

## COMPUTING DISCRETE LOGARITHMS IN REAL QUADRATIC CONGRUENCE FUNCTION FIELDS OF LARGE GENUS

VOLKER MÜLLER, ANDREAS STEIN, AND CHRISTOPH THIEL

ABSTRACT. The discrete logarithm problem in various finite abelian groups is the basis for some well known public key cryptosystems. Recently, real quadratic congruence function fields were used to construct a public key distribution system. The security of this public key system is based on the difficulty of a discrete logarithm problem in these fields. In this paper, we present a probabilistic algorithm with subexponential running time that computes such discrete logarithms in real quadratic congruence function fields of sufficiently large genus. This algorithm is a generalization of similar algorithms for real quadratic number fields.

### 1. INTRODUCTION

A lot of public key cryptosystems are based on the difficulty of a *discrete logarithm problem* (DL problem) in some finite abelian group. For some groups, such as the multiplicative group  $\mathbb{F}_q^*$  of a finite field (see [10]), or the class group of a real quadratic number field (see [1]), subexponential algorithms for solving the DL problem are known. Using the infrastructure of the set  $\mathcal{R}$  of reduced principal ideals of a real quadratic congruence function field (that is very similar to the infrastructure of the cycle of reduced ideals of a real quadratic number field; see [5], [24], et al.), Scheidler, Stein and Williams (see [21]) recently constructed a public key distribution system. To break their system, it is sufficient to solve the following problem: given an integral basis of a reduced principal ideal  $\mathfrak{A}$ , find the degree of an arbitrary generator of  $\mathfrak{A}$ . If one has found a generator of  $\mathfrak{A}$ , one has solved the problem. Note that, in general, the integral basis of  $\mathfrak{A}$  does not imply a generator of  $\mathfrak{A}$ . In this paper, we will describe a probabilistic algorithm with subexponential running time that solves that problem provided the genus of the function field is at least logarithmic in the order of the field of constants. To be more precise, the algorithm finds, for an arbitrary principal ideal, the degree of one of its generators. We also describe an extension of our algorithm that can be used to solve the real quadratic congruence function field DL problem defined in [21] in subexponential time.

---

Received by the editor March 25, 1996 and, in revised form, September 10, 1997.

1991 *Mathematics Subject Classification*. Primary 11Y16, 11R29; Secondary 11T71, 11R58, 68Q25, 94A60.

*Key words and phrases*. Discrete logarithm, class group, subexponential algorithm, real quadratic congruence function field.

This research was supported by the Deutsche Forschungsgemeinschaft.

We start our description of the algorithm by summarizing some basics about algebraic congruence function fields. In Section 2, we describe the main algorithm of this paper which solves the given problem. Section 3 describes some theoretical results concerning generating systems for the ideal class group. In Section 4, we estimate the probability that we have found a generating system for some lattice. This probability is used in Section 5 to compute the expected running time of the algorithm of this paper.

**1.1. Basic definitions.** The following basic information about congruence function fields can be found in [7], [22], [2] and [32].

Let  $K/k$  be an *algebraic congruence function field* of one variable over the finite field  $k = \mathbb{F}_q$  of *constants* of odd characteristic with  $q$  elements, and let  $x \in K$  be such that  $K$  is a finite, separable extension of the rational function field  $k(x)$ . The *ring of integers* of  $K$  is  $\mathcal{O} = \overline{k[x]}$ , i.e. the integral algebraic closure of  $k[x]$  in  $K$ . The ring  $\mathcal{O}$  is a Dedekind domain. The set  $\mathcal{I}$  of fractional  $\mathcal{O}$ -ideals in  $K$  forms a group with the set  $\mathcal{H}$  of principal  $\mathcal{O}$ -ideals  $\alpha\mathcal{O}$  ( $\alpha \in K^*$ ) as a subgroup. Denote by  $\text{Cl} = \mathcal{I}/\mathcal{H}$  the *ideal class group* of  $K$ . Its order  $h'$  is called the *ideal class number* of  $K$  with respect to  $\mathcal{O}$ . Furthermore, we denote by  $\mathcal{D}$ ,  $\mathcal{D}_0$ ,  $\mathcal{P}$ ,  $\mathcal{C} = \mathcal{D}/\mathcal{P}$  the *group of divisors*, the *group of divisors of degree 0*, the *group of principal divisors* and the *divisor class group* of  $K/k$ , respectively. The group  $\mathcal{C}_0 = \mathcal{D}_0/\mathcal{P}$  of all divisor classes of degree 0 is called the *zero class group* and its order  $h$  the *divisor class number* of  $K/k$ . Let  $\mathcal{U}$  be the subgroup of  $\mathcal{D}$  generated by the set of infinite places of  $K/k$  with respect to  $\mathcal{O}$ , and let  $\mathcal{U}_0 = \mathcal{U} \cap \mathcal{D}_0$ . We know that

$$(1) \quad \mathcal{I} \cong \mathcal{D}/\mathcal{U},$$

$$(2) \quad \text{Cl} = \mathcal{I}/\mathcal{H} \cong \mathcal{D}/\mathcal{P}\mathcal{U},$$

and

$$(3) \quad h' = \frac{h[\mathcal{D} : (\mathcal{D}_0\mathcal{U})]}{[\mathcal{U}_0 : (\mathcal{P} \cap \mathcal{U}_0)]},$$

where the index  $R := [\mathcal{U}_0 : (\mathcal{P} \cap \mathcal{U}_0)]$  is called the *regulator* of  $K$  with respect to  $\mathcal{O}$ .

A quadratic extension  $K$  of the rational function field  $\mathbb{F}_q(x)$  is called a *quadratic congruence function field*. The ring of integers of a quadratic congruence function field  $K$  is

$$\mathcal{O} = \mathbb{F}_q[x][\sqrt{D}] = \mathbb{F}_q[x] + \mathbb{F}_q[x]\sqrt{D}.$$

We say that  $K$  is a *real quadratic congruence function field*, if  $K$  is of the form

$$K = \mathbb{F}_q(x)(\sqrt{D}) = \mathbb{F}_q(x) + \mathbb{F}_q(x)\sqrt{D},$$

where  $D \in \mathbb{F}_q[x]$  is a monic, square-free polynomial of even degree (this is in analogy to the case of a real quadratic number field  $\mathbb{Q}(\sqrt{\Delta})$ , where  $\Delta$  is a positive, square-free integer). In this case, the infinite place  $\mathfrak{P}_\infty$  of  $\mathbb{F}_q(x)$  splits completely in  $K$  as  $\mathfrak{P}_\infty = \mathfrak{P}_1 \cdot \mathfrak{P}_2$ , where  $\mathfrak{P}_1$  and  $\mathfrak{P}_2$  are the infinite places of  $K$  with respect to  $\mathcal{O}$ . For  $\alpha = u + v\sqrt{D} \in K$ , where  $u, v \in \mathbb{F}_q(x)$ , we denote by  $\bar{\alpha} = u - v\sqrt{D}$  its *conjugate*. The *norm* of  $\alpha$  is defined as  $N(\alpha) = \alpha\bar{\alpha} = u^2 - v^2D$ .

In this case,  $\mathbb{F}_q((1/x))$  is the completion of  $\mathbb{F}_q(x)$  with respect to  $\infty$ , and the completions of  $K$  with respect to  $\mathfrak{P}_1$  and  $\mathfrak{P}_2$  are isomorphic to  $\mathbb{F}_q((1/x))$ . Also,  $K \leq \mathbb{F}_q((1/x))$ . Let  $\mathfrak{P}_1$  be the place which corresponds to the branch where  $\sqrt{1} = 1$ . We then consider elements of  $K$  as Laurent series at  $\mathfrak{P}_1$  in  $1/x$ . Now, let

$\alpha \in \mathbb{F}_q((1/x))$  be a non-zero element. Then  $\alpha = \sum_{i=-\infty}^m c_i x^i$  with  $c_m \neq 0$ . We denote by  $\deg(\alpha) = m$  the *degree* of  $\alpha$ , by  $|\alpha| = q^m$  the *absolute value* of  $\alpha$ , by  $\text{sgn}(\alpha) = c_m$  the *sign* of  $\alpha$ , and by  $[\alpha] = \sum_{i=0}^m c_i x^i$  the *principal part* of  $\alpha$ . If  $m$  is negative, then  $[\alpha] = 0$ . We set  $\deg(0) = -\infty$  and  $|0| = 0$ .

In analogy to the case of a real quadratic number field, the *unit group*  $E$  of  $K$  is of the form  $E = \mathbb{F}_q^* \times \langle \epsilon \rangle$ , where  $\epsilon \in K$  is a *fundamental unit* of  $K$ . Then,  $R = \deg(\epsilon)$ .

**1.2. Ideals.** We summarize the most important facts about ideals of  $\mathcal{O}$  (cf. [2], [26]). Any non-zero integral ideal  $\mathfrak{A}$  of  $\mathcal{O}$  can be written as

$$\mathfrak{A} = SQ\mathbb{F}_q[x] + (SP + S\sqrt{D})\mathbb{F}_q[x],$$

where  $S, P, Q \in \mathbb{F}_q[x]$  with  $Q|(D - P^2)$  and  $\text{sgn}(S) = \text{sgn}(Q) = 1$ . The polynomials  $S$  and  $Q$  are uniquely determined, and  $P$  is unique modulo  $Q$ . This representation is called a *standard representation* of  $\mathfrak{A}$ . The set  $\{SQ, SP + S\sqrt{D}\}$  is called an  $\mathbb{F}_q[x]$ -basis of  $\mathfrak{A}$ . An ideal is called *primitive* if  $S = 1$ . If  $\mathfrak{A}$  is given in standard representation, then the *norm* of  $\mathfrak{A}$  is defined by

$$N(\mathfrak{A}) = \frac{QS^2}{\text{sgn}(QS^2)} \in \mathbb{F}_q[x].$$

The *absolute norm* of  $\mathfrak{A}$  is defined by  $|N(\mathfrak{A})|$ .

**Lemma 1.** *If  $\mathfrak{A}$  and  $\mathfrak{B}$  are integral ideals then  $N(\mathfrak{A}\mathfrak{B}) = N(\mathfrak{A})N(\mathfrak{B})$ . If  $\mathfrak{A} = \alpha\mathcal{O}$ , where  $\alpha \in \mathcal{O}$ , then there exists  $c \in \mathbb{F}_q$  such that  $N(\mathfrak{A}) = c \cdot N(\alpha)$ .*

If  $\mathfrak{A}$  is a non-zero ideal of  $\mathcal{O}$ , then we denote by  $\overline{\mathfrak{A}}$  the ideal that contains the elements that are conjugates of the elements of  $\mathfrak{A}$ .

We say that two ideals  $\mathfrak{A}, \mathfrak{B}$  of  $\mathcal{O}$  are equivalent if there exists  $\alpha \in K^*$  (i.e.  $\alpha \neq 0$ ) such that  $\alpha\mathfrak{B} = \mathfrak{A}$ . The equivalence classes of that equivalence relation are called *ideal classes*. The ideal classes form a finite group, the *ideal class group*  $\text{Cl}$ , whose order is denoted by  $h'$ , the *ideal class number*. If  $\mathfrak{A}$  is a non-zero ideal of  $\mathcal{O}$  then we denote the corresponding ideal class by  $[\mathfrak{A}]$ . Given two ideals, we can compute their product in polynomial time.

The theory of prime ideals is analogous to the case of real quadratic number fields. Every ideal can be uniquely factored (up to the order) into a product of prime ideals. We are especially interested in the set  $\mathcal{P}$  of those prime ideals that *split completely* or *ramify*. By [2], they can be obtained in the following way: For each  $P \in \mathbb{F}_q[x]$  that is monic and irreducible such that  $P$  does not divide  $D$  and  $D$  is a square modulo  $P$ , the principal ideal  $(P)$  splits into a product of two conjugate prime ideals with bases  $\{P, B + \sqrt{D}\}$  and  $\{P, B - \sqrt{D}\}$ , where  $B$  is a square root of  $D \pmod{P}$ . For each monic and irreducible divisor  $P$  of  $D$ ,  $(P)$  is the square of a prime ideal with base  $\{P, \sqrt{D}\}$ . For  $C \in \mathbb{Z}_{>0}$ , we say that an ideal is  $\mathcal{P}$ - $C$ -smooth if it can be factored into a product of prime ideals in  $\mathcal{P}$  of absolute norm bounded by  $q^C$ . Given a  $\mathcal{P}$ - $C$ -smooth ideal, such a factorization can be computed in  $O(k_C \deg(D)^3 \log q)$  operations in  $\mathbb{F}_q$ , where  $k_C$  is the cardinality of  $\mathcal{P}$ .

A primitive ideal  $\mathfrak{A}$  is called *reduced* if there exists a standard representation of the form  $\mathfrak{A} = Q\mathbb{F}_q[x] + (P + \sqrt{D})\mathbb{F}_q[x]$ , where  $|P - \sqrt{D}| < |Q| < |P + \sqrt{D}|$ . This *reduced basis* representation is unique.

**Lemma 2.** *Let  $\mathfrak{A}$  be a primitive ideal with standard representation  $\mathfrak{A} = Q\mathbb{F}_q[x] + (P + \sqrt{D})\mathbb{F}_q[x]$ . Then  $\mathfrak{A}$  is reduced if and only if  $|N(\mathfrak{A})| = |Q| < |\sqrt{D}|$ .*

In [26], [21], the *infrastructure* of the set of reduced ideals is explained in detail. Here, we only give a short overview. The set of reduced ideals belonging to the same equivalence class is bounded by the regulator  $R$ . If  $\mathfrak{A}$ ,  $\mathfrak{B}$  are two equivalent reduced principal ideals then we define the *distance from  $\mathfrak{A}$  to  $\mathfrak{B}$*  by  $\delta(\mathfrak{B}, \mathfrak{A}) = \deg(\bar{\theta})$ , where  $\mathfrak{B} = \bar{\theta}\mathfrak{A}$ . Given any ideal  $\mathfrak{A}$  of  $\mathcal{O}$  and  $y \in \mathbb{Z}$ , we can find in polynomial time a reduced ideal  $\mathfrak{B}$  with  $\alpha\mathfrak{B} = \mathfrak{A}$ , with  $\alpha \in K$  such that  $|\deg(\alpha) - y| \leq |\deg(\alpha') - y|$  for all  $\alpha' \in K$  with  $\alpha'\mathfrak{B}' = \mathfrak{A}$  and  $\mathfrak{B}'$  is reduced. We say that  $\mathfrak{B}$  is *closest* to  $y$  with respect to  $\mathfrak{A}$ . By [26], we have

$$(4) \quad 1 \leq |\deg(\alpha) - y| \leq \deg(D)/2.$$

Moreover, we can determine  $\deg(\alpha)$  in polynomial time.

**1.3. The problem.** In this paper, we present an algorithm for solving the following problem: given two polynomials  $P, Q \in \mathbb{F}_q[x]$  such that  $\{Q, P + \sqrt{D}\}$  is an  $\mathbb{F}_q[x]$ -basis of an arbitrary principal ideal of  $\mathcal{O}$ , compute the degree of a generator of that ideal. We will describe a probabilistic algorithm with subexponential running time which solves that problem provided the genus of the function field is “sufficiently large”. If we want to find the degree of the generator of a reduced principal ideal modulo the regulator  $R$ , we say that we have to compute the so called *discrete logarithm* of the ideal. We will also explain how the discrete logarithm problem can be solved in subexponential running time. Using these algorithms, it is possible to break the key exchange system of [21] in subexponential time.

## 2. THE ALGORITHM

**2.1. The main idea.** In this section, we describe the main ideas used in our algorithm to compute a generator of a given principal ideal and the degree of that generator. The idea of our algorithm is similar to the algorithm of Hafner and McCurley [18] (resp. of Buchmann [4] and Abel [1]) for computing the class group and the regulator of imaginary quadratic (resp. real quadratic) number fields. In both cases, it could be proved under the assumption of the generalized Riemann Hypothesis (GRH) that the expected running time of these methods is  $L(D)^{\sqrt{2}+o(1)}$ , where  $L(D) = \exp \sqrt{\log D \log \log D}$ . These algorithms can also be used to find generators of principal ideals (this is explained in [1] or [6] in more detail). We will apply the ideas to real quadratic congruence function fields. Note that the analogous Riemann Hypothesis holds for function fields (see [31]).

In the following, we shall always assume that the degree of  $D$  is at least 4. This is no restriction since it is known that  $R = 1$  for  $\deg(D) = 2$ . But then the given problem can be solved in polynomial time.

**2.2. The factor basis.** Our algorithm makes use of the fact that the ideal class group  $\text{Cl}$  of a real quadratic congruence function field is generated by prime ideals of small absolute norm. In the case of real quadratic number fields, it could be proven (see [3]) that if GRH is true then the class group is generated by the classes containing prime ideals of norm at most  $12(\log(\Delta))^2$ , where  $\Delta$  is the discriminant. For real quadratic congruence function fields, a completely analogous result, up to the fact that here GRH is known to be true, will be proven in Section 3 of this paper.

For  $C \in \mathbb{Z}_{>0}$ , we define

$$F_C = \{\mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}, |N(\mathfrak{p})| \leq q^C\} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{k_C}\}.$$

Using the estimates in [16, p. 59] or [27, Lemma 6.2.3], we see that  $F_C$  is a finite set of size  $k_C \leq 4Cq^C$ . Hence, the set  $F_C$  can be computed in  $O(Cq^C \deg(D)^3 \log q)$  operations in  $\mathbb{F}_q$ . Note that this bound for the size of the factor basis is polynomial in the length of the input. In the complexity analysis of the algorithm in Section 5, however, we expand the factor basis to subexponential size.

We assume that we have found a number  $C$  such that the equivalence classes of the ideals  $\mathfrak{p}_i \in F_C$  generate the whole ideal class group  $\text{Cl}$ . In Theorem 4 we will prove an explicit bound for  $C$  (we show that  $q^C \approx (2 \deg(D) - 5)^2$ ).

Next, we consider the sets

$$(5) \quad \Gamma_C = \left\{ (v_1, \dots, v_{k_C}, \deg(\alpha)) \mid (v_1, \dots, v_{k_C}) \in \mathbf{Z}^{k_C} \text{ and } \prod_{i=1}^{k_C} \mathfrak{p}_i^{v_i} = \alpha \mathcal{O} \right\},$$

and

$$(6) \quad \Gamma'_C = \left\{ (v_1, \dots, v_{k_C}) \mid (v_1, \dots, v_{k_C}) \in \mathbf{Z}^{k_C} \text{ and } \prod_{i=1}^{k_C} \mathfrak{p}_i^{v_i} \text{ is principal} \right\}.$$

Similarly, as in [4], we have the following.

**Theorem 1.** *Suppose, that the prime ideals in  $F_C$  generate the class group. Then the set  $\Gamma_C$  is a  $(k_C + 1)$ -dimensional lattice of determinant  $h'R$ . The set  $\Gamma'_C$  is a  $k_C$ -dimensional lattice of determinant  $h'$ .*

To find a generator of a given principal ideal  $\mathfrak{A}$ , we construct a generating system  $B_C$  of  $\Gamma_C$ . Suppose that

$$(7) \quad B_C = \begin{pmatrix} b_{1,1} & \dots & b_{1,k_C} & b_{1,k_C+1} & \dots & b_{1,N} \\ & & \vdots & \vdots & & \vdots \\ & & \vdots & \vdots & & \vdots \\ \hline b_{k_C,1} & \dots & b_{k_C,k_C} & b_{k_C,k_C+1} & \dots & b_{k_C,N} \\ \deg(\beta_1) & \dots & \deg(\beta_{k_C}) & \deg(\beta_{k_C+1}) & \dots & \deg(\beta_N) \end{pmatrix},$$

where  $N \geq k_C + 1$ . Then  $(b_{1,j}, \dots, b_{k_C,j}, \deg(\beta_j)) \in \Gamma_C$  and

$$(8) \quad \prod_{i=1}^{k_C} \mathfrak{p}_i^{b_{i,j}} = \beta_j \mathcal{O}, \quad 1 \leq j \leq N.$$

Now, by removing the last line in  $B_C$ , we obtain a matrix  $B'_C$  whose columns are a generating system of  $\Gamma'_C$ . How can we use  $B'_C$  to find a generator of a given principal ideal  $\mathfrak{A}$ ? To show this, we distinguish two situations:

If we can factor  $\mathfrak{A}$  over the factor basis  $F_C$ , then  $\mathfrak{A}$  is of the form  $\mathfrak{A} = \prod_{i=1}^{k_C} \mathfrak{p}_i^{z_i}$ . Hence,  $\underline{z} = (z_1, \dots, z_{k_C}) \in \Gamma'_C$  and therefore there exists  $\underline{x} \in \mathbf{Z}^N$  such that

$$(9) \quad B'_C \cdot \underline{x} = \underline{z}.$$

From (8) and (7) it follows that  $\prod_{i=1}^N \beta_i^{x_i}$  is a generator of  $\mathfrak{A}$  of degree

$$(10) \quad \sum_{i=1}^N x_i \deg(\beta_i).$$

If  $\mathfrak{A}$  cannot be factored over the factor basis, then we use the following standard trick. We try to find an equivalent principal ideal  $\alpha \mathfrak{B} = \mathfrak{A}$  ( $\alpha \in K$ ) that can be

factored over the factor basis. If we succeed and find a generator  $\beta$  of  $\mathfrak{B}$  by the method given above, then  $\mathfrak{A}$  is generated by  $\alpha \cdot \beta$ .

**2.3. Generating relations.** To construct the above mentioned generating system  $B_C$ , we find *random* vectors of  $\Gamma_C$ . This will be done in a way very similar to the case of real quadratic number fields (see [1, Section 5.3]):

We pick at random a vector  $\underline{e} = (e_1, \dots, e_{k_C}) \in \{0, \dots, |D|\}^{k_C}$  and  $y \in \{0, \dots, |D|\}$ . Then we compute a pair  $(\mathfrak{B}, \deg(\alpha))$  where  $\mathfrak{B}$  is a reduced ideal that is equivalent to

$$(11) \quad \mathfrak{A} = \prod_{i=1}^{k_C} \mathfrak{p}_i^{e_i}$$

and closest to  $y$  with respect to  $\mathfrak{A}$ , and where  $\alpha \in K$  is such that  $\alpha\mathfrak{B} = \mathfrak{A}$ . Using the algorithms described in [26] and [21] (see also [5] and [1] for the case of real quadratic number fields), this computation can be done in  $O(k_C \deg(D)^3 C^3 \log q)$  operations in  $\mathbb{F}_q$ . We note that we compute  $\mathfrak{B}$  and  $\alpha$  without explicitly computing the ideal  $\mathfrak{A}$ , whose size may be exponential. We do this by using well known fast exponentiation methods and by reducing each intermediate power and product. This technique is again completely analogous to the method for real quadratic number fields described in [1].

Next, we try to factor  $\mathfrak{B}$  over the factor basis  $F_C$ . Suppose this factorization can be completed successfully, i.e.

$$(12) \quad \mathfrak{B} = \prod_{i=1}^{k_C} \mathfrak{p}_i^{z_i},$$

where the exponent vector  $\underline{z} = (z_1, \dots, z_{k_C})$  has rational integer entries. Then

$$(13) \quad \mathfrak{A}(\mathfrak{B})^{-1} = \alpha\mathcal{O} = \prod_{i=1}^{k_C} \mathfrak{p}_i^{e_i - z_i},$$

which means that the vector  $(e_1 - z_1, \dots, e_{k_C} - z_{k_C}, \deg(\alpha))$  belongs to  $\Gamma_C$ . By our remarks in Section 1.2, the factorization of  $\mathfrak{B}$  can be done in  $O(k_C \deg(D)^3 \log q)$  operations in  $\mathbb{F}_q$ . For further reference, we denote the whole procedure of this subsection as the procedure RELATION.

**2.4. Computing class number and regulator.** Suppose that we know a generating system  $\underline{b}_1, \dots, \underline{b}_N$  for  $\Gamma_C$ , and the matrix  $B_C$  given in (7). We can compute the Hermite normal form of  $B_C$  and its determinant. Thus, we will obtain  $h'R$ .

Next we consider the matrix  $B'_C$  whose columns are the vectors  $\underline{b}'_1, \dots, \underline{b}'_N$  consisting of the first  $k_C$  entries of the vectors  $\underline{b}_1, \dots, \underline{b}_N$ . Its entries are rational integers whose binary length is polynomially bounded in  $\log |D|$ . As in [18], we can compute both the Hermite and the Smith normal form of  $B'_C$ . The Smith normal form will yield the ideal class number  $h'$  and the structure of the ideal class group. Finally, the regulator  $R$  can be computed by  $R := h'R/h'$ .

**2.5. Computing the discrete logarithm.** We “compute” a generating system for  $\Gamma_C$  by generating “sufficiently many” random vectors in  $\Gamma_C$ . In Section 4, we estimate the number of random vectors we have to find such that these vectors are a generating system for  $\Gamma_C$  with high probability. Until now, we have not mentioned how to verify that the produced vectors really generate the lattice  $\Gamma_C$ . In fact, if we

only want to find the degree of an arbitrary generator of a principal ideal (and this is what is needed to attack the system in [21]) such a verification is not necessary.

But if we want to compute the regulator  $R$  or discrete logarithms as defined in [21] (i.e. the degree of a generator modulo  $R$ ), then we must be sure that the generated lattice indeed is  $\Gamma_C$ .

Again we use a method analogous to Abel’s algorithm for real quadratic number fields. Using standard results on zeta functions for function fields, we can approximate the value of  $h'R$  by a number  $\Theta$  satisfying  $h'R \leq \Theta \leq 2h'R$ . The approximation  $\Theta$  can be derived by techniques similar to those used in [28] and can be found in [27, Theorem 6.2.1]. Suppose that, using the methods of Section 2.4, we have computed values  $\tilde{h}$  and  $\tilde{R}$  assumed to be ideal class number and regulator. We have found a generating system of the whole lattice, if and only if  $\tilde{h}\tilde{R} \leq \Theta$ , and we know that  $h' = \tilde{h}$  and  $R = \tilde{R}$ . In this way, we can always find the correct value for  $h'$ ,  $R$  and the discrete logarithm.

### 3. EXPLICIT BOUNDS FOR A GENERATING SYSTEM

**3.1.  $\zeta$ - and  $L$ -functions.** Let  $K/k$  be an algebraic congruence function field over the finite field  $k = \mathbb{F}_q$  of odd characteristic. Let  $\mathfrak{P}$  be a prime divisor of  $K$  of degree  $f_{\mathfrak{P}}$  and residue class field  $k_{\mathfrak{P}}$ . Then, the *absolute norm* of  $\mathfrak{P}$  is defined to be the integer  $N(\mathfrak{P}) = q^{f_{\mathfrak{P}}}$ . Similarly, the *absolute norm* of a divisor  $\mathfrak{A}$  of degree  $f_{\mathfrak{A}}$  is defined as  $N(\mathfrak{A}) = q^{f_{\mathfrak{A}}}$ . Let  $E$  be the principal class. According to [7, p. 62], a *character*  $\chi$  of finite order on the divisor class group  $\mathcal{C}$  is a homomorphism of  $\mathcal{C}$  into the multiplicative group  $\mathbb{C}^*$  of non-zero complex numbers such that there exists an integer  $N$  with  $\chi^N(\mathfrak{c}) = 1$  for all  $\mathfrak{c} \in \mathcal{C}$ . This character induces a character on  $\mathcal{D}$  by composing with the natural homomorphism,  $\mathcal{D} \rightarrow \mathcal{C}$ ,  $\mathfrak{A} \mapsto \mathfrak{A}E$ . Again, we denote this character by  $\chi$ . The *L-function*  $L(s, \chi, K)$  associated to a character  $\chi$  (of finite order) on  $K/k$  is then defined as

$$(14) \quad L(s, \chi, K) = \sum_{\mathfrak{A}} \frac{\chi(\mathfrak{A})}{N(\mathfrak{A})^s} \quad (\Re(s) > 1),$$

where the summation is over all integral divisors  $\mathfrak{A}$  of  $K$ . As usual, we set  $u := q^{-s}$ . We also have the Euler product for  $L(s, \chi, K)$ ,

$$(15) \quad L(s, \chi, K) = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{\chi(\mathfrak{P})}{N(\mathfrak{P})^s}} = \prod_{\mathfrak{P}} \frac{1}{1 - \chi(\mathfrak{P})u^{f_{\mathfrak{P}}}},$$

where the product is over all prime divisors of  $K$ . For  $\chi = 1$ , we obtain the  $\zeta$ -function of  $K$ , namely

$$(16) \quad \zeta(s, K) = \sum_{\mathfrak{A}} \frac{1}{N(\mathfrak{A})^s} = \prod_{\mathfrak{P}} \frac{1}{1 - \frac{1}{N(\mathfrak{P})^s}} = \prod_{\mathfrak{P}} \frac{1}{1 - u^{f_{\mathfrak{P}}}}.$$

To compute explicit bounds, we need further representations of the  $L$ -function and the  $\zeta$ -function by series and products. We denote by  $g$  the genus of  $K$ . It is well-known (see for example [9], [12] or [29]) that

$$(17) \quad \zeta(s, K) = Z(u, K) = \frac{\prod_{i=1}^{2g} (1 - \omega_i u)}{(1 - u)(1 - qu)},$$

where  $\omega_i = q^{\rho_i}$  ( $i = 1, 2, \dots, 2g$ ) and  $\rho_1, \dots, \rho_{2g}$  are zeros of  $\zeta(s, K)$ . Then,  $1/\omega_i$  ( $i = 1, 2, \dots, 2g$ ) are zeros of  $Z(u, K)$ . Because of the truth of the Riemann Hypothesis (see [31]) in  $K$ , we have  $|\omega_i| = q^{\frac{1}{2}}$  ( $i = 1, 2, \dots, 2g$ ). Note that the  $\zeta$ -function is periodic with period  $2\pi i/\log q$  and analytic in the whole plane with the exception of simple poles at  $s = 0, 1 + l \cdot 2\pi i/\log q$  ( $l \in \mathbf{Z}$ ). From now on, we assume that  $\chi$  is not trivial when restricted to  $\mathcal{D}_0$ . By results in [7, p. 66], we know that if  $k$  is a field with  $q$  elements, then  $L(s, \chi, K)$  is a polynomial in  $u = q^{-s}$  of degree  $2g - 2$ , and

$$(18) \quad L(s, \chi, K) = Z(u, \chi, K) = \prod_{i=1}^{2g-2} (1 - \omega_i(\chi) u),$$

where  $1/\omega_i(\chi)$  ( $i = 1, 2, \dots, 2g - 2$ ) are the zeros of  $Z(u, \chi, K)$ . Let  $\omega_i(\chi) = q^{\rho_i(\chi)}$  ( $i = 1, 2, \dots, 2g - 2$ ). Then  $\rho_1(\chi), \dots, \rho_{2g-2}(\chi)$  are the zeros of  $L(s, \chi, K)$ . As a consequence of the Riemann Hypothesis (see for example [13, p. 155-156], or [30, p. 260], and [7, p. 148-149]), we have  $|\omega_i(\chi)| = q^{\frac{1}{2}}$  ( $i = 1, 2, \dots, 2g - 2$ ).

**3.2. Explicit bounds.** In this subsection we develop explicit bounds for the degree of the least prime divisor with  $\chi(\mathfrak{P}) \neq 1$  in algebraic congruence function fields. If one proceeds in the same way as Bach [3] did in the case of algebraic number fields, one obtains the same bound as in Corollary 1 (see [27]); however, since  $L$ -functions of function fields are essentially polynomials, the result can be derived more easily than in the traditional context.

**Theorem 2.** *Let  $\chi$  be a character (of finite order) which is not trivial when restricted to  $\mathcal{D}_0$ . If  $\chi(\mathfrak{P}) = 1$  for all prime divisors  $\mathfrak{P}$  of  $K$  of degree  $f_{\mathfrak{P}} \leq d$ , where  $d \in \mathbb{N}$ , then we have*

$$d < \frac{2 \log(4g - 2)}{\log q},$$

where  $g$  denotes the genus of  $K$ .

*Proof.* If all prime divisors  $\mathfrak{P}$  of  $K$  of degree  $f_{\mathfrak{P}} \leq d$  have the property that  $\chi(\mathfrak{P}) = 1$ , then the first few Euler factors of  $Z(u, \chi, K)$  are equal to the corresponding Euler factors of  $Z(u, K)$ . In other words,

$$Z(u, K) = \prod_{f_{\mathfrak{P}} \leq d} \frac{1}{1 - u^{f_{\mathfrak{P}}}} \prod_{f_{\mathfrak{P}} > d} \frac{1}{1 - u^{f_{\mathfrak{P}}}} = \frac{\prod_{i=1}^{2g} (1 - \omega_i u)}{(1 - u)(1 - qu)},$$

by (16) and (17), and

$$\begin{aligned} \prod_{i=1}^{2g-2} (1 - \omega_i(\chi) u) &= Z(u, \chi, K) = \prod_{f_{\mathfrak{P}} \leq d} \frac{1}{1 - u^{f_{\mathfrak{P}}}} \prod_{f_{\mathfrak{P}} > d} \frac{1}{1 - \chi(\mathfrak{P}) u^{f_{\mathfrak{P}}}} \\ &= \frac{\prod_{i=1}^{2g} (1 - \omega_i u)}{(1 - u)(1 - qu)} \prod_{f_{\mathfrak{P}} > d} \frac{1 - u^{f_{\mathfrak{P}}}}{1 - \chi(\mathfrak{P}) u^{f_{\mathfrak{P}}}}, \end{aligned}$$

by (15) and (18). If we take logarithmic derivatives, we obtain

$$(19) \quad \sum_{\nu=0}^{\infty} \sum_{i=1}^{2g-2} \omega_i(\chi)^{\nu+1} u^\nu = \sum_{\nu=0}^{\infty} \sum_{i=1}^{2g} \omega_i^{\nu+1} u^\nu - \sum_{\nu=0}^{\infty} u^\nu - \sum_{\nu=0}^{\infty} q^{\nu+1} u^\nu + P(u^d),$$

where

$$P(u^d) = \sum_{f_{\mathfrak{P}} > d} \sum_{\nu=1}^{\infty} f_{\mathfrak{P}} u^{\nu f_{\mathfrak{P}}-1} (\chi(\mathfrak{P})^\nu - 1)$$

is a series in  $u$  with terms of degree at least  $d$ . Equating coefficients at  $u^{d-1}$ , we find that

$$\sum_{i=1}^{2g-2} \omega_i(\chi)^d = \sum_{i=1}^{2g} \omega_i^d - 1 - q^d,$$

so that, by the Riemann Hypothesis,

$$q^d + 1 \leq (2g + (2g - 2)) q^{\frac{d}{2}},$$

and hence

$$q^{\frac{d}{2}} \leq 2g - 1 + \sqrt{4g^2 - 4g} < (4g - 2).$$

□

**Corollary 1.** *Let  $\chi$  be a character (of finite order) which is not trivial when restricted to  $\mathcal{D}_0$ . If we define*

$$d := \left\lceil \frac{2 \log(4g - 2)}{\log q} \right\rceil,$$

*there must exist a prime divisor  $\mathfrak{P}$  of degree  $f_{\mathfrak{P}} \leq d$  such that  $\chi(\mathfrak{P}) \neq 1$ .*

Notice that  $d$  is at least 1. This corollary is an analogue of the results for algebraic number fields in [3].

**3.3. Real quadratic congruence function fields.** Now let  $K/k$  be a real quadratic congruence function field. The decomposition of the infinite place  $\mathfrak{P}_\infty$  of  $k(x)$  is  $\mathfrak{P}_\infty = \mathfrak{P}_1 \cdot \mathfrak{P}_2$ , where  $\mathfrak{P}_1$  and  $\mathfrak{P}_2$  are two different infinite places of  $K/k$ . It follows that

$$\mathcal{U} = \langle \mathfrak{P}_1, \mathfrak{P}_2 \rangle,$$

and that

$$\mathcal{U}_0 = \langle \mathfrak{P}_1 \cdot \mathfrak{P}_2^{-1} \rangle.$$

From [32, p. 263], we have that  $f_{\mathfrak{P}_1} = f_{\mathfrak{P}_2} = 1$ , and that

$$\mathcal{D} = \mathcal{D}_0 \mathcal{U},$$

and

$$h = R h'.$$

We deduce from (1) and (2) that

$$\mathcal{I} \cong \mathcal{D}_0 \mathcal{U} / \mathcal{U},$$

and

$$\text{Cl} \cong \mathcal{D}_0 \mathcal{U} / \mathcal{P} \mathcal{U}.$$

As in Section 3.1, any character  $\chi$  (of finite order) defined on the ideal class group  $\text{Cl}$  induces a character on  $\mathcal{I}$ . A character that takes only the value 1 is called the *trivial character*. We also denote it by 1. From the above, we see that any non-trivial character  $\chi$  on  $\mathcal{I}$  can be induced by a character defined on  $\mathcal{D}$  that is not trivial when restricted to  $\mathcal{D}_0$ . Also, we know that  $f_{\mathfrak{p}_1} = f_{\mathfrak{p}_2} = 1$ . Thus, we immediately derive from Corollary 1 the result for prime ideals.

**Theorem 3.** *Let  $\chi$  be any non-trivial character (of finite order) defined on  $\text{Cl}$ . If we set*

$$d := \left\lceil \frac{2 \log(2 \deg(D) - 6)}{\log q} \right\rceil,$$

*then there must exist a prime ideal  $\mathfrak{p}$  of  $K$  with absolute norm  $|N(\mathfrak{p})| \leq q^d$  such that  $\chi(\mathfrak{p}) \neq 1$ .*

Here, we use the fact that  $g = \deg(D)/2 - 1$ . We notice that  $d$  is at least 1, and that  $q^d$  is almost equal to  $(2 \deg(D) - 5)^2$ .

As in the case of a quadratic number field (see [23, p. 266]), we use the argument that we can produce a generating system for the ideal class group by using only the prime ideals with norm less than  $q^d$ , where  $d$  is given as in Theorem 3. We derive from character theory (see, for instance, [11, p. 68]) the following theorem.

**Theorem 4.** *The ideal class group  $\text{Cl}$  of a real quadratic congruence function field can be generated by all prime ideals  $\mathfrak{p}$  with absolute norm  $|N(\mathfrak{p})| \leq q^d$ , where*

$$d := \left\lceil \frac{2 \log(2 \deg(D) - 6)}{\log q} \right\rceil,$$

*i.e.*

$$\text{Cl} = \langle \{ [\mathfrak{p}] : \mathfrak{p} \text{ a prime ideal and } |N(\mathfrak{p})| \leq q^d \} \rangle.$$

#### 4. PRODUCING A GENERATING SYSTEM

In this section, we estimate how many vectors in  $\Gamma_C$  we must generate in order to obtain (with high probability) a generating system for  $\Gamma_C$ . Suppose that the algorithm RELATION of Section 2.3 chooses the vector  $\underline{e} = (e_1, \dots, e_{k_C}) \in \{0, \dots, |D|\}^{k_C}$  and  $y \in \{0, \dots, |D|\}$  and outputs a vector  $(v_1, \dots, v_{k_C}, v_{k_C+1})$ . From Lemma 2 it follows that the exponents  $z_i$  ( $1 \leq i \leq k_C$ ) in (12) satisfy  $|z_i| \leq \deg(D)/2$ . Thus, we have  $-\deg(D)/2 \leq e_i - z_i = v_i \leq |D| + \deg(D)/2$ . Analogously, we have by (4) that  $-\deg(D)/2 \leq e_{k_C+1} - z_{k_C+1} = v_{k_C+1} \leq |D| + \deg(D)/2$ . Therefore, any vector which is computed by RELATION belongs to the set

$$(20) \quad \begin{aligned} \mathcal{W}^+ &= \{-\deg(D)/2, \dots, |D| + \deg(D)/2\}^{k_C} \\ &\quad \times \{-\deg(D)/2, \dots, |D| + \deg(D)/2\}. \end{aligned}$$

On the other hand, we see that all vectors  $(v_1, \dots, v_{k_C}, v_{k_C+1})$  that can be produced by RELATION only from vectors  $(\underline{e}, y) \in \{0, \dots, |D|\}^{k_C} \times \{0, \dots, |D|\}$  must belong to

$$(21) \quad \mathcal{W}^- = \{0, \dots, |D| - \deg(D)/2\}^{k_C} \times \{0, \dots, |D| - \deg(D)/2\}.$$

Finally, we let  $N_{red}(C)$  be the number of reduced ideals of  $\mathcal{O}$  that can be factored over  $F_C$ .

**Proposition 1.** *Let  $N_{\underline{v}}$  be the number of pairs*

$$(\underline{e}, y) \in \{0, \dots, |D|\}^{k_C} \times \{0, \dots, |D|\}$$

*which as choice in RELATION can yield the vector  $\underline{v} = (v_1, \dots, v_{k_C}, v_{k_C+1}) \in \mathcal{W}^-$ . Then  $N_{red} \leq N_{\underline{v}}$ .*

*Proof.* Let  $(v_1, \dots, v_{k_C}, v_{k_C+1}) \in \mathcal{W}^-$ . Let

$$\mathcal{Z} := \{\mathfrak{B} \mid \mathfrak{B} \text{ a reduced ideal of } \mathcal{O} \text{ that can be factored over } F_C\} \quad .$$

Then for each  $\underline{z}$  with  $\prod_{i=1}^{k_C} \mathfrak{p}_i^{z_i} \in \mathcal{Z}$  there exists  $\underline{e} \in \{0, \dots, |D|\}^{k_C}$  such that

$$\prod_{i=1}^{k_C} \mathfrak{p}_i^{v_i} = \prod_{i=1}^{k_C} \mathfrak{p}_i^{e_i - z_i} \quad .$$

This implies the assertion. □

Suppose we have found the vectors  $\underline{v}_1, \dots, \underline{v}_j$ . (If  $j = 0$ , we have not yet found anything.) Let  $\Gamma_j \subseteq \Gamma_C$  be the sublattice generated by those vectors and let  $d_j$  be its dimension. If  $d_j = k_C + 1$ , let  $I_j = [\Gamma_C : \Gamma_j]$ . We will estimate the probability  $p_{j+1}$  for the procedure RELATION to yield a vector  $\underline{v}_{j+1} \in \Gamma_C - \Gamma_j$ .

Let  $N_1 = \#\Gamma_j \cap \mathcal{W}^+$ ,  $N_2 = \#\Gamma_C \cap \mathcal{W}^-$ . Then by Proposition 1 we have

$$(22) \quad p_{j+1} \geq \frac{N_{red}(C)}{(|D| + 1)^{k_C+1}} (N_2 - N_1) \quad .$$

To find a lower bound for that probability, we compute an upper bound for  $N_1$  and a lower bound for  $N_2$ .

**Lemma 3.** (i) *If  $d_j = k_C + 1$ , then we have*

$$N_1 \leq \frac{1}{h'R I_j} \left( |D| + \deg(D) + 2I_j (\deg(D) - 1)^2 (\sqrt{q})^{\deg(D)-2} \right)^{k_C+1} .$$

(ii) *If  $d_j < k_C + 1$  and  $\Gamma'$  is a  $(k_C + 1)$ -dimensional sublattice of  $\Gamma_C$  with  $\Gamma_j \subseteq \Gamma'$ , then we have*

$$N_1 \leq \frac{1}{h'R [\Gamma_C : \Gamma'] } \left( |D| + \deg(D) + 2[\Gamma_C : \Gamma'] (\deg(D) - 1)^2 (\sqrt{q})^{\deg(D)-2} \right)^{k_C+1} .$$

*Proof.* (i) We have  $\det(\Gamma_j) = I_j \det(\Gamma_C)$ , which by Theorem 1 implies  $\det(\Gamma_j) = I_j h'R$ . As in [2, p. 236, (9)], we can bound  $h'R$  by

$$h'R \leq 2 (\deg(D) - 1)^2 (\sqrt{q})^{\deg(D)-2} .$$

Hence, there is a basis of  $\Gamma_j$  that is contained in

$$\{0, \dots, 2I_j (\deg(D) - 1)^2 (\sqrt{q})^{\deg(D)-2}\}^{k_C+1} .$$

Let  $\mathcal{F}_j$  be the fundamental parallelepiped of that basis. Then for every  $\underline{v} \in \Gamma_j \cup \mathcal{W}^+$  the translated set  $\underline{v} + \mathcal{F}_j$  belongs to

$$\{-\deg(D)/2, \dots, |D| + \deg(D)/2 + 2I_j (\deg(D) - 1)^2 (\sqrt{q} + 1)^{\deg(D)-2}\}^{k_C+1} .$$

It follows that

$$\begin{aligned} N_1 &= \#\Gamma_j \cap \mathcal{W}^+ \\ &\leq \frac{1}{\det(\Gamma_j)} \left( |D| + \deg(D) + 2I_j (\deg(D) - 1)^2 (\sqrt{q})^{\deg(D)-2} \right)^{k_C+1} \\ &= \frac{1}{I_j h'R} \left( |D| + \deg(D) + 2I_j (\deg(D) - 1)^2 (\sqrt{q})^{\deg(D)-2} \right)^{k_C+1}. \end{aligned}$$

(ii) Since  $\#\Gamma_j \leq \mathcal{W}^+ \subseteq \#\Gamma' \cap \mathcal{W}^+$ , this is an immediate consequence of (i).  $\square$

Analogously, we obtain

**Lemma 4.** *We have*

$$N_2 \geq \frac{1}{h'R} \left( |D| - \deg(D) - 2(\deg(D) - 1)^2 (\sqrt{q})^{\deg(D)-2} \right)^{k_C+1}.$$

Finally, from (22), Lemma 3 and Lemma 4, we obtain

**Corollary 2.**

$$p_{j+1} \geq \frac{N_{red}(C)}{h'R} (1 - o(1)).$$

## 5. THE EXPECTED RUNNING TIME OF THE ALGORITHM

In this section, we use the results of the previous two sections to derive the expected running time of the algorithm described in this paper.

First of all, we compute the factor basis  $F_C$ . The factor basis  $F_C$  is the set of prime ideals whose norm is bound by  $q^C$  for some constant  $C$  (see Section 2.2). Using the estimates in [16, p. 59] or [27, Lemma 6.2.3], we see that the size of the factor basis is bounded by  $k_C = 4Cq^C$ . It can be computed in  $O(Cq^C \deg(D)^3 \log q)$  operations in  $\mathbb{F}_q$ .

Let us now estimate the expected time until we have found a generating system for the lattice  $\Gamma_C$ . We define for  $\rho \in \mathbb{R}_{>0}$

$$L[\rho] = \exp \left( \sqrt{\log |D| \log \log |D|} \right)^{\rho+o(1)},$$

where the notation  $o(1)$  represents a function of  $|D|$  which tends to 0 as  $|D|$  tends to infinity.

According to Theorem 4, it is sufficient to choose  $C \geq \lceil 2 \log(2 \deg(D) - 5) / \log q \rceil$  for  $F_C$ , which implies that the minimal size of the factor basis is  $O(\deg(D)^2)$ . This is polynomial in the input length  $|D|$ . Note that  $C$  is at least 1. To get a better probability of success in the algorithm RELATION, we extend the factor basis to subexponential size, i.e. we choose

$$C = \log_q(L[\rho]),$$

where  $\rho$  is some positive constant. Thus,  $L[\rho] = q^C$ . Since  $C \geq 1$ , it follows in particular that  $q$  must be subexponential in the input length, and we obtain the following condition:

$$L[\rho] = q^{(\rho+o(1)) \frac{\sqrt{\deg(D)}}{\sqrt{\log q}}} \sqrt{\log \log |D|} = q.$$

In order to assure this condition, we assume from now on that  $\deg(D) > \log q$ .

In Section 4, we examined the probability of finding a relation. In order to determine the expected running time of our algorithm, we have to find a lower

bound for  $N_{red}(C)$  in Corollary 2. In this context, we immediately derive from [17, Theorem 2.1] (see also [25]) the following fact.

**Theorem 5.** For  $\lceil 2 \log(2 \deg(D) - 5) / \log q \rceil \leq C \leq q^{\deg(D)/2}$  we have

$$N_{red}(C) \geq q^{\frac{1}{2} \deg(D) - 1} L \left[ -\frac{1}{4\rho} \right].$$

Using this theorem, we obtain

**Corollary 3.** If  $\Gamma_j \neq \Gamma_C$ , then for  $\lceil 2 \log(2 \deg(D) - 5) / \log q \rceil \leq C \leq q^{\deg(D)/2}$  we have

$$p_{j+1} \geq L \left[ -\frac{1}{4\rho} \right].$$

*Proof.* We have  $h'R \leq (\deg(D) - 1)^2 (\sqrt{q})^{\deg(D) - 2}$ . From Corollary 2 and Theorem 5, we obtain  $p_{j+1} \geq L \left[ -\frac{1}{4\rho} \right]$ .  $\square$

Finally, the next theorem determines the expected running time for computing a generating system for the relation lattice  $\Gamma_C$ .

**Theorem 6.** Assume that  $\deg(D) > \log q$ . A generating system for  $\Gamma_C$  consisting of  $L[\rho]$  elements can be computed in expected running time  $L[2\rho + \frac{1}{4\rho}]$ .

*Proof.* We recall that  $C = \log_q(L[\rho])$ . Then  $C \geq \lceil 2 \log(2 \deg(D) - 5) / \log q \rceil$ , and therefore the conditions of Theorem 4 are satisfied. We also have  $k_C = L[\rho]$ . By Corollary 3, we have  $p_{j+1} \geq L \left[ -\frac{1}{4\rho} \right]$ . The expected number of applications of the procedure RELATION before a sublattice  $\Gamma_0$  of  $\Gamma_C$  of finite index is found is  $L[\rho + \frac{1}{4\rho}]$ . Now, we have to estimate the index  $[\Gamma_C : \Gamma_0] = \det(\Gamma_{k_C+1}) \det(\Gamma_C)$ . Obviously,  $\det(\Gamma_C) = h'R \geq 1$ . To bound  $\det(\Gamma_{k_C+1})$  we use Hadamard's inequality. By (20), we obtain  $\det(\Gamma_0) \leq (|D| + \deg(D))^{k_C+1} = \exp(L[\rho])$ . Hence the expected number of applications of RELATION before a generating system of  $\Gamma_C$  is found is again  $L \left[ \rho + \frac{1}{4\rho} \right]$ . Each application of RELATION requires  $L[\rho]$  operations in  $\mathbb{F}_q$ , and this completes the proof.  $\square$

By standard techniques in probability theory (see for example [14]), we obtain

**Corollary 4.** If the number of applications of RELATION exceeds  $4L[\rho + \frac{1}{4\rho}]$ , then the probability that the produced vectors generate  $\Gamma_C$  is at least  $1/2$ .

If we know a generating system for  $\Gamma_C$ , we have the matrices  $B_C$  and  $B'_C$  as in (7). As described in Section 2.4, we compute the Hermite normal forms and the determinants of  $B_C$  and  $B'_C$ . In addition, we compute the Smith normal form of  $B'_C$ . The computation of the Hermite normal form, the Smith normal form, and the determinant, respectively, can be done in  $L[5\rho]$ ,  $L[3\rho]$ ,  $L[3\rho]$  (see [6], [8], [18]). For computing the degree of a generator of an ideal  $\mathfrak{A}$ , we considered two situations in Section 2.3: if  $\mathfrak{A}$  splits over  $F_C$ , we need time  $L[4\rho]$  for computing the degree of a generator. If the ideal  $\mathfrak{A}$  should not split over the factor basis  $F_C$ , we construct another ideal  $\mathfrak{B}$ . This is done as follows: we choose at random a vector  $\underline{e} \in \{0, \dots, |D|\}^{k_C}$  and  $y \in \{0, \dots, |D|\}$  and compute a reduced ideal  $\mathfrak{C}$  closest to  $y$  and  $\alpha \in K$  such that

$$\mathfrak{C} = \alpha \mathfrak{A} \prod_{i=1}^{k_C} \mathfrak{p}_i^{e_i}.$$

We repeat this step until we can factor  $\mathfrak{C}$  over  $F_C$ , but at most  $L[\rho]$  times. By the same arguments as above, we obtain that the probability that we can factor one of the ideals  $\mathfrak{C}$  over  $F_C$  is at least  $1/2$ . The expected number of operations in  $\mathbb{F}_q$  performed by the algorithm is therefore  $L[2\rho + \frac{1}{4\rho}]$ .

If  $\mathfrak{C}$  can be factored, i.e.  $\mathfrak{C} = \prod_{i=1}^{k_C} \mathfrak{p}_i^{z_i}$  then we have

$$\mathfrak{B} = \prod_{i=1}^{k_C} \mathfrak{p}_i^{z_i - e_i} = \alpha \mathfrak{A}.$$

Finally, we have to solve (9) and to compute (10). By the techniques described in [19], this can be done in  $L[4\rho]$  operations in  $\mathbb{F}_q$ .

We can now discuss the optimal choice for  $\rho$ . Since the computation of the generating system requires  $L[2\rho + \frac{1}{4\rho}]$  operations, optimizing  $\rho$  means solving the equation

$$2\rho + \frac{1}{4\rho} = 5\rho.$$

One solution of this equation is  $\rho = \frac{5}{2\sqrt{3}}$  which means that the expected running time of the whole procedure is  $L[1.44]$ . Therefore we obtain the following main result of this paper:

**Theorem 7.** *Let  $K = \mathbb{F}_q(x)(\sqrt{D})$  be a real quadratic congruence function field with  $\deg(D) > \log q$ . Then we can find the degree of a generator of an arbitrary principal ideal in the ring of integers  $\mathcal{O}$  of  $K$  in expected running time  $L[1.44]$  with probability at least  $1/2$ .*

By iterating our algorithm  $l$ -times ( $l \in \mathbb{Z}_{>0}$ ), we can increase the probability up to  $1 - 2^{-l}$ . As described in Section 2.5, we can solve the discrete logarithm problem in real quadratic congruence function fields of large genus with the same algorithm and an additional approximation  $\Theta$  of  $h'R$ . This approximation is described in detail in [28] and [27]. It can be done in polynomial time  $O(\deg(D)^2)$ . Note that, if  $q \geq (2/(2^{1/2g} - 1) + 1)^2$ , then it is sufficient to use  $\Theta := 2(\sqrt{q} - 1)^{2g}$ . Thus we obtain

**Theorem 8.** *The discrete logarithm problem for real quadratic congruence function fields  $\mathbb{F}_q(x)(\sqrt{D})$ , where  $\deg(D) > \log q$ , can be solved in expected running time  $L[1.44]$ . The structure of the ideal class group, the ideal class number, and the regulator can be computed in the same expected running time.*

#### ACKNOWLEDGMENTS

We would like to thank Hugh Williams, who strongly supported us during this work. Part of this work was done when the second author visited Hugh Williams at the University of Winnipeg. Hendrik W. Lenstra, Jr. gave us helpful comments on the proof of some of the theorems in this paper. Last but not least, we would like to thank an anonymous referee for suggesting a different proof of Theorem 2 which considerably shortened the paper.

#### REFERENCES

- [1] C.S. ABEL, *Ein Algorithmus zur Berechnung der Klassenzahl und des Regulators reell-quadratischer Ordnungen*, PhD Thesis, Universität des Saarlandes, Saarbrücken, (1994).

- [2] E. ARTIN, Quadratische Körper im Gebiete der höheren Kongruenzen I, II, *Math. Zeitschr.* **19** (1924), 153-206.
- [3] E. BACH, Explicit Bounds for Primality Testing and Related Problems, *Math. Comp.*, Vol **55**, Number 191 (1990), 355-380. MR **91m**:11096
- [4] J. BUCHMANN, A subexponential algorithm for the determination of class groups and regulators of algebraic number fields, *Séminaire de théorie des nombres, Paris (1988-1989)* 28-41. MR **92g**:11125
- [5] J. BUCHMANN, C. THIEL & H.C. WILLIAMS, Short representation of quadratic integers, *Computational Algebra and Number Theory (Sydney, 1992)*, *Math. Appl.*, vol. 325, Reidel, Dordrecht, 1995, pp. 159-185. MR **96c**:11144
- [6] H. COHEN, A course in computational algebraic number theory, *Springer Verlag* (1993). MR **94i**:11105
- [7] M. DEURING, Lectures on the Theory of Algebraic Functions of One Variable, *Lect. Notes in Math.* **314**, Berlin (1973). MR **49**:8970
- [8] P. D. DOMICH & R. KANNAN & L. E. TROTTER JR., Hermite normal form computation using modular determinant arithmetic, *Math. of Operations Research* **12**, No. 1, February (1987), 50-59. MR **88e**:65047
- [9] M. EICHLER, Introduction to the Theory of Algebraic Numbers and Functions, *Academic Press, New York* (1966). MR **35**:160
- [10] D. GORDON, Discrete Logarithms in  $GF(p)$  using the Number Field Sieve, *SIAM J. Discrete Math.* **6** (1993), 124-138. MR **94d**:11104
- [11] H. HASSE, Number Theory, *Springer, New York*, 1980. MR **84c**:12001
- [12] H. HASSE, Über die Kongruenzzetafunktionen, *Sitzungsb. d. Preuß. Akad. d. Wiss.* **H17**, (1934), 250-263.
- [13] H. HASSE & H. DAVENPORT, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, *Journal f. d. reine u. angew. Math.*, **172** (1934), 151-182.
- [14] F. HEIGL & J. FEUERPFEL, Stochastik, *BSV* (1974).
- [15] A.E. INGHAM, The Distribution of Prime Numbers, *Cambridge Univ. Press, Cambridge*, (1932).
- [16] R. LOVORN [RENEE LOVORN BENDER], *Rigorous, Subexponential Algorithms for Discrete Logarithms Over Finite Fields*, PhD Thesis, University of Georgia (1992).
- [17] R. LOVORN [RENEE LOVORN BENDER] & C. POMERANCE, *Rigorous discrete logarithm computations in finite fields via smooth polynomials*, *Computational Perspectives on Number Theory (Chicago, 1995)* *AMS/IP Stud. Adv. Math.*, vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 221-232. CMP 98:05
- [18] K.S. McCURLEY, Cryptographic key distribution and computation in class groups, *Proceedings of NATO ASI Number Theory and Applications*, *Kluwer Academic Publishers* (1989), 459-479. MR **92e**:11149
- [19] A. MÜLLER, *Lineare Algebra über  $\mathbf{Z}$* , Diploma Thesis, Universität des Saarlandes, Saarbrücken, (1994).
- [20] H. REICHARDT, Der Primdivisorsatz für algebraische Funktionenkörper über einem endlichen Konstantenkörper, *Mathematische Zeitschrift* **40** (1936), 713-719.
- [21] R. SCHEIDLER, A. STEIN & H.C. WILLIAMS, Key-exchange in real quadratic congruence function fields, *Designs, Codes and Cryptography*, Vol. **7**, Number 1/2 (1996), 153-174. MR **97d**:94009
- [22] F.K. SCHMIDT, Analytische Zahlentheorie in Körpern der Charakteristik  $p$ , *Mathematische Zeitschrift* **33** (1931), 1-32.
- [23] R.J. SCHOOF, Quadratic fields and factorization, *Computational Methods in Number Theory (H.W. Lenstra and R. Tijdeman, eds.)*, *Math. Centrum Tracts* **155**, Part II, Amsterdam (1983), 235-286. MR **85g**:11118
- [24] D. SHANKS, The infrastructure of a real quadratic field and its applications, *Proc. 1972 Number Theory Conference, Boulder, (1972)*, 217-224. MR **52**:10672
- [25] K. SOUNDARARAJAN, *Smooth Polynomials: Analogies and Asymptotics*, To appear in *J. London Math. Society*.
- [26] A. STEIN, *Baby Step-Giant Step-Verfahren in reell-quadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2*, Diploma Thesis, Universität des Saarlandes, Saarbrücken, (1992).

- [27] A. STEIN, *Algorithmen in reell-quadratischen Kongruenzfunktionenkörpern*, PhD Thesis, Universität des Saarlandes, Saarbrücken, (1996).
- [28] A. STEIN & H.C. WILLIAMS, *Some Methods for Evaluating the Regulator of a Real Quadratic Function Field*, to appear in Experimental Mathematics.
- [29] H. STICHTENOTH, *Algebraic Function Fields and Codes*, Springer Verlag, Berlin (1993). MR **94k**:14016
- [30] A. WEIL, *Basic Number Theory, Third Edition*, Springer Verlag (1974). MR **55**:302
- [31] A. WEIL, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris, (1948). MR **10**:262c
- [32] B. WEIS & H.G. ZIMMER, *Artins Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen*, Mitt. Math. Ges. Hamburg, Sond. , **XII**, 2, (1991), 261–282. MR **93e**:11141

TECHNISCHE UNIVERSITÄT DARMSTADT, FACHBEREICH INFORMATIK, ALEXANDERSTR. 10, 64283 DARMSTADT, GERMANY

*E-mail address*: `vmueller@cdc.informatik.tu-darmstadt.de`

DEPARTMENT OF COMBINATORICS AND OPTIMIZATION, UNIVERSITY OF WATERLOO, WATERLOO, ONTARIO, CANADA, N2L 3G1

*E-mail address*: `astein@cacr.math.uwaterloo.ca`

GAO, EUCKENSTRASSE 12, 81368 MÜNCHEN, GERMANY