. A fractional or integral ideal $\mathcal{A}$ is *principal* if $\mathcal{A} = (\alpha) = \{\theta\alpha \mid \theta \in \mathcal{O}\}$ for some α. Henceforth, we assume all ideals (fractional and integral) to be nonzero, i.e. the term "ideal" will be synonymous with "nonzero ideal". An integral ideal $\mathcal{A}$ is *primitive* if there exists no nonconstant polynomial $f \in k[t]$ such that every $\alpha \in \mathcal{A}$ is a multiple in $\mathcal{O}$ of f. For a primitive integral ideal $\mathcal{A}$, the greatest common divisor of all polynomials in $\mathcal{A} \cap k[t]$ is denoted by $L(\mathcal{A})$.

Every integral or fractional ideal $\mathcal{A}$ of $\mathcal{O}$ is a $k[t]$-module of rank 3. If $\mathcal{A}$ has a $k[t]$-basis $\{\lambda, \mu, \nu\}$, write $\mathcal{A} = [\lambda, \mu, \nu]$. Specifically, if a fractional ideal $\mathcal{A}$ contains 1, then $\mathcal{A}$ has a $k[t]$-basis of the form $\{1, \mu, \nu\}$ where

$$\mu = (m_0 + m_1\rho + m_2\omega)/d,$$
$$\nu = (n_0 + n_1\rho + n_2\omega)/d,$$

with $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[t]$. If $\gcd(m_0,\ m_1,\ n_0,\ n_1,\ n_2,\ d) = 1$, then $d\mathcal{A}$ is a primitive integral ideal with $L(d\mathcal{A}) = d/\mathrm{sgn}(d)$.

The $(t-)$*norm* of a fractional ideal $\mathcal{A} = [\lambda, \mu, \nu]$ is $N(\mathcal{A}) = \mathrm{sgn}(\det(T))^{-1}\det(T) \in k(t)^*$ where $T \in Gl_3(k(t))$ such that

$$\begin{pmatrix} \lambda \\ \mu \\ \nu \end{pmatrix} = T \begin{pmatrix} 1 \\ \rho \\ \omega \end{pmatrix}.$$

$N(\mathcal{A})$ is independent of the choice of bases for $\mathcal{A}$ and $\mathcal{O}$. The norm of an integral ideal $\mathcal{A}$ is $N(\mathcal{A}) = L(\mathcal{A})^3 N(L(\mathcal{A})^{-1}\mathcal{A}) \in k[t]$. For an integral ideal $\mathcal{A}$, we have $L(\mathcal{A}) \mid N(\mathcal{A})$, and if $\mathcal{A}$ is primitive, then $N(\mathcal{A}) \mid L(\mathcal{A})^2$.

The $(t-)$*discriminant* of a fractional or integral ideal $\mathcal{A} = [\lambda, \mu, \nu]$ is the quantity

$$\Delta(\mathcal{A}) = \det \begin{pmatrix} \lambda \; \lambda' \; \lambda'' \\ \mu \; \mu' \; \mu'' \\ \nu \; \nu' \; \nu'' \end{pmatrix}^2 \in \begin{cases} k(t) & \text{if } \mathcal{A} \text{ is a fractional ideal,} \\ k[t] & \text{if } \mathcal{A} \text{ is an integral ideal.} \end{cases}$$

$\Delta(\mathcal{A})$ is independent of the choice of $k[t]$-basis of $\mathcal{A}$. The discriminant of $\mathcal{O} = [1, \rho, \omega]$ is $\Delta = -27G^2H^2$. We have

$$\Delta(\mathcal{A}) = a^2 N(\mathcal{A})^2 \Delta \text{ for some } a \in k^*. \tag{2.1}$$

If $\mathcal{A}$ is a fractional ideal and $\alpha \in \mathcal{A}$, $\alpha \neq 0$, then α is a *minimum* in $\mathcal{A}$ if for $\beta \in \mathcal{A}$ with $\beta \neq 0$, $|\beta| \leq |\alpha|$ and $|\beta'| \leq |\alpha'|$ imply $\beta \in k^*\alpha$, i.e. β and α differ only by a factor that is a trivial unit. $\mathcal{A}$ is *reduced* if $1 \in \mathcal{A}$ and 1 is a minimum in $\mathcal{A}$. An integral ideal $\mathcal{A}$ is reduced if the fractional ideal $(L(\mathcal{A})^{-1})\mathcal{A}$ is reduced, i.e. if and only if $L(\mathcal{A})$ is a minimum in $\mathcal{A}$. It is easy to see that $\mathcal{O}$ is reduced. If $\mathcal{A}$ is a fractional ideal of $\mathcal{O}$ with a minimum $\theta \in \mathcal{A}$, then $\eta\theta$ is a minimum in $\mathcal{A}$ for every unit $\eta \in \mathcal{O}^*$. In particular, every unit in $\mathcal{O}$ is a minimum in $\mathcal{O}$.

Theorem 2.1. *If $\mathcal{A}$ is a reduced fractional ideal, then $|\Delta(\mathcal{A})| > 1$, so $|N(\mathcal{A})| > 1/|\sqrt{\Delta}|$.*

Proof. See [11]. □

Corollary 2.2. *If $\mathcal{A}$ is a reduced integral ideal, then $|L(\mathcal{A})| < |\sqrt{\Delta}|$ and $|N(\mathcal{A})| < |\Delta|$.*

Proof. Since $\mathcal{A}$ is reduced, we have $L(\mathcal{A}) \mid N(\mathcal{A}) \mid L(\mathcal{A})^2$. Also $\mathcal{B} = (L(\mathcal{A})^{-1})\mathcal{A}$ is a reduced fractional ideal, so by Theorem 2.1, $|L(\mathcal{A})|^2 \geq |N(\mathcal{A})| = |L(\mathcal{A})|^3|N(\mathcal{B})| > |L(\mathcal{A})|^3/|\sqrt{\Delta}|$, so $|L(\mathcal{A})| < |\sqrt{\Delta}|$ and $|N(\mathcal{A})| \leq |L(\mathcal{A})|^2 < |\Delta|$. □

Corollary 2.3. *If $\mathcal{A}$ is a reduced fractional ideal and $\alpha \in \mathcal{A}$ is nonzero, then $|N(\alpha)| > 1/|\Delta|$.*

Proof. Let $d \in k[t]$ be of minimal degree so that $\mathcal{B} = d\mathcal{A}$ is an integral ideal. Then $d\alpha \in \mathcal{B}$, so $(d\alpha)(d^2\alpha'\alpha'') = N(d\alpha) = d^3N(\alpha) \in \mathcal{B}$. Hence $L(\mathcal{B}) = d \mid d^3N(\alpha)$, so $|N(\alpha)| \geq 1/|d|^2 = 1/|L(\mathcal{B})|^2 > 1/|\Delta|$ by Corollary 2.2. □

Let $\mathcal{A}$ be a fractional ideal and let $\theta \in \mathcal{A}$ be a minimum in $\mathcal{A}$. An element $\phi \in \mathcal{A}$ is a *minimum adjacent to θ in $\mathcal{A}$* if

(M1) ϕ is a minimum in $\mathcal{A}$,
(M2) $|\theta| < |\phi|$,
(M3) For no $\alpha \in \mathcal{A}$, $|\theta| < |\alpha| < |\phi|$ and $|\alpha'| < |\theta'|$.

Note that conditions (M1) and (M2) imply $|\phi'| < |\theta'|$, as $|\theta'| \leq |\phi'|$ would yield $\theta \in k^*\phi$ by (M1) and hence $|\theta| = |\phi|$, contradicting (M2).

In the number field setting, the existence of adjacent minima is guaranteed by Minkowski's lattice point theorem. However, in function fields, we have no such tool available, so we need to establish their existence analytically.

Theorem 2.4. *Let $\mathcal{A}$ be a fractional ideal and let $\theta \in \mathcal{A}$ be a minimum in $\mathcal{A}$. Then a minimum ϕ adjacent to θ in $\mathcal{A}$ exists and is unique up to a trivial unit factor.*

Proof. The set $H(\theta) = \{\alpha \in \mathcal{A} \mid |\alpha| > |\theta| \text{ and } |\alpha'| < |\theta'|\}$ is nonempty as $\epsilon\theta \in H(\theta)$. Let $\alpha \in H(\theta)$ have minimal degree. Then the set $D(\theta) = \{\deg(N(\alpha)) \mid \alpha \in H(\theta), |\alpha| \text{ is minimal}\}$ is a nonempty subset of $\mathbb{Z}$ which is bounded below by $-\deg(\Delta)$ by Corollary 2.3. Let $\phi \in H(\theta)$ so that $|\phi|$ is minimal and $\deg(N(\phi))$ is a smallest element of $D(\theta)$. Then

(a) $|\phi| > |\theta|$ and $|\phi'| < |\theta'|$,
(b) if $\alpha \in \mathcal{A}$ with $|\alpha| > |\theta|$ and $|\alpha'| < |\theta'|$, then $|\alpha| \geq |\phi|$,
(c) if $\alpha \in \mathcal{A}$ with $|\alpha| = |\phi|$ and $|\alpha'| < |\theta'|$, then $|\alpha'| \geq |\phi'|$.

Conditions (M2) and (M3) for ϕ follow from properties (a) and (b), respectively, so we only need to show that ϕ is a minimum in $\mathcal{A}$. Let $\alpha \in \mathcal{A}$, $\alpha \neq 0$ with $|\alpha| \leq |\phi|$ and $|\alpha'| \leq |\phi'|$. By (a), $|\alpha'| < |\theta'|$. If $|\alpha| \leq |\theta|$, then $\alpha \in k^*\theta$ as θ is a minimum in $\mathcal{A}$, implying $|\theta'| = |\alpha'| < |\theta'|$. So $|\alpha| > |\theta|$. By (b), $|\alpha| \geq |\phi|$, so $|\alpha| = |\phi|$. Hence by (c), $|\alpha'| \geq |\phi'|$, so $|\alpha'| = |\phi'|$. Thus we have $|\alpha| = |\phi|$ and $|\alpha'| = |\phi'|$.

Let $\beta = \alpha - (\mathrm{sgn}(\alpha)\mathrm{sgn}(\phi)^{-1})\phi$, then $\beta \in \mathcal{A}$, $|\beta| < |\phi|$ and $|\beta'| \leq \max\{|\alpha'|, |\phi'|\} < |\theta'|$. Suppose $\beta \neq 0$, then by (M3), $|\beta| \leq |\theta|$, so $\beta \in k^*\theta$. But then $|\theta'| = |\beta'| < |\theta'|$. So we must have $\beta = 0$ and thus $\alpha \in k^*\phi$. Therefore, ϕ is a minimum in $\mathcal{A}$.

To see that ϕ is unique up to a factor in k^*, let ϕ_1, ϕ_2 be two minima in $\mathcal{A}$ adjacent to θ. Without loss of generality, assume $|\phi_1'| \leq |\phi_2'|$. Both ϕ_1 and ϕ_2 are minima in $\mathcal{A}$ by (M1) and $|\theta| < |\phi_1|, |\phi_2|$ by (M2). If $|\phi_1| < |\phi_2|$, then by (M3), $|\phi_1'| \geq |\theta'|$, so since ϕ_1 is a minimum in $\mathcal{A}$, $\theta \in k^*\phi_1$, implying the contradiction $|\theta| = |\phi_1| > |\theta|$. Similarly we can rule out $|\phi_1| > |\phi_2|$. Hence $|\phi_1| = |\phi_2|$, so $\phi_1 \in k^*\phi_2$. □

We will henceforth speak of *the* minimum adjacent to an element in a fractional ideal, keeping in mind that it is only unique up to a trivial unit factor.

If $\mathcal{A}$ is a reduced fractional ideal with a minimum $\theta \in \mathcal{A}$, then it is easy to see that $\mathcal{A}^* = (1/\theta)\mathcal{A}$ is reduced. Furthermore, if θ^* is the minimum adjacent to 1 in $\mathcal{A}^*$, then $\theta\theta^*$ is the minimum adjacent to θ in $\mathcal{A}$.

3 The Algorithm

The basic idea for our algorithm is the same as in the unit rank 1 case of number fields. Start with the reduced ideal $\mathcal{A}_1 = \mathcal{O}$, and recursively define a sequence of reduced fractional ideals $\mathcal{A}_n$ as follows. Let μ_n be the minimum adjacent to 1 in $\mathcal{A}_n$ and set $\mathcal{A}_{n+1} = (\mu_n^{-1})\mathcal{A}_n$. Then $\mathcal{A}_{n+1}$ is a reduced fractional ideal. Define

$$\theta_1 = 1, \quad \theta_n = \prod_{i=1}^{n-1} \mu_i \quad \text{for } n \geq 2. \tag{3.1}$$

Then $\mathcal{A}_n = (\theta_n^{-1})$ and $\theta_{n+1} = \mu_n \theta_n$, so by our above remarks, θ_{n+1} is the minimum adjacent to θ_n in $\mathcal{O}$ ($n \in \mathbb{N}$). Thus we have a *chain*

$$\theta_1 = 1,\ \theta_2,\ \theta_3,\ \ldots \tag{3.2}$$

of successive minima in $\mathcal{O}$. This sequence can easily be shown to contain *all* the minima in $\mathcal{O}$ of nonnegative degree. In particular, the fundamental unit ϵ must appear in the sequence (3.2), and since ϵ is the unit of smallest positive degree, the first index $l \in \mathbb{N}$ such that $N(\theta_{l+1})$ is a trivial unit yields $\theta_{l+1} = \epsilon$ (up to a constant factor). l is the *period* of ϵ (or of K). We have $\mathcal{A}_{l+1} = \mathcal{A}_1$, $\mu_{l+1} = \mu_1$ and in fact $\mu_{ml+i} = \mu_i$ for $m, i \in \mathbb{N}$, where the last two equalities again only hold up to a trivial unit factor. Hence the sequence (3.2) is equal to

$$1, \theta_2, \ldots, \theta_l, \epsilon, \epsilon\theta_2, \ldots, \epsilon\theta_l, \epsilon^2, \epsilon^2\theta_2, \ldots, \epsilon^3, \ldots$$

and contains all nonnegative powers of ϵ.

A simpler termination condition for the computation of the chain (3.2) that avoids computing norms is given as follows. Let $\mathcal{A} = (\theta^{-1}) = [1, \mu, \nu]$ where θ is an element of the chain (3.2) and $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$ with $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[t]$ and $\gcd(m_0, m_1, m_2, n_0, n_1, n_2, d) = 1$. Then $N(\theta) \in k^*$ if and only if $d \in k^*$.

We are now ready to present our algorithm for computing the fundamental unit of K. In each iteration, we have a basis $\{1, \tilde{\mu}_n = (m_0 + m_1\rho + m_2\omega)/d, \tilde{\nu}_n = (n_0 + n_1\rho + n_2\omega)/d\}$ of our current ideal $\mathcal{A}_n = (\theta_n^{-1})$ where $\theta_n = (e_0 + e_1\rho + e_2\omega)/f$ ($m_i, n_i, d, e_i, f \in k[t]$ for $i = 0, 1, 2$). This basis is replaced by a *reduced basis* $\{1, \mu_n, \nu_n\}$; that is, a basis containing the minimum μ_n adjacent to 1 in $\mathcal{A}_n$. Details on how to obtain such a basis are given in the next section. Then θ_n is updated to $\theta_{n+1} = \mu_n\theta_n$, and since $\mathcal{A}_{n+1} = (\mu_n^{-1})\mathcal{A}_n$, μ_n and ν_n are replaced by $\tilde{\mu}_{n+1} = 1/\mu_n = \mu'_n\mu''_n/N(\mu_n)$ and $\tilde{\nu}_n/\mu_n = \nu_n\mu_{n+1}$, respectively. Initially, $\theta_1 = 1$, $\mu_1 = \rho$, and $\nu_1 = \omega$. According to our termination condition, we end the algorithm as soon as we encounter a basis denominator d that is a constant.

Algorithm 3.1 (Fundamental Unit Algorithm).

Input: The polynomials G, H where $D = GH^2$.

Output: $e_0, e_1, e_2 \in k[t]$ *where* $\epsilon = e_0 + e_1\rho + \epsilon_2\omega$ *is the fundamental unit of* K.

Algorithm:

```
1. Set $e_0 = f = 1$, $e_1 = e_2 = 0$; $m_0 = m_2 = n_0 = n_1 = 0$, $m_1 = n_2 = d = 1$.
2. Repeat
   (a) { Reduce the basis }
       Use Algorithm 4.1 below to replace $m_0, m_1, m_2, n_0, n_1, n_2, d$ by the coefficients of a reduced basis.
   (b) { Update $\theta_n$ }
       i. Replace
          $$\begin{pmatrix} e_0 \\ e_1 \\ e_2 \\ f \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} e_0m_0 + (e_1m_2 + e_2m_1)GH \\ e_0m_1 + e_1m_0 + e_2m_2G \\ e_0m_2 + e_1m_1H + e_2m_0 \\ df \end{pmatrix}.$$
       ii. Compute $g = \gcd(e_0, e_1, e_2, f)$. For $i = 0, 1, 2$, replace $e_i$ by $e_i/g$ and $f$ by $f/g$.
   (c) { Update $\mu$ and $\nu$ }
       i. Set
          $$\begin{aligned} a_0 &= m_0^2 - m_1m_2GH, \\ a_1 &= m_2^2G - m_0m_1, \\ a_2 &= m_1^2H - m_0m_2, \\ b &= m_0^3 + m_1^3GH^2 + m_2^3G^2H - 3m_0m_1m_2GH. \end{aligned}$$
       ii. Replace
          $$\begin{pmatrix} m_0 \\ m_1 \\ m_2 \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} a_0d \\ a_1d \\ a_2d \end{pmatrix}.$$
       iii. Replace
          $$\begin{pmatrix} n_0 \\ n_1 \\ n_2 \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} a_0n_0 + (a_1n_2 + a_2n_1)GH \\ a_0n_1 + a_1n_0 + a_2n_2G \\ a_0n_2 + a_1n_1H + a_2n_0 \end{pmatrix}.$$
       iv. Replace $d$ by $b$.
       v. Compute $h = \gcd(m_0, m_1, m_2, n_0, n_1, n_2, d)$. For $i = 0, 1, 2$, replace $m_i$ by $m_i/h$, $n_i$ by $n_i/h$ and $d$ by $d/h$.
   until $d \in k^*$.
```

The number of reduction steps is exactly the period l of ϵ. This number can be quite large.

Theorem 3.2. $l \leq 2R = \deg(\epsilon) = O(q^{\frac{1}{2}\deg\Delta - 2})$, *so* $|\epsilon| = O(q^{q^{\frac{1}{2}\deg(\Delta)-2}})$.

Proof. For $n \in \mathbb{N}$, let $\delta_n = \deg(\theta_n) \in \mathbb{N}_0$. Since $\delta_1 = 0$ and δ_n strictly increases with n, a simple induction argument shows $\delta_n \geq n - 1$. Hence $l \leq \deg(\theta_{l+1}) = \deg(\epsilon) = 2R$. Using the inequality $h \leq (\sqrt{q}+1)^{2g}$ deduced in [12], together with (1.1) and (1.2), we obtain $R \leq (\sqrt{q}+1)^{\deg(\Delta)-4} = O(q^{1/2\deg(\Delta)-2})$, whence follows the bound on ϵ. □

The above theorem shows that the coefficients e_0, e_1, e_2 of ϵ can be so huge that it might be infeasible to compute or even simply write down the fundamental unit for large values of $|\Delta|$. For this situation, we modify Algorithm 3.1 to avoid calculating the minima θ_n and compute only the regulator R of K as follows. In step 1, initialize only the m_i, n_i ($i = 0, 1, 2$), and d, as well as setting $R = 0$. Perform step 2 as in Algorithm 3.1, except omit part (b) of step 2. Instead, we need to add $\deg(\mu_n)$ to R. Since $\deg(\mu_n) = \deg(m_0/d)$ (see Theorem 4.4), we replace step 2 (b) of Algorithm 3.1 by the instruction "replace R by $R + \deg(m_0) - \deg(d)$". Since the algorithm with these modifications computes $\deg(\epsilon) = 2R$, we must divide the value of R by 2 after the loop in step 2 terminates to obtain the correct value for the regulator.

4 Computation of a minimum adjacent to 1

The above discussion shows that the task of finding ϵ (or R) reduces to the problem of computing a reduced basis of a reduced fractional ideal $\mathcal{A}$. In particular, we need to be able to generate the minimum adjacent to 1 in $\mathcal{A}$. This is accomplished by applying a sequence of suitable unimodular transformations to the pair $(\tilde{\mu}, \tilde{\nu})$ where $\{1, \tilde{\mu}, \tilde{\nu}\}$ is a $k[t]$-basis of $\mathcal{A}$, until a basis $\{1, \mu, \nu\}$ is obtained such that μ is our desired minimum. Before we present the details of this reduction technique, we require several somewhat technical definitions. Henceforth, we exclude the characteristic 2 case; that is, we require k to be a finite field of characteristic at least 5. If $\alpha = a + b\rho + c\omega \in K$ with $a, b, c \in k(t)$, let

$$\begin{aligned} \xi_\alpha &= b\rho + c\omega &&= \alpha - a, \\ \eta_\alpha &= b\rho - c\omega &&= \frac{1}{2\iota + 1}(\alpha' - \alpha''), \\ \zeta_\alpha &= 2a - b\rho - c\omega &&= \alpha' + \alpha'', \end{aligned} \tag{4.1}$$

where we recall that ι is a primitive cube root of unity. Then $\xi_{f\alpha+g\beta} = f\xi_\alpha + g\xi_\beta$, $\eta_{f\alpha+g\beta} = f\eta_\alpha + g\eta_\beta$, $\zeta_{f\alpha+g\beta} = f\zeta_\alpha + g\zeta_\beta$ for any $\alpha, \beta \in K$ and $f, g \in k(t)$. Simple calculations show

$$\alpha = \frac{1}{2}(3\xi_\alpha + \zeta_\alpha), \qquad \alpha'\alpha'' = \frac{1}{4}(3\eta_\alpha^2 + \zeta_\alpha^2). \tag{4.2}$$

and if $\mathcal{A} = [1, \mu, \nu]$ is a fractional ideal, then

$$\det \begin{pmatrix} \xi_\mu & \eta_\mu \\ \xi_\nu & \eta_\nu \end{pmatrix} = \xi_\mu \eta_\nu - \xi_\nu \eta_\mu = -2\sqrt{\Delta(\mathcal{A})}, \tag{4.3}$$

so this determinant is independent of the choice of basis of $\mathcal{A}$.

We are now ready to present our reduction method.

Algorithm 4.1 (Reduction Algorithm).

Input: $\tilde{\mu}$, $\tilde{\nu}$ *where* $\{1, \tilde{\mu}, \tilde{\nu}\}$ *is a basis of some reduced fractional ideal* $\mathcal{A}$.

Output: μ, ν *where* $\{1, \mu, \nu\}$ *is a basis of* $\mathcal{A}$ *such that* $|\zeta_\mu| < 1$, $|\zeta_\nu| < 1$, $|\xi_\mu| > |\xi_\nu|$, $|\eta_\mu| < 1 \leq |\eta_\nu|$.

Algorithm:

1. *Set* $\mu = \tilde{\mu}$, $\nu = \tilde{\nu}$.
2. *If* $|\xi_\mu| < |\xi_\nu|$ *or if* $|\xi_\mu| = |\xi_\nu|$ *and* $|\eta_\mu| < |\eta_\nu|$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
3. *If* $|\eta_\mu| \geq |\eta_\nu|$
   (a) *while* $\lfloor \xi_\mu / \xi_\nu \rfloor = \lfloor \eta_\mu / \eta_\nu \rfloor$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu / \xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
   (b) *Replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu / \xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
   (c) *If* $|\eta_\mu| = |\eta_\nu|$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}$$
   where $a = sgn(\eta_\mu) sgn(\eta_\nu)^{-1} \in k^*$.
4. (a) *While* $|\eta_\nu| < 1$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} 0 & 1 \\ -1 & \lfloor \xi_\mu / \xi_\nu \rfloor \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
   (b) *While* $|\eta_\mu| \geq 1$, *replace*
$$\begin{pmatrix} \mu \\ \nu \end{pmatrix} \quad by \quad \begin{pmatrix} \lfloor \eta_\nu / \eta_\mu \rfloor & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \mu \\ \nu \end{pmatrix}.$$
5. *If* $|\zeta_\mu| \geq 1$, *replace* μ *by* $\mu - (1/2)\lfloor \zeta_\mu \rfloor$.
   If $|\zeta_\nu| \geq 1$, *replace* ν *by* $\nu - (1/2)\lfloor \zeta_\nu \rfloor$.

Proposition 4.2. *Algorithm 4.1 terminates and produces the output specified above.*

Proof. It is easy to see that all transformations of μ and ν in steps 2, 3 and 4 maintain a basis $\{1, \mu, \nu\}$ of $\mathcal{A}$ because the basis transformation matrices all have determinant 1.

We claim that after step 3, we have

$$|\xi_\mu| > |\xi_\nu|, \quad |\eta_\mu| < |\eta_\nu|. \tag{4.4}$$

This can be seen as follows. Since step 2 replaces μ by ν and ν by $-\mu$, we have $|\xi_\mu| > |\xi_\nu|$ or $|\xi_\mu| = |\xi_\nu|$ and $|\eta_\mu| > |\eta_\mu|$ after step 2. If at the beginning of step 3, $|\eta_\mu| < |\eta_\nu|$, then from the previous step $|\xi_\mu| > |\xi_\nu|$, so conditions (4.4) hold and step 3 is skipped.

Assume now that $|\eta_\mu| \geq |\eta_\nu|$, so step 3 is entered. Consider step 3 (a) and set $\alpha = \nu$ and $\beta = \lfloor \xi_\mu / \xi_\nu \rfloor \nu - \mu$, so α and β are obtained by applying the linear transformation of step 3 (a) to μ and ν. Then

$$\begin{aligned} |\xi_\beta| &= \left| \left\lfloor \frac{\xi_\mu}{\xi_\nu} \right\rfloor \xi_\nu - \xi_\mu \right| < |\xi_\nu| \;=\; |\xi_\alpha|, \\ |\eta_\beta| &= \left| \left\lfloor \frac{\eta_\mu}{\eta_\nu} \right\rfloor \eta_\nu - \eta_\mu \right| < |\eta_\nu| \;=\; |\eta_\alpha|. \end{aligned}$$

Hence, $|\xi_\nu|$ and $|\eta_\nu|$ strictly decrease in each iteration, so the loop must terminate at the latest before $|\xi_\nu \eta_\nu| \leq 1$, for otherwise by (4.3): $|\sqrt{\Delta(\mathcal{A})}| = |\xi_\nu \eta_\nu| |\eta_\mu / \eta_\nu - \xi_\mu / \xi_\nu| < |\xi_\nu \eta_\nu| \leq 1$, contradicting Theorem 2.1. After step 3 (b), we have $|\xi_\beta| < |\xi_\nu| = |\xi_\alpha|$ and

$$|\eta_\beta| = \left| \left(\left\lfloor \frac{\xi_\mu}{\xi_\nu} \right\rfloor - \left\lfloor \frac{\eta_\mu}{\eta_\nu} \right\rfloor \right) \eta_\nu + \left(\left\lfloor \frac{\eta_\mu}{\eta_\nu} \right\rfloor \eta_\nu - \eta_\mu \right) \right| \geq |\eta_\nu| = |\eta_\alpha|$$

because $|\lfloor \xi_\mu / \xi_\nu \rfloor - \lfloor \eta_\mu / \eta_\nu \rfloor| \geq 1$ and $|\lfloor \eta_\mu / \eta_\nu \rfloor \eta_\nu - \eta_\mu| < |\eta_\nu|$. Finally, observe that in step 3 (c), $a = \lfloor \eta_\mu / \eta_\nu \rfloor$. If we set $\alpha = \mu - a\nu$ and $\beta = \nu$, then as before $|\eta_\alpha| < |\eta_\beta|$, and since $|\xi_\mu| > |\xi_\nu|$, we have $|\xi_\alpha| = |\xi_\mu - a\xi_\nu| = |\xi_\mu| > |\xi_\nu| = |\xi_\beta|$. So step 3 achieves the inequalities (4.4) above.

In step 4, we ensure that $|\eta_\mu| < 1 \leq |\eta_\nu|$. From (4.4), it is clear that at most one of the while loops in step 4 is entered. Consider first the case $|\eta_\nu| < 1$, i.e. case 4 (a). Set $\alpha = \nu$ and $\beta = \lfloor \xi_\mu / \xi_\nu \rfloor \nu - \mu$. Then

$$|\xi_\beta| < |\xi_\nu| = |\xi_\alpha|, \quad |\eta_\beta| = \left| \left\lfloor \frac{\xi_\mu}{\xi_\nu} \right\rfloor \eta_\nu - \eta_\mu \right| > |\eta_\nu| = |\eta_\alpha|, \quad |\eta_\alpha| = |\eta_\nu| < 1,$$

so inequalities (4.4) and the condition $|\eta_\mu| < 1$ are maintained throughout the loop. Furthermore, $|\eta_\nu|$ strictly increases in each iteration, so the while loop will terminate with the desired basis. Step 4 (c) can be analyzed analogously.

Finally, step 5 achieves $|\zeta_\mu|, |\zeta_\nu| < 1$. To see this, let $\alpha = \mu - (1/2)\lfloor\zeta_\mu\rfloor$, then by (4.1) $|\zeta_\alpha| = |\zeta_\mu - (1/2)\zeta_{\lfloor\zeta_\mu\rfloor}| = |\zeta_\mu - \lfloor\zeta_\mu\rfloor| < 1$. Similarly for ν. □

We proceed to prove that the basis of Algorithm 4.1 is indeed a reduced basis, Using the identities (4.2), one can show that if $\alpha \in K$, then $|\alpha'| < 1$ if and only if $|\eta_\alpha| < 1$ and $|\zeta_\alpha| < 1$.

Theorem 4.3. *Let $\{1, \mu, \nu\}$ be a basis of a reduced fractional ideal $\mathcal{A}$ such that $|\zeta_\mu| < 1$, $|\zeta_\nu| < 1$, $|\xi_\mu| > |\xi_\nu|$, $|\eta_\mu| < 1 \le |\eta_\nu|$. Then μ is the minimum adjacent to 1 in $\mathcal{A}$, so $\{1, \mu, \nu\}$ is a reduced basis of $\mathcal{A}$.*

Proof. Let θ be the minimum adjacent to 1 in $\mathcal{A}$, $\theta = l + m\mu + n\nu$ with $l, m, n \in k[t]$. We need to show that $l = n = 0$ and $m \in k^*$. Since $|\theta'| < 1$, we have $|\zeta_\theta| < 1$ and $|\eta_\theta| < 1$. Also $|\zeta_\mu| < 1$ and $|\eta_\mu| < 1$ imply $|\mu'| < 1$. Then $|\mu| > 1$ as otherwise $\mu \in k$. Hence $|\mu| \ge |\theta|$ since otherwise $1 < |\mu| < |\theta|$ and $|\mu'| < 1$, contradicting (M3) for θ. Now $|\xi_\theta| = |2\theta - \zeta_\theta|$, so since $|\zeta_\theta| < 1$ and $|\theta| > 1$, $|\theta| = |\xi_\theta|$. Similarly, $|\mu| = |\xi_\mu|$.

If $n = 0$, then $m \ne 0$ as $\theta \notin k[t]$, so $|m| > |n|$ and $|m\xi_\mu| > |n\xi_\nu|$. If $n \ne 0$, then $1 > |\eta_\theta| = |m\eta_\mu + n\eta_\nu|$ with $|n\eta_\nu| \ge 1$ implies $|m\eta_\mu| = |n\eta_\nu|$. Thus, $|n| \le |n\eta_\nu| = |m\eta_\mu| < |m|$, so $|m| > |n|$ and $|m\xi_\mu| > |n\xi_\nu|$ as well. It follows that

$$|\theta| = |\xi_\theta| = |m\xi_\mu + n\xi_\nu| = |m\xi_\mu| = |m\mu| \ge |m\theta|,$$

so $|m| \le 1$. Thus, $1 \ge |m| > |n|$, so $n = 0$ and $m \in k^*$.

Now $1 > |\zeta_\theta| = |\zeta_{l+m\mu}| = |2l + \zeta_\mu|$, so since $|\zeta_\mu| < 1$, $|l| < 1$, so $l = 0$ and $\theta = m\mu \in k^*\mu$. □

The coefficients of the basis generated by Algorithm 4.1 are small:

Theorem 4.4. *Let $\mathcal{A}$ be a reduced fractional ideal and let $\{1, \mu, \nu\}$ be the basis of $\mathcal{A}$ produced by Algorithm 4.1. Let $\mu = (m_0 + m_1\rho + m_2\omega)/d$, $\nu = (n_0 + n_1\rho + n_2\omega)/d$ with $m_0, m_1, m_2, n_0, n_1, n_2, d \in k[t]$ and* $\gcd(m_0, m_1, m_2, n_0, n_1, n_2, d) = 1$. *Then $|d| < |d\mu| = |m_0| = |m_1\rho| = |m_2\omega| \le |\sqrt{\Delta}|$, and $|n_0|, |n_1\rho|, |n_2\omega| < |\sqrt{\Delta}|$.*

Proof. $|d| < |d\mu|$ follows from $|\mu| > 1$. From $|\mu| > 1$ and $|\zeta_\mu| = |3m_0/d - \mu| < 1$, it follows that $|d\mu| = |m_0|$. The inequalities $|\xi_\mu| > 1$ and $|\eta_\mu| < 1$ imply $|m_1\rho| = |m_2\omega| = |d\xi_\mu|$. From $|\zeta_\mu| = |2m_0/d - \xi_\mu| < 1$, we obtain $|d\xi_\mu| = |m_0|$. So $|d| < |d\mu| = |m_0| = |m_1\rho| = |m_2\omega|$.

Now $d\mathcal{A}$ is a reduced integral ideal with $L(d\mathcal{A}) = \operatorname{sgn}(d)^{-1}d$, so $d^3N(\mathcal{A}) = N(d\mathcal{A}) \mid d^2$, and thus $|dN(\mathcal{A})| \le 1$. From (2.1) and (4.3), we obtain

$$|\sqrt{\Delta}| \ge |dN(\mathcal{A})\sqrt{\Delta}| = |d\sqrt{\Delta(\mathcal{A})}| = |d(\xi_\mu\eta_\nu - \xi_\nu\eta_\mu)| \ge |d\xi_\mu|$$

as $|\xi_\mu| > |\xi_\nu|$ and $|\eta_\mu| < 1 \le |\eta_\nu|$.

Since $|\xi_\mu| > |\xi_\nu|$, we have $|\sqrt{\Delta}| \geq |m_1\rho + m_2\omega| > |n_1\rho + n_2\omega|$. Also, $|\sqrt{\Delta(\mathcal{A})}| = |\xi_\mu\eta_\nu| > |\eta_\nu|$, so $|\sqrt{\Delta}| > |d\eta_\nu| = |n_1\rho - n_2\omega|$. Hence $|n_1\rho|, |n_2\omega| < |\sqrt{\Delta}|$. Finally, $|\zeta_\nu| < 1$ implies $|2n_0 - n_1\rho + n_2\omega| < |d| < |\sqrt{\Delta}|$, so $|n_0| < |\sqrt{\Delta}|$. □

5 Implementation

We implemented our algorithm on a Silicon Graphics Challenge workstation using the computer algebra system SIMATH developed by the research group of Professor H. G. Zimmer at the Universität des Saarlandes in Saabrücken, Germany. To compute with Puiseux series, it was necessary to use truncated series as approximations, in analogy to using rational approximations when computing with real numbers. To that end, we employed the method for extracting cube roots as described in [8] and implemented by Mang in [9] to compute "approximations" $\hat{\rho}$ and $\hat{\omega}$ of the basis elements ρ and ω, respectively. That is, if $\rho = \sum_{i=-\deg(\rho)}^{\infty} r_i/t^i$, then for $\delta \geq 0$, $\hat{\rho} = \sum_{i=-\deg(\rho)}^{\delta} r_i/t^i$ is an *approximation of precision* δ to ρ, so $|\rho - \hat{\rho}| < q^{-\delta}$. Similarly for ω. In contrast to Voronoi's algorithm in number fields, it was possible to establish conditions on the required precision δ that could be checked throughout the algorithm; it is a simple matter to flag the cases where the precision is not large enough and increase it as required. It turned out that a uniform precision of $\delta = \deg(\Delta)$ was sufficient throughout our computations. Examples show that reducing the precision to $\deg(\Delta)/2$ or even $\deg(\Delta)/4$ might still produce correct results, but computation times improved only marginally with smaller precision.

Since the polynomials and series approximations in our algorithm generally had few zero coefficients, they were given in *dense representation*; that is, as a list starting with the degree of the polynomial or the series, followed by the coefficients in order of decreasing degree of monomial.

The main difficulty in our implementation was the computation of the principal parts of quotients as required in steps 3 – 5 of Algorithm 4.1. Here, an approximation $\hat{\xi}_\mu$ of $\xi_\mu = (m_1\rho + m_2\omega)/d$ was represented as a pair (α_μ, d) where $\alpha_\mu = m_1\hat{\rho} + m_2\hat{\omega}$; similarly for ξ_ν, η_μ, and η_ν. To compute a quotient $\lfloor \xi_\mu/\xi_\nu \rfloor$ for example, we performed "division with remainder" on the quanitities α_μ and $\alpha_\nu = n_1\hat{\rho} + n_2\hat{\omega}$. Note that it is possible to reduce the division with remainder of two truncated series to a division of a truncated series by just a polynomial by using formulas such as

$$\frac{\xi_\mu}{\xi_\nu} = \frac{A - B\eta_\nu}{C}$$

where

$$A = m_1 n_1^2 H + m_2 n_2^2 G, \quad B = m_1 n_2 - m_2 n_1, \quad C = n_1^3 H + n_2^3 G.$$

Then $\lfloor \xi_\mu/\xi_\nu \rfloor = \lfloor (A - B\hat{\eta}_\nu)/C \rfloor$, provided $|n_1|, |n_2| < |C|$ which is extremely likely. Here, $\hat{\eta}_\nu$ is an approximation of precision $\deg(B)$ to η_ν. Similar formulas, involving different values of A and C, but using the same B value, hold for the other quotients. Note that $N(d\mathcal{A}) = dB/\mathrm{sgn}(dB)$, so B is independent of the basis and need only be computed once per reduction. Furthermore, $|B| < |\Delta|/|d| \leq |\Delta|$ by Corollary 2.2, so $\deg(B) < \deg(\Delta)$. We performed computations with both explicit division with remainder and the above formulas, and the division with remainder version of the algorithm turned out to be about 20 percent faster.

In step 5 of Algorithm 3.1, we approximate $\zeta_\mu = 2m_0/d + \xi_\mu$ by $\hat{\zeta}_\mu = (2m_0 + \alpha_\mu)/d$. Then the principal part $\lfloor \zeta_\mu \rfloor$ of ζ_μ can be computed as simply $\lfloor (2m_0 - \alpha_\mu)/d \rfloor$. This will always produce the correct polynomial as $|\zeta_\mu - (2m_0 + \alpha_\mu)/d| < \max\{|m_1|, |m_2|\}/|d|\, q^{-\delta} < 1$ since $|d| \geq 1$ and at this point $|m_1|, |m_2| < |\sqrt{\Delta}|$ by Theorem 4.4. Similarly for ζ_ν.

6 Numerical Examples

All our examples were done over prime fields $k = \mathbb{F}_p$ where p is a prime with $p \equiv -1 \pmod 3$, and used monic polynomials G and H. Not surprisingly, our regulator algorithm was significantly faster than our unit algorithm due to the time-consuming polynomial arithmetic involved in updating θ_n in step 2 (b) of each iteration of Algorithm 3.1.

The largest unit we computed was the fundamental unit ϵ of $K = \mathbb{F}_{17}(\sqrt[3]{GH^2})$ where $G = t + 4$ and $H = t^4 + t^3 + 11t^2 + 5t + 12$. Here, $\epsilon = e_0 + e_1\rho + e_2\omega$ where $\deg(e_0) = 1554$, $\deg(e_1) = 1551$, and $\deg(e_2) = 1552$, so $|\epsilon| = 17^{1554}$, a number of 3109 decimal digits. The period of ϵ is 775. It took just under 15 CPU minutes to compute ϵ.

For the examples given in the table below, we randomly generated monic polynomials $G, H \in \mathbb{F}_p[t]$ so that $\deg(GH^2) \equiv 0 \pmod 3$, G and H are both squarefree, and $\gcd(G, H) = 1$. Each row of the table specifies the prime p, the polynomials G and H, the period l of the fundamental unit ϵ of $K = \mathbb{F}_p(t, \sqrt[3]{GH^2})$, the regulator R of K, and the CPU time required to compute R.

We point out that for small genus and large field of constants, knowledge of the regulator oftentimes uniquely determines the divisor class number h of the field, or at least narrows h down to only a few possible values. From the Hasse-Weil Theorem (see [13, Theorem V.1.15, p. 166, and Theorem V.2.1 , p. 169]), we can infer that $(\sqrt{q} - 1)^{2g} \leq h \leq (\sqrt{q} + 1)^{2g}$. By (1.2), h is a multiple of R. Usually, there are only a few multiples of R that fall within these bounds. For example, the last five examples in our table below each permit only three possible values for h. We plan to investigate the computation of a suitable approximation of h by means of truncated Euler products in a forthcoming paper.

Table 1. Regulator Computations

p	G	H	l	R	*Time*
5	$t+4$	$t^7+t^6+t^5+4t^4+2t^3+t^2+t+1$	6387	6655	38.52 sec
5	t^2+4t+2	$t^8+t^7+3t^5+3t^4+3t^3+2t^2+t+2$	57105	59501	8 min 13 sec
5	$t^4+t^3+2t^2+3t+3$	t^4+t^2+2t+3	2834	2950	17.31 sec
5	$t^5+t^4+3t^3+2t^2+2t+4$	$t^5+t^4+4t^3+4t^2+3$	251783	262322	37 min 9 sec
11	$t+4$	$t^7+4t^6+2t^5+9t^3+t^2+4t+10$	189893	191487	22 min 58 sec
11	t^3+4t^2+7t+8	t^3+2t^2+t+1	855	870	3.97 sec
11	t^4+10t^2+2t+6	$t^4+2t^3+10t^2+6t+6$	122619	123718	15 min 7 sec
11	$t^5+2t^4+8t^3+t^2+t+2$	t^2+4t+8	61702	62204	8 min 45 sec
17	$t^3+9t^2+12t+2$	t^3+5t^2+3t+5	31987	32077	2 min 40 sec
17	$t^4+15t^3+12t^2+14t+6$	$t+3$	892	894	3.38 sec
17	$t^5+3t^4+13t^3+15t^2+7t+13$	t^2+6t+3	562601	564510	58 min 3 sec
23	$t+3$	$t^4+3t^3+17t+13$	1145	1146	4.20 sec
23	t^3+5t+2	t^3+22t^2+2t+2	102347	102553	8 min 42 sec
23	$t^4+22t^3+16t^2+4t+4$	$t+7$	4251	4256	16.50 sec
23	$t^5+15t^4+16t^3+16t^2+4t+16$	$t^2+21t+10$	744378	745808	1 h 21 min
29	$t^3+24t^2+12t+24$	$t^3+16t^2+10t+1$	80008	80103	7 min 3 sec
29	$t^4+22t^3+17t^2+12$	$t+5$	8508	8520	33.62 sec
29	$t^5+27t^4+13t^3+10t^2+23t+3$	$t^2+4t+17$	1483564	1485310	2 h 44 min
41	$t^4+15t^3+4t^2+37t+14$	$t+28$	24238	24248	1 min 37 sec
41	$t^3+30t^2+35t+9$	$t^3+29t^2+15t+38$	961413	962005	1 h 25 min
71	$t^4+9t^3+9t^2+3t+20$	$t+56$	41058	41064	2 min 49 sec
71	$t^3+30t^2+37t+2$	$t^3+13t^2+66t+34$	1408409	1408658	2 h 7 min
89	$t^2+8t+56$	$t^2+22t+67$	1317	1318	3.87 sec
89	$t^4+23t^3+50t^2+67t+35$	$t+79$	116511	116520	8 min 1 sec
107	$t^2+58t+74$	$t^2+54t+86$	3862	3863	11.98 sec
197	$t^2+27t+125$	$t^2+65t+158$	6525	6526	20.20 sec
401	$t^2+51t+400$	$t^2+71t+59$	26925	26926	1 min 24 sec
797	$t^2+526t+353$	$t^2+765t+687$	70680	70681	3 min 42 sec
983	$t^2+15t+279$	$t^2+740t+864$	107574	107575	5 min 33 sec

References

1. Buchmann, J. A.: A generalization of Voronoi's algorithm I, II. J. Number Theory **20** (1985) 177-209
2. Buchmann, J. A.: The computation of the fundamental unit of totally complex quartic orders. Math. Comp. **48** (1987) 39–54
3. Buchmann, J. A.: On the computation of units and class numbers by a generalization of Lagrange's algorithm. J. Number Theory **26** (1987) 8–30
4. Buchmann, J. A.: On the period length of the generalized Lagrange algorithm. J. Number Theory **26** (1987) 31–37
5. Buchmann, J. A.: Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper. Habilitationsschrift, Universität Düsseldorf, Germany, (1987)
6. Buchmann, J. A., Williams, H. C.: On the infrastructure of the principal ideal class of an algebraic number field of unit rank one. Math. Comp. **50** (1988) 569–579
7. Delone, B. N.,Fadeev, D. K.: The Theory of Irrationalities of the Third Degree. Transl. Math. Monographs **10**, Amer. Math. Soc., Providence, Rhode Island (1964)
8. Jung, E.: Theorie der Algebraischen Funktionen einer Veränderlichen. Berlin (1923)
9. Mang, M.: Berechnung von Fundamentaleinheiten in algebraischen, insbesondere rein-kubischen Kongruenzfunktionenkörpern. Diplomarbeit, Universität des Saarlandes, Saarbrücken, Germany, (1987)
10. Pohst, M., Zassenhaus, H.: Algorithmic Algebraic Number Theory. Cambridge University Press, 1st paperpack ed., Cambridge (1997)
11. Scheidler, R., Stein, A.: Voronoi's Algorithm in Purely Cubic Congruence Function Fields of Unit Rank 1 (in preparation)
12. Stein, A., Williams, H. C.: Some Methods for Evaluating the Regulator of a Real Quadratic Function Field. Experimental Mathematics (to appear)
13. Stichtenoth, H.: Algebraic Function Fields and Codes. Springer, Berlin (1993)
14. Voronoi, G. F.: On a Generalization of the Algorithm of Continued Fractions (in Russian). Doctoral Dissertation, Warsaw, Poland, (1896)
15. Williams, H. C.: Continued fractions and number-theoretic computations. Rocky Mountain J. Math. **15** (1985) 621–655
16. Williams, H. C., Cormack, G., Seah, E.: Calculation of the regulator of a pure cubic field. Math. Comp. **34** (1980) 567–611
17. Williams, H. C., Dueck, G. W., Schmid, B. K.: A rapid method of evaluating the regulator and class number of a pure cubic field. Math. Comp. **41** (1983) 235–286