Arithmetic on Superelliptic Curves

S. D. Galbraith[†], S. Paulus[‡], Nigel P. Smart
Extended Enterprise Laboratory
HP Laboratories Bristol
HPL-98-179
October, 1998

superelliptic curves,
jacobians,
cryptography,
discrete logarithm
problem

In this paper we present an efficient, polynomial-time method to perform calculations in the divisor class group of a curve which has a single point on its normalization above infinity. In particular, we provide a unique representation of divisor classes and an algorithm for reducing a divisor on such a curve to its corresponding representative. Such curves include the case of elliptic, odd-degree hyperelliptic and superelliptic curves.

In the case when the curve is defined over a finite field, the divisor class group is a finite group which can be used for implementing discrete logarithm based public key cryptosystems. This paper therefore provides a new class of groups for cryptography.

On the other hand, we present a method to solve the discrete logarithm problem in these groups. This method is sub-exponential when the degree of the defining equation of the curve is large.

[†]Mathematics Department, Royal Holloway University of London, Egham, Surrey, U.K.
[‡]Technische Universitt Darmstadt, Fachbereich 20 - Informatik Alexanderstr, Darmstadt, Germany

ARITHMETIC ON SUPERELLIPTIC CURVES

S.D. GALBRAITH, S. PAULUS AND N.P. SMART

ABSTRACT. In this paper we present an efficient, polynomial-time method to perform calculations in the divisor class group of a curve which has a single point on its normalization above infinity. In particular, we provide a unique representation of divisor classes and an algorithm for reducing a divisor on such a curve to its corresponding representative. Such curves include the case of elliptic, odd-degree hyperelliptic and superelliptic curves.

In the case when the curve is defined over a finite field, the divisor class group is a finite group which can be used for implementing discrete logarithm based public key cryptosystems. This paper therefore provides a new class of groups for cryptography.

On the other hand, we present a method to solve the discrete logarithm problem in these groups. This method is sub-exponential when the degree of the defining equation of the curve is large.

1. INTRODUCTION

The goal of this paper is to describe a practical and efficient method for computing in the Jacobian of a large class of algebraic curves.

This research is primarily motivated by cryptography, as abelian varieties over finite fields can be used for implementing discrete logarithm based cryptosystems. However, the methods are equally applicable to the situation where the curves are defined over characteristic zero fields, and so our methods are also relevant for studying the arithmetic of curves.

We also generalize the subexponential algorithm of Adleman-DeMarrais-Huang [1] (which is based on the function field sieve) for solving discrete logarithms on these curves.

Explicit computation on elliptic curves is easily performed as the group law is given by simple formulae. Jacobians of hyperelliptic curves have also been implemented. The addition rule is given by Cantor's algorithm [6]. The key to Cantor's algorithm is a reduction method which is analogous to reduction of binary quadratic forms.

For computing in Jacobians it is essential to be able to determine if two divisors are equivalent. This is usually done using some form of reduction theory. The main obstacle to computing in more general Jacobians is finding a suitable method of reducing divisors. The approach adopted in this paper is to use lattice reduction techniques to provide a reduction method. This is analogous to the strategy used for computing with ideals in number fields (see Cohen [8] Section 6.5).

1991 *Mathematics Subject Classification.* 14Q05, 14H05, 14H40, 11G20, 11Y16.

Key words and phrases. superelliptic curves, jacobians, cryptography, discrete logarithm problem.

In this paper we are concerned with curves given in the form

$$C : c_n(x)y^n + c_{n-1}(x)y^{n-1} + \cdots + c_1(x)y + c_0(x) \tag{1}$$

where $c_j(x) \in k[x]$ for some field k. The function field of the curve C is $K := k(C)$. We will think of this as being a degree n algebraic extension of the function field $k(x)$ and will sometimes write $K = k(x, y)$ where the algebraic relation $C(x, y) = 0$ is implicit. We will impose the following further conditions on C.

1. C non-singular as an affine curve.
2. $c_n(x) = 1$ (which can always be arranged by a change of variables, though this may render the curve singular).
3. There should be only one point at infinity on the desingularisation of the projective model of the curve. Equivalently, the "infinite" place of $k(x)$ (i.e., the place corresponding to the element x^{-1}) should be totally ramified in $K/k(x)$.
4. The integral closure of $k[x]$ in $k(C) = k(x, y)$ is $k[x, y]$ (where the algebraic relation $C(x, y) = 0$ is implicit).

The most serious of these restrictions is the third. In Section 3 we will give a large class of curves satisfying these four conditions.

We note that there have already been methods proposed to compute in general Jacobians (see for instance Coates [7], Huang-Ieradi [13], Volcheck [23]). These methods, however, are not practical and they require taking extensions of the base field. We observe that the restriction of our method to the hyperelliptic case yields Cantor's algorithm (which in turn, restricted to elliptic curves, gives the usual addition formulae) and so our method is a very natural generalization.

We now summarise the contents of the paper. In Section 2 we list some results about Jacobians and divisor class groups. In Section 3 we describe superelliptic curves. In Sections 4 and 5 we provide some background theory. Section 6 contains the details of the reduction algorithm. The remainder of the paper is concerned with the discrete logarithm problem on Jacobians of curves over finite fields.

2. Divisor Class Groups of Curves

For this section let C be *any* non-singular algebraic curve over *any* field k. A *divisor* of C over k is a formal sum $D = \sum_{\mathfrak{p} \in C(k)} n_\mathfrak{p} \mathfrak{p}$ where $\mathfrak{p}$ runs over all places of the function field $k(C)$ and where $n_\mathfrak{p} \in \mathbb{Z}$. The *degree* of a divisor D is $\sum_\mathfrak{p} n_\mathfrak{p} \deg(\mathfrak{p})$ where $\deg(\mathfrak{p})$ is the degree of the residue field $k(C)_\mathfrak{p}/k$ (equivalently, the degree of the field of definition of the $\bar{k}$-points corresponding to $\mathfrak{p}$). An *effective divisor* is one for which all $n_\mathfrak{p} \geq 0$. We say that $D_1 \geq D_2$ if $D_1 - D_2$ is an effective divisor. Given a function $f \in k(C)$ we can define the *order* of f at a prime divisor $\mathfrak{p}$ in the usual way (using uniformizers at $\mathfrak{p}$). The divisor of a function f is $(f) = \sum_\mathfrak{p} ord_\mathfrak{p}(f)\mathfrak{p}$, which is a divisor of degree zero (and is called a *principal divisor*).

Write $\mathrm{Div}_k^0(C)$ for the set of all divisors of C which are defined over k (which means that they are fixed by the action of $Gal(\bar{k}/k)$) and which have degree zero. Write $Prin_k(C)$ for the set of all divisors of functions $f \in k(C)$. Then $Prin_k(C)$ is a subgroup of $\mathrm{Div}_k^0(C)$ and the *Divisor Class Group* of the curve C is defined to be the quotient

$$\mathrm{Pic}_k^0(C) = \mathrm{Div}_k^0(C)/Prin_k(C). \tag{2}$$

To actually compute in the Divisor Class Group of a general curve we need a suitable representation of divisors. Addition of divisors is trivial, however determining whether two divisors differ by a principal divisor is much more difficult. This difficulty may be solved in the case of hyperelliptic curves by borrowing Gauss' algorithm for reducing quadratic forms. However, the definition of reduced divisor used in the hyperelliptic case does not generalize to give a unique divisor in our more general setting. This paper overcomes the obstacle of unique representation of divisors for a class of curves.

Our task in this section is to show that there does exist a candidate for a unique representation of divisors. For a divisor D let $L(D) = \{f \in k(C) : (f) \geq -D\}$ and $l(D) = dim_k(L(D))$ as usual. We first give the following standard lemma.

Lemma 1. *Let C be a non-singular curve over k of genus g with a given k-point P_∞. Let D be a degree zero divisor in $\mathrm{Div}_k^0(C)$. Then there is an effective divisor E over k of degree g such that D is equivalent to $E - gP_\infty$.*

Proof. By the Riemann-Roch theorem (see, for instance, Fulton [12])

$$l(D + gP_\infty) = l(\kappa - D - gP_\infty) + \deg(D + gP_\infty) + 1 - g \geq 1.$$

This means there is a function $f \in k(C)$ such that $(f) \geq -D - gP_\infty$. Define $E := (f) + D + gP_\infty \geq 0$. Then E is effective and $E - gP_\infty = D + (f)$. □

The problem with the above result is that there may be several different effective divisors E so that $E - gP_\infty$ is equivalent to D. The next result shows that there is a unique choice of E having minimal degree.

Theorem 2. *Let C be a non-singular curve over k of genus g with a given k-point P_∞. Let $D \in \mathrm{Div}_k^0(C)$. Then there is a uniqe effective divisor over k of minimal degree $m \leq g$ such that $E - mP_\infty$ is equivalent to D.*

Proof. If D is principal then obviously $m = 0$ and $E = 0$. If D is not principal then $l(D) = 0$. Consider the difference $l(D + (m+1)P_\infty) - l(D + mP_\infty) \geq 0$. The Riemann-Roch theorem shows that this difference is

$$l(\kappa - D - (m+1)P_\infty) + (m+1) + 1 - g - (l(\kappa - D - mP_\infty) + m + 1 - g)$$

which is $l(\kappa - D - (m+1)P_\infty) - l(\kappa - D - mP_\infty) + 1$. Now, $l(\kappa - D - (m+1)P_\infty) \leq l(\kappa - D - mP_\infty)$. It follows that the values of $l(D + mP_\infty)$ increase with m in steps of only 0 or 1.

Let m be the unique smallest positive integer such that $l(D + mP_\infty) > 0$ and let f be the unique (up to scalar multiple) function $f \in L(D + mP_\infty)$. Then, as in the previous lemma, we define $E := (f) + D + mP_\infty$ and see that $E - mP_\infty = D + (f)$. □

The above result shows that there is a unique representative for each divisor class. The problem is then to give an algorithm which will reduce any divisor to this form. In Section 6 we describe a method which achieves this for the class of curves described in the introduction.

We now discuss a subtle point which is usually not mentioned in this context. The *Jacobian* of a curve C is naturally defined over the algebraic closure of the field k via the exact sequence

$$1 \longrightarrow Prin_{\bar{k}}(C) \cong \bar{k}(C)^*/\bar{k}^* \longrightarrow \mathrm{Div}_{\bar{k}}^0(C) \longrightarrow Jac_{\bar{k}}(C) = \mathrm{Pic}_{\bar{k}}^0(C) \longrightarrow 0. \tag{3}$$

This definition allows one to see that the Jacobian has a more functorial and geometric interpretation. One then defines the Jacobian over the field k to be $Jac_k(C) := Jac_{\bar{k}}(C)^G$ where $G = Gal(\bar{k}/k)$. Taking Galois cohomology of the short exact sequence (3) yields

$$1 \longrightarrow Prin_k(C) \longrightarrow \mathrm{Div}_k^0(C) \longrightarrow \mathrm{Pic}_{\bar{k}}^0(C)^G \longrightarrow H^1(G, Prin_{\bar{k}}(C))$$

which shows that the divisor class group is only a subgroup of the Jacobian. We now show that the Divisor Class Group is actually equal to the Jacobian.

Theorem 3. *Let C/k be a curve with a k-point. The map $\mathrm{Div}_k^0(C) \longrightarrow Jac_{\bar{k}}(C)^G$ is surjective.*

Proof. Fix a point P_∞ in $C(k)$. Let D be any divisor in $Jac_{\bar{k}}(C)^G$. As in Theorem 2 there is a unique smallest integer m such that $l(D + mP_\infty) = 1$ and $l(D + (m-1)P_\infty) = 0$. Let $f \in L(D + mP_\infty)$ and set E to be the effective divisor $(f) + D + mP_\infty$. We want to show that E is actually defined over k, rather than $\bar{k}$.

Now, let σ be any element of G. That $E - mP_\infty$ lies in $Jac_{\bar{k}}(C)^G$ means that $E^\sigma - mP_\infty^\sigma = E^\sigma - mP_\infty = E - mP_\infty + (h)$ for some function $h \in \bar{k}(C)$. In other words, $(h) = E^\sigma - E$.

This means that $(fh) = E^\sigma - D - mP_\infty$ and so $fh \in L(D + mP_\infty)$. It follows that h is a scalar, and that $E^\sigma = E$. □

Before giving the method of reduction of divisors we introduce a large class of curves which satisfy the restrictions imposed in the introduction.

3. The Geometry Of Superelliptic Curves

In this section we will provide a large class of curves of the form (1) which satisfy the four properties imposed in the introduction.

Let n and δ be any positive integers. Note that we do not assume that either n or δ are prime. By a *superelliptic curve* we will mean

$$C : y^n = c(x) := a_\delta x^\delta + \cdots + a_0 \tag{4}$$

defined over a field k (by which we mean that the coefficients a_j lie in k). We will assume $n, \delta \geq 3$ since elliptic and hyperelliptic curves can already be easily handled using other techniques.

In this section we will discuss some aspects of the geometry of superelliptic curves. For background consult Fulton [12].

To ensure that the affine curve C is non-singular we will impose the condition that $gcd(c(x), c'(x)) = 1$ (i.e., the polynomial $c(x)$ has no repeated roots) and the field k has characteristic not dividing n (in particular, characteristic zero is permitted). Note that, if we take n to be odd, all our results will be valid in characteristic 2.

We now consider the projective closure of C. If $n < \delta$ then the curve has the homogeneous equation

$$y^n z^{\delta - n} = a_\delta x^\delta + a_{\delta-1} x^{\delta-1} z + \cdots + a_0 z^\delta.$$

From this we see that the only point at infinity is $[x : y : z] = [0 : 1 : 0]$. This point is a singular point as long as $n + 1 < \delta$. If $n > \delta$ then similar arguments show that the point $[1 : 0 : 0]$ is the only point at infinity (and that this is singular when $n + 1 > \delta$). If $n = \delta$ then there are n different points at infinity (defined over $\bar{k}$), namely $[x : y : 0]$ where $y^n = a_\delta x^n$. These points are all not singular.

In the case $n \neq \delta$ we may blow up the singular point at infinity repeatedly until we have a non-singular model for the curve C. It can be shown that, if $(n, \delta) = 1$, then there is only one point above infinity on the non-singular model. In other words, the infinite prime is totally ramified. Furthermore, the condition that n be coprime to the characteristic of k implies that the ramification is tame.

For the case of hyperelliptic curves it is much easier to handle the behaviour of functions in the situation where infinity is ramified. Details of the more general case can be found in Paulus-Rück [19], where it is necessary to consider the infrastructure. Similar techniques may also work for the case of more general curves. in this paper, however, we will impose the restriction $(n, \delta) = 1$.

In this paper, "superelliptic curve" will always mean the non-singular model of the curve (4) over the field k, subject to the three restrictions:

1. $gcd(c(x), c'(x)) = 1$
2. n is not divisible by char k
3. $(n, \delta) = 1$.

Note that we will always be working with the non-singular model of C, but that there is no danger from just using the affine model (4) and treating the point at infinity as a formal symbol. The next task is to determine the genus of C.

Proposition 4. *The genus of the curve C is equal to $\frac{1}{2}(n-1)(\delta-1)$.*

Proof. Consider the map $\phi : C \to \mathbb{P}^1(k)$ given by $\phi : [x : y : z] \mapsto [x : z]$. This is a degree n map which has ramification points at infinity and the δ distinct zeroes of $c(x)$. All these points are totally ramified and have ramification index equal to n.

The Hurwitz formula (see Fulton [12] 8–36) therefore implies that

$$2(g-1) = 2n(0-1) + (\delta+1)(n-1)$$

from which we see $g = \frac{1}{2}(\delta-1)(n-1)$. □

Note that if $\delta = n+1$ then the genus of C attains the maximal possible genus for a degree δ curve.

We now make some comments about the number of points on a curve (4) over a finite field $\mathbb{F}_q$ (where we assume that the curve only has singular points at infinity and so, in particular, $(n, q) = 1$). If $(n, q-1) = 1$ then each value of $x \in \mathbb{F}_q$ gives rise to exactly one value $y \in \mathbb{F}_q$ (since nth roots always exist and are unique in this case). Similarly, if $(n, q^j - 1) = 1$ for $j = 1, 2, \ldots, g$ then $\#C(\mathbb{F}_{q^j}) = q^j + 1$ for $j = 1, 2, \ldots, g$. In this case, all the symmetric functions in the roots of the characteristic polynomial of Frobenius are equal to zero, from which it follows that the characteristic polynomial of Frobenius is simply $X^{2g} + q^g$. The Jacobian of C therefore has $q^g + 1$ points and is supersingular. For cryptographic purposes, supersingular abelian varieties must be avoided, as their discrete logarithms may be reduced to those in a finite field using the Tate pairing attack of Frey and Rück [10].

We now consider the function field $K = k(C)$ as a degree n extension of $k(x)$. The condition imposed earlier that n not be divisible by char k ensures that this algebraic extension of fields is separable. The discriminant of the field extension $K/k(x)$ is $(-1)^{n(n-1)/2} n^n c(x)^{n-1}$.

As above, this extension of fields is totally (and tamely) ramified at the infinite place of $k(x)$. One of the conditions imposed in the introduction is that the integral closure of $k[x]$ in K should be $k[x, y]$. The following result shows that this property holds for the curves we are considering.

Proposition 5. *Let C be a curve of the form (4) which satisfies the other conditions of this section. Then the integral closure of $k[x]$ in $K = k(C)$ is $k[x, y]$.*

Proof. Write $\mathcal{O}$ for the integral closure of $k[x]$ in K. The element y is integral over $k(x)$ and so the $\mathcal{O}$ must contain $k[x, y]$ with finite index (see, for instance, Frölich and Taylor [11] I.2.2).

The only primes which can effect this index are ones arising from square factors of the discriminant of $K/k(x)$ (in other words, powers of primes dividing $c(x)$).

Let $l(x)$ be some irreducible factor of $c(x)$. The minimal polynomial of y is $y^n - c(x)$ and this is an Eisenstein polynomial at $l(x)$. We now appeal to [11] Theorem 24 (also see Stichtenoth [22] III.5.12) which implies that $l(x)$ is totally ramified in $K/k(x)$ and that, locally at $l(x)$, the index of $k[x, y]$ in $\mathcal{O}$ is 1. □

4. The Divisor Class Group as an Ideal Class Group

Let C/k be a curve satisfying the properties listed in the introduction. Let $\mathcal{O}$ be the Dedekind ring which is the intersection of all valuation rings at all places expect for the place P_∞ at infinity. Then $\mathcal{O}$ is the integral closure of $k[x]$ in the extension $k(C)/k(x)$ and we have insisted that this be $k[x, y]$ (where the algebraic relation $C(x, y) = 0$ is implicit in $k[x, y]$).

We now show that the divisor class group of the curve C and the ideal class group of $\mathcal{O}$ are isomorphic.

Lemma 6. *Let C/k be a curve as above. Let $\mathrm{Cl}(\mathcal{O})$ be the ideal class group of $\mathcal{O} = k[x, y]$. Then*

$$\mathrm{Cl}(\mathcal{O}) \cong \mathrm{Pic}_k^0(C).$$

Proof. Let S be any (finite) set of places of the function field $k(C)$ and write $\mathcal{O}_S$ for the intersection of all valuation rings for places not in S. For any divisor $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$ we may identify each place $\mathfrak{p} \notin S$ with a prime ideal $\mathfrak{p} \subset \mathcal{O}_S$ and obtain the ideal $\prod_{\mathfrak{p} \notin S} \mathfrak{p}^{n_{\mathfrak{p}}}$. This induces the exact sequence

$$1 \rightarrow \mathrm{Ker} \rightarrow \mathrm{Pic}_k^0(C) \rightarrow \mathrm{Cl}(\mathcal{O}_S) \rightarrow 1$$

where Ker is the subgroup of $\mathrm{Pic}_k^0(C)$ generated by all degree zero divisors with support lying in S.

In our case we have $S = \{P_\infty\}$, which implies $\mathrm{Ker} = \{0\}$, and the result follows. □

For curves C/k which satisfy the properties of the introduction, we therefore have

$$Jac_k(C) \simeq \mathrm{Pic}_k^0(C) \simeq \mathrm{Cl}(k[x, y]).$$

Our task of computing in $Jac_k(C)$ is therefore reduced to task of composing and reducing ideal classes in $\mathrm{Cl}(\mathcal{O})$. First we will introduce some of the basic theory of ideals in $k[x, y]$.

5. Ideals in Function Fields

Every element of $K = k(C)$ may be written as $\sum_{i=0}^{n-1} a_i(x)y^i$ where $a_i(x) \in k(x)$. The extension $K/k(x)$ is Galois since it is the splitting field of the polynomial $C(x,y)$ over $k(x)$. The *norm* of an element $\alpha = \sum_{i=0}^{n-1} a_i(x)y^i \in k(C)$ is defined to be $N_{K/k(x)}(\alpha) := \prod_{\sigma \in Gal(K/k(x))} \sigma(\alpha)$. The norm of α lies in $k(x)$. In other words $N_{K/k(x)}(\alpha)$ is the degree zero (in Y) coefficient of the *minimal polynomial* $\prod_{\sigma \in Gal(K/k(x))}(Y - \sigma(\alpha))$ for α. We define the *degree* of an element α to be $\deg(\alpha) = \deg_x N_{K/k(x)}(\alpha)$. Therefore, $\deg(a(x)) = n \deg_x(a(x))$.

An *integral ideal* of $\mathcal{O}$ is an additive subgroup of $\mathcal{O}$ which is also a $\mathcal{O}$-module. We will use two different representations of ideals (and hopefully no confusion will arise):

- The notation $(a_1(x,y), ..., a_m(x,y))$ (where m is usually 1 or 2) will represent the ideal
$$\{b_1(x,y)a_1(x,y) + \cdots + b_m(x,y)a_m(x,y) : b_1(x,y), \ldots, b_m(x,y) \in \mathcal{O}\}.$$
- The notation $[a_1(x,y), \ldots, a_n(x,y)]$ represents the $k[x]$-module
$$\{b_1(x)a_1(x,y) + \cdots + b_n(x)a_n(x,y) : b_1(x), \ldots, b_n(x) \in k[x]\}.$$
Every ideal may be written in this form. However, it is not true that every such module is an ideal.

A *fractional $\mathcal{O}$-ideal* (i.e. an ideal corresponding to a non-effective divisor) is represented by an integral $\mathcal{O}$-ideal and a denominator which lies in $k[x]$. The set of classes of fractional ideals forms the abelian group $\mathrm{Cl}(\mathcal{O})$. In this paper we will mainly be considering integral ideals and so we will usually omit the adjective "integral".

Every integral ideal of $\mathcal{O}$ is a $k[x]$-module and thus (using the notation above) can be represented by a basis $[\alpha_0, \cdots, \alpha_{n-1}]$, where
$$\alpha_i = \sum_{j=0}^{n-1} a_{ij}(x)y^j,$$
with $a_{ij}(x) \in k[x]$. This representation can be made unique by computing the Hermite Normal Form (HNF) of the matrix $(a_{ij})_{i,j=0,\ldots n-1}$. Similarly, a fractional ideal is represented by a denominator and a $k[x]$-module in HNF as above.

Composition of $k[x]$-modules is performed by multiplying termwise and then taking the HNF reduction as described in Cohen [8].

The *degree* of a (fractional) ideal in HNF is given by the degree of the product of the diagonal elements (minus the degree of the norm of the denominator) and denoted by deg. It turns out that the degree of a principal ideal equals the degree of a generator. The degree of an ideal is equal to the degree of the divisor corresponding to the ideal.

If $(x_0, y_0) \in C(k)$ then the unique HNF $k[x]$-module corresponding to the place (x_0, y_0) is given by $[x - x_0, y - y_0, y^2 - y_0^2, \cdots, y^{n-1} - y_0^{n-1}]$. One sees that the degree of this ideal is indeed 1. Similar calculations enable one to find a $k[x]$-module representation of any ideal.

We emphasise that we are considering three different notions of degree:

- If $a(x,y) \in \mathcal{O}$ then we write $\deg_x(a(x,y))$ and $\deg_y(a(x,y))$ for the usual degrees of $a(x,y)$ as a polynomial.

- If $\alpha = \sum_{i=0}^{n-1} a_i(x)y^i \in K = k(C)$ then we write
$$\deg(\alpha) = \deg_x(N_{K/k(x)}(\alpha)).$$
- If $\mathfrak{a}$ is an ideal then we have $\deg(\mathfrak{a})$ to be the degree of the corresponding divisor (which can be computed from the HNF of the $k[x]$-module representation of $\mathfrak{a}$).

We now explain how to determine how a "finite" prime of $k(x)$ decomposes in K.

Proposition 7. *Let C/k be a curve satisfying the properties of the introduction. Let $p(x)$ be an irreducible polynomial in $k[x]$ and suppose $C(x,y)$ factors modulo $p(x)$ as $\prod_{i=1}^{m} r_i(x,y)^{e_i}$. Then the prime $p(x)$ splits as $(p(x)) = \prod_{i=1}^{m}(p(x), r_i(x,y))^{e_i}$ where each ideal $(p(x), r_i(x,y))$ is a prime ideal of K of ramification degree e_i and residue class degree $f_i = \deg_y r_i(x,y)$.*

Proof. See Stichtenoth [22] Theorem III.3.7. □

We now give an interpretation of Lemma 1 and Theorem 2 in terms of the ideal class group of $\mathcal{O}$. Lemma 1 becomes

> *Let D be an ideal of $\mathcal{O}$. There is an integral ideal E of $\mathcal{O}$ equivalent to D with* $\deg(E) = g$.

and Theorem 2 becomes

> *Let D be an ideal of $\mathcal{O}$ and let E be an integral ideal equivalent to D for which* $\deg(E)$ *is minimal. Then E is unique.*

6. Computing reduced divisors

6.1. The idea. For this section we allow k to be a field of any characteristic. The methods given will work for any curve C/k of the form described in the introduction, however we only provide the full details in the case of superelliptic curves.

We have seen that the problem of reduction of divisors comes down to the problem of reduction of ideals. We will solve this problem by using similar ideas to those developed for number field arithmetic (see Cohen [8] or [4]). Unlike the number field situation, we can prove that our algorithm always computes the "smallest" reduced ideal (with respect to the degree of the norm). The strategy is as follows:

Assume that we can compute an element e of smallest norm in an integral ideal D. Then we prove that $(e)/D$ is an ideal equivalent to D^{-1} which has smallest norm among all ideals equivalent to D^{-1}. This fact can be used in our situation by first computing an ideal which is equivalent to D^{-1} and then looking for an element of smallest norm therein. Thus, a class is uniquely given by a representation of the specific reduced divisor. The representation of such a divisor can be made unique by using the Hermite normal form representation of the ideal as a $k[x]$-module.

The computation of the element e can be achieved by a modified lattice reduction as follows: We first show that the degree of the norm of an element is a "metric" on the Dedekind ring $\mathcal{O}$ by using properties of the embedding of superelliptic curves into a field of Puiseux expansions. We use the word "metric" to mean that it satisfies the properties required for the lattice reduction (the word "norm" would be more appropriate, but also more confusing). Furthermore, we modify the lattice basis reduction algorithm and corresponding invariants from [18] in such a way that they work with the new metric. In this way, we can compute a element of an ideal whose norm is of smallest degree.

All these computations are exact and do not need any computation in the field of puiseux expansions. This is due to the very special nature of these superelliptic curves and the representation with a Dedekind ring where the prime at infinity is totally ramified. This situation does not exist in the number field case for $n > 2$ since there is no number field with a totally ramified prime at infinity. Therefore, this is a natural generalization of the imaginary quadratic case, which enables a simple arithmetic for jacobians of hyperelliptic curves.

6.2. **The reduction procedure.** Let D be a fractional ideal of $\mathcal{O}$. Then we call the unique integral ideal E equivalent to D such that $\deg E$ is minimal the *reduced* ideal corresponding to D. To compute E for a given D, we need the following lemma.

Lemma 8. *Let D be an integral ideal of $\mathcal{O}$. Let e be an element of D with minimal degree and define $A := (e)/D$. Then A is the reduced ideal corresponding to D^{-1}.*

Proof. First note that $(e)/D$ is an integral ideal. Now, consider the set of principal ideals which are constructed as follows: multiply D by every integral ideal A in the class of D^{-1}. The generators of the ideals in this set are elements e of D and their degree is equal to $\deg D + \deg A$, where A. Obviously $\deg e$ is minimal iff $\deg A$ is minimal. Thus, determining an element of smallest degree in D yields an ideal A of smallest degree equivalent to D^{-1}.
But since there is only one integral ideal in a given class of smallest degree, namely the reduced ideal, e must be unique up to multiplication by a unit (and the units are all scalars in this case), and so $A = (e)/D$ is the reduced ideal in the class of D^{-1}. □

We can then formulate the following algorithm for computing the reduced ideal corresponding to an integral ideal D:

- Compute an integral ideal equivalent to D^{-1}, namely $E := \prod_{\sigma \neq 1} D^{\sigma}$.
- Compute the shortest vector e in E.
- Output $(e)/E = (e) \cdot D/N_{K/k(x)}(D)$.

It is possible to generalize this algorithm to Jacobians of function fields which do not have a totally ramified prime (at infinity). In that case, the divisor class group is not isomorphic to the ideal class group, and so one one must pay attention to the infrastructure. This is the set of divisors whose support contains only infinite primes and it is related to the behaviour of the non-trivial units of $\mathcal{O}$. In any case, the reduced ideal produced by the above algorithm would not correspond to a single divisor class and it is not clear how to distinguish the divisor classes corresponding to the given ideal.

6.3. **Embeddings of function fields.** To explain the algorithm, we need to introduce some theory and notation about embeddings of function fields into Puiseux expansion fields. In this paper, we limit ourselves to the situation of a curve with a totally ramified prime at infinity. The more general theory goes back to Mahler [15]; we adopt the notation of [20].

Let $l \in \mathbb{N}$. We call

$$k\langle x^{1/l}\rangle := \left\{ \sum_{i=-\infty}^{m} \zeta_i x^{i/l} \mid \zeta_i \in k, \zeta_m \neq 0 \right\}$$

the *field of puiseux series* in $x^{1/l}$ over k. A slightly non-standard valuation deg on $k\langle x^{1/l}\rangle$ is given by

$$\deg\left(\sum_{i=-\infty}^{m}\zeta_i x^{i/l}\right) := m/l.$$

These fields allow some geometry analogous to Minkowski's theory [15]. We will now explain how to embed $k(C)$ into such fields.

Theorem 9. *Let $C(x,y)$ be a curve over a field k. Suppose $k(C)/k(x)$ is a degree n extension having a totally ramified prime at the "infinite" place of $k(x)$. Let $\rho_1,\dots,\rho_n$ be the distinct elements in $\overline{k(x)}$ such that $C(x,\rho_i)=0$ and let k_n the field extension of k containing the n-th roots of unity. Then*

$$\rho_1,\dots,\rho_n \in k_n\langle x^{1/n}\rangle.$$

For the proof see e.g. [24]. This is a special case of Theorem 9 in [20]. By this method, we get an embedding of $k(C)$ into $L := (k_n\langle x^{1/n}\rangle)^n$:

$$k(C)\ni\alpha=\sum_{j=0}^{n-1}a_j(x)y^j\longmapsto(\alpha^{(1)},\dots,\alpha^{(n)})=\left(\sum_{j=0}^{n-1}a_j(x)\rho_i^j\right)_{i=1,\dots,n}\in L.$$

Let us call this map L by abuse of notation. The image of an ideal of $\mathcal{O}$ under L is a *lattice* (i.e., it is a $k[x]$-module and it has a basis as a $k[x]$-module which is also a basis for L as a vector space over $k_n\langle x^{1/n}\rangle$). The vector space L is equipped with a norm N, namely $N(L(\alpha))=\max\{\deg(\alpha^{(i)})\}$.

We now return to the case of superelliptic curves: $y^n=c(x)$ and define δ to be $\deg_x c(x)$ with $(\delta,n)=1$. To generalize to a larger class of curves one must consider a more general norm form.

All $\deg(\rho_i)$ are equal to δ/n; this can be seen as follows: since $\rho_i=\mu_n^k\rho_j$ for some k, where μ_n is an n-th root of unity and $\prod_{i=1}^n\rho_j=c(x)$, and $(\delta,n)=1$. So, $\deg(\alpha^{(i)})$ equals $\max_j\{\deg a_j+\delta j/n\}$, thus they are all equal.

Recall that $\deg(\alpha)$ is defined to be the degree (in x) of the norm of α in the extension $k(C)/k(x)$. The following lemma relates the two definitions of norm.

Lemma 10. *Let C/k be a superelliptic curve and let $\alpha=\sum_{j=0}^{n-1}a_j(x)y^j\in k(C)$. We have $\deg(\alpha)=n\cdot N(L(\alpha))=\max_j\{(\deg_x a_j(x))n+\delta j\}$.*

Proof. The following computation is performed in $k_n\langle x^{1/n}\rangle$. We have

$$\begin{aligned}\deg(\alpha) &= \deg_x(N_{k(C)/k(x)}(\alpha))=\deg_x(\prod_{i=1}^n\alpha^{(i)})=\sum_{i=1}^n\deg(\alpha^{(i)})\\ &= n\cdot\max_j\{\deg_x a_j(x)+\delta j/n\}\end{aligned}$$

and the proof follows. □

From this lemma one sees that we have a suitable "metric" (or norm) on $\mathcal{O}$ for performing lattice reduction techniques. In other words

Corollary 1. *Let $\alpha=\sum_{j=0}^{n-1}a_jy^j\in\mathcal{O}$. The function*

$$\deg(\alpha)=\max_j\{\deg a_jn+\delta j\}$$

is a metric on $\mathcal{O}$.

Due to this result, we do not need to compute with elements of the field of puiseux expansions but we can compute with just elements of $k(C)$. Observe that we do not need to extend the ground field in order to be able to add divisors. This is a very important consideration for the applications.

Nevertheless, we do need a modified lattice basis reduction algorithm which takes the modified metric into account.

6.4. **Modified lattice basis reduction.** In contrast to lattices in vector spaces over $\mathbb{Q}$, there exists a lattice basis reduction algorithm which always computes a reduced basis for lattices over function fields. In particular, this algorithm computes the smallest element with respect to the maximum norm as a metric. In this section, we will mention the necessary modifications to show that we can apply the lattice reduction algorithm with our modified metric to compute an element of an ideal with smallest norm. The original algorithm, as well as the proofs, can be found in [18].

To an element $\beta = \sum_{i=0}^{n-1} b_j y^j \in K(C)$ we associate its vector representation $b = (b_0, \dots, b_{n-1})$. To agree with the new norm, we define $|b_i| = n \deg b_i + i\delta$ and $|b| = \max |b_i| = \deg \beta$.

Let $b_1, b_2, \dots, b_n \in k[x]^n$ be linearly independent over $k(x)$. The *lattice* $L \subset k[x]^n$ of *rank* n spanned by $b_1, \dots, b_n$ is defined as

$$L = \sum_{j=1}^{n} k[x] b_j = \left\{ \sum_{j=1}^{n} r_j b_j : r_j \in k[x] \quad (1 \leq i \leq n) \right\}.$$

In our special situation, an ideal given by a basis as a $k[x]$-module will be the lattice spanned by the elements of the basis.

The *determinant* $d(L) \in k[x]$ of L is defined as the determinant of the $n \times n$ matrix B having the modified vectors $b_1^*, \dots, b_n^*$ as columns. The vectors are modified in the following way: if $b = (b_0, \dots, b_{n-1})$, then $b^* = ((b_0)^n, (b_1)^n \cdot x^{\delta}, \dots, (b_i)^n \cdot x^{i\delta}, \dots, (b_{n-1})^n \cdot x^{(n-1)\delta})$. The value of $d(L)$ does not depend on the choice of a basis of L up to units of K. The *orthogonality defect* $OD(b_1, \dots, b_n)$ of a basis $b_1, \dots, b_n$ for a lattice L is defined as

$$\sum_{i=1}^{n} |b_i| - \deg_x d(L).$$

We have $OD(b_1, \dots, b_n) \geq 0$; this is easily proved by computing the determinant by e.g. starting by the first column. We say that the basis $b_1, \dots, b_n$ is *reduced* if $OD(b_1, \dots, b_n) = 0$. It follows immediately that the length of the i-th vector of a reduced basis is the i-th successive minimum of L with respect to the new metric. Especially, the first vector will be the shortest vector of the lattice, i.e. it will represent an element of the ideal with smallest degree norm.

In the following, if we speak about permuting coordinates, this means that we put the y-exponent and thus its degree modification to the corresponding coordinate when flipping its place in the vector.

Lemma 11. *Let $b_1, \dots, b_n$ be a basis for a lattice L and denote $b_{i,j}$ the j-th coordinate of b_i. If the coordinates of the vectors $b_1, \dots, b_n$ can be permuted in such a way that they satisfy*

1. $|b_i| \leq |b_j|$ *for $1 \leq i < j \leq n$ and*
2. $|b_{i,j}| < |b_{i,i}| \leq |b_{i,k}|$ *for $1 \leq j < i < k \leq n$,*

then the basis $b_1, \dots, b_n$ is reduced.

Again, this is easily proved by developing the determinant according to the first column and paying attention to the degree modifications. We only mention the existence and the complexity of the reduction algorithm, since the formulation and its correctness are now analogous to the original case and can be found in [18]:

Lemma 12. *There exists an algorithm which takes*

$$O(n^3 \cdot \max|b_i| \cdot OD(b_1, \dots, b_n))$$

arithmetical operations in k to compute a reduced basis starting from a basis $b_1, \dots, b_n$.

We give now a very rough estimate on the complexity for the composition algorithm on the divisor class group of a curve.

Lemma 13. *The composition on the divisor class group C of a superelliptic curve C/k as in the introduction may be performed in $O(n^6\delta^2 g^2)$ operations in the field k.*

Proof. The composition algorithm consists of the following steps: multiplication of ideal representations, computation of an ideal equivalent to the inverse, finding a shortest vector and finally compute a product of ideals. We refer to the standard literature [8] for the complexity of arithmetic of ideals. Let m be an upper bound for the degree of every element in each of the vectors in a basis of a reduced ideal in Hermite normal form.

The multiplication of ideal representations is possible in $O(n^4m)$ field operations, the subsequent Hermite normal form computation is then of complexity $O(n^2m^2)$. Thus ideal multiplication is of complexity

$$O(\max\{n^4m, n^2m^2\}).$$

The computation of the product of the other conjugates amounts to about n multiplications of ideals and thus is therefore (the degrees of the polynomials involved may grow by m with every multiplication) $O(\max\{n^6m, n^5m^2\})$.
The computation of a smallest element in an ideal is of complexity $O(n^3 \cdot \delta m \cdot OD)$, where OD is bounded by $\sum_{i=1}^{n} nm = O(n^2m)$, thus is at most $O(n^6m^2)$. The final multiplication now is of lower complexity, thus can be omitted.

Finally, we have to estimate an upper bound for the norms of the basis vectors of an ideal I, i.e. for m. Since the matrix representation will be given in Hermite normal form and the determinant of the matrix is equal to the degree of the norm of the corresponding ideal, we get immediately $m \leq \delta \deg I$. Since $\deg I \leq g$ for a reduced ideal I, we have $m \leq \delta g$. This finishes the proof. □

7. Discrete Logarithms

We now return to the more general model

$$C : C(x, y) = \sum_{i=0}^{n} c_i(x) y^i$$

for our curve C (subject to the restrictions given in the introduction) but restrict to the case where the field k is a finite field $\mathbb{F}_q$. We let $\delta = \max \deg_x c_i(x)$.

The discrete logarithm problem on $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ is the following: given a divisor class D_1 and some divisor class D_2 in the subgroup of $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$ generated by D_1, find an integer λ such that $D_2 \equiv \lambda D_1$. This problem is the central problem for cryptography on abelian varieties.

In the following sections we will generalize the algorithm of Adleman-DeMarrais-Huang [1], which was developed for solving discrete logarithms in jacobians of hyperelliptic curves.

8. Explicit bounds for a generating system

In this section we generalize the method of Müller, Stein and Thiel [16] to show the following result, for the curves $C(x,y)$ above.

Theorem 14. *Let*

$$d := \mathit{next\_prime}\left(\max\left\{n, \frac{2\log(4g-2)}{\log q}\right\}\right)$$

then the divisor class group (which, in this case we are thinking of as an ideal class group), of C is generated by the set of prime ideals of residue class degree one whose norm is less than q^d.

To prove this result we will need to use zeta functions. We refer the reader to [16] for further explanation of the notation. Let χ denote a character of finite order on $\mathrm{Pic}_k^0(C)$ and extend χ to act on $\mathrm{Div}_k^0(C)$ in the natural way. We let 1 denote the trivial character, and define two zeta functions, where $u = q^{-s}$, by

$$\begin{aligned} Z(u,\chi,K) &= \prod_{\mathfrak{p}} \frac{1}{1-\chi(\mathfrak{p})u^{\deg \mathfrak{p}}}, \\ Z(u,K) &= Z(u,1,K) = \prod_{\mathfrak{p}} \frac{1}{1-u^{\deg \mathfrak{p}}}, \end{aligned}$$

where both products are over the set of prime divisors of K. It is well known that both zeta functions can be expressed as polynomials in u, with respective roots $\omega_i(\chi)$ and ω_i,

$$\begin{aligned} Z(u,K) &= \frac{\prod_{i=1}^{2g}(1-\omega_i u)}{(1-u)(1-qu)}, \\ Z(u,\chi,K) &= \prod_{i=1}^{2g-2}(1-\omega_i(\chi)u). \end{aligned}$$

A consequence of the Riemann Hypothesis (which was proved by Weil) for function fields is that all roots satisfy

$$|\omega_i| = |\omega_i(\chi)| = \sqrt{q}.$$

We can now prove the theorem.

Proof. Suppose the prime divisors of residue class degree one and norm less than q^d only generate a proper subgroup $G \subsetneq \mathrm{Pic}_k^0(C)$. Then let χ be any character which is trivial on G but non-trivial on $\mathrm{Pic}_k^0(C)$.

Since $\chi(\mathfrak{p}) = 1$ for all prime divisors $\mathfrak{p}$ of residue class degree one and norm less than q^d then some of the Euler factors in $Z(u,K)$ agree with some of the Euler factors in $Z(u,\chi,K)$. We let $\prod^*$ denote the product over all prime divisors of residue degree one and norm less than or equal to q^d, whilst $\prod^{\dagger}$ will denote the product over all other prime divisors. We obtain

$$\begin{aligned}
\prod_{i=1}^{2g-2} (1 - \omega_i(\chi)u) &= Z(u, \chi, K) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p})u^{\deg \mathfrak{p}}}, \\
&= \prod{}^{*} \frac{1}{1 - \chi(\mathfrak{p})u^{\deg \mathfrak{p}}} \prod{}^{\dagger} \frac{1}{1 - \chi(\mathfrak{p})u^{\deg \mathfrak{p}}}, \\
&= Z(u, K) \prod{}^{\dagger} \frac{1 - u^{\deg \mathfrak{p}}}{1 - \chi(\mathfrak{p})u^{\deg \mathfrak{p}}}, \\
&= \frac{\prod_{i=1}^{2g}(1 - \omega_i u)}{(1-u)(1-qu)} \prod{}^{\dagger} \frac{1 - u^{\deg \mathfrak{p}}}{1 - \chi(\mathfrak{p})u^{\deg \mathfrak{p}}}.
\end{aligned}$$

We take the logarithmic derivatives of this equation to obtain

$$\sum_{v=0}^{\infty} \sum_{i=1}^{2g-2} \omega_i(\chi)^{v+1} u^v = \sum_{v=0}^{\infty} \sum_{i=1}^{2g-2} \omega_i^{v+1} u^v - \sum_{v=0}^{\infty} u^v - \sum_{v=0}^{\infty} q^{v+1} u^v + P(u), \qquad (5)$$

where $P(u)$ is the polynomial

$$P(u) = \sum{}^{\dagger} \sum_{v=1}^{\infty} (\deg \mathfrak{p}) u^{v(\deg \mathfrak{p})-1} (\chi(\mathfrak{p})^v - 1),$$

and $\sum^{\dagger}$ is the sum over all prime divisors of norm greater than q^d of residue class degree greater than one. If we consider the coefficient of u^{d-1} of $P(u)$ we find that it is equal to

$$A = \sum{}^{+} (\deg \mathfrak{p})(\chi(\mathfrak{p})^{d/\deg \mathfrak{p}} - 1),$$

where the sum is now over all prime divisors of degree a divisor of d and of residue class degree greater than one. Hence, since d is prime, the only divisors in the last sum must be of degree d or 1. But they cannot be of degree one, since if $\mathfrak{p}$ lies above p and $\mathfrak{p}$ has residue class degree greater than one, we have

$$\deg \mathfrak{p} \geq f_{\mathfrak{p}} > 1.$$

So the sum is over all divisors of degree d and of residue class degree greater than one. But, again since d is prime, we then conclude that the residue class degree is equal to d, but this is impossible since the residue class degree must be less or equal to than n and $d > n$. Hence the sum is empty and $A = 0$.

We now look at the coefficient of u^{d-1} in equation (5). Since the coefficient of u^{d-1} in $P(u)$ vanishes we have

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

By the Riemann Hypothesis for function fields we deduce that

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

which implies

$$d \leq \frac{2\log(4g-2)}{\log q}.$$

This contradicts the choice of d. Therefore χ must be the trivial character and $G = \mathrm{Pic}_k^0(C)$. □

9. The Algorithm

In this section we shall describe a method (based on that of Adleman-DeMarrais-Huang [1]) for solving discrete logarithms on $\mathrm{Pic}_k^0(C)$. A variant of the Hafner-McCurley method as described in [17] could also be applied to solve this problem. This would involve composing random multiples of divisors, reducing them and then factoring them over the given factor base. The Hafner-McCurley method is easier to analyse from a theoretical point of view. Nevertheless, obtaining a non-heuristic analysis would be very difficult to achieve. For function fields of degree greater than two the Hafner-McCurley approach is less amenable to practical implementation than the method we shall give below. This last fact is for a number of reasons:

1. To obtain the non-heuristic running time one must restrict to dense matrices. This means we cannot use sparse techniques. In a practical algorithm this would become a major computational bottleneck. The method we propose will produce sparse matrices.
2. In function fields of degree greater than two it appears unlikely that an efficient sieving technique like that applied in degree two fields in [9] can be found. The method below does allow efficient sieving strategies to be employed.
3. The factor base for the Hafner-McCurley style method is the set of all prime ideals of norm less than some bound. In our method we need only to take all prime ideals *of residue class degree one* less than some bound. This means for the same size factor base we have a larger bound, and hence more chance of factoring an element of a fixed size.

We therefore leave, as a theoretical exercise for the reader, the analysis for the Hafner-McCurley style method for function fields of degree greater than two. We shall focus instead on giving a heuristic analysis of a method which would appear to be far more suitable in practice.

First we recall the result of [1].

Theorem 15 (Adleman, De Marrais and Huang). *There is a heuristic sub-exponential algorithm to solve the discrete logarithm problem in the Jacobian of an (odd degree) hyperelliptic curve $C/\mathbb{F}_p$ of genus g, assuming that*

$$\log p < (2g+1)^{0.98}.$$

A heuristic analysis shows that the method runs in time

$$O\left(L_{p^{2g+1}}(1/2, c)\right)$$

for some constant c as $g \to \infty$.

As usual we have used the function

$$L_N(\alpha, \beta) = \exp(\beta(\log N)^\alpha (\log\log N)^{1-\alpha})$$

to interpolate between polynomial ($\alpha = 0$) and exponential ($\alpha = 1$) time.

In this section we shall show

Theorem 16. *Let $C/\mathbb{F}_q$ be a curve as in the introduction. There is a heuristic sub-exponential algorithm to solve the discrete logarithm problem in $\mathrm{Pic}_{\mathbb{F}_q}^0(C)$ for the general curve C above assuming*

$$\log q \geq \frac{2\log\delta}{\delta}.$$

The heuristic complexity is given by

$$O\left(L_{e^\delta}(1/2, \sqrt{2\log q} + o(1))\right)$$

as $\delta \to \infty$. We assume in the analysis that n and q are fixed.

In the case of hyperelliptic curves our method and that of Adleman, De Marrais and Huang are practically identical.

If C is a superelliptic curve then the group size is $O(q^g)$ and the complexity estimate in the above theorem becomes $L_{q^g}(1/2, 2/\sqrt{n-1} + o(1))$ as δ tends to infinity.

9.1. **Basic Definitions and Results.** Each prime divisor of K (resp. prime in $\mathbb{F}_q[x]$) induces a valuation on K (resp. $\mathbb{F}_q[x]$). Each prime divisor D_i corresponds to a non-conjugate embedding, $K^{(i)}$, of K into some local field, where the image of this divisor is the only prime. If $\phi \in K$ and $\phi^{(i)}$ is its image in $K^{(i)}$ then we can extend the valuation $p(x)$ of $\mathbb{F}_q[x]$ to $K^{(i)}$ in an essentially unique way by defining

$$\mathrm{ord}_{p(x)}(\phi^{(i)}) = \frac{1}{e_i}\mathrm{ord}_{D_i}(\phi)$$

We will be interested in functions of the form

$$\phi(x,y) = a(x) + b(x)y \in K.$$

We have

$$N_\phi = N_{K/\mathbb{F}_q[x]}(\phi) = a(x)^n - c_{n-1}(x)a(x)^{n-1}b(x) + \cdots + (-1)^n c_0(x)b(x)^n.$$

We wish to have a simple procedure which will allow us to decompose $\mathrm{div}\phi$ into prime divisors

$$\mathrm{div}\phi = \sum m_i D_i - \sum m_i \infty$$

with $m_i > 0$. Clearly if D is a prime divisor which lies above $p(x)$ and $\mathrm{ord}_{p(x)}(\phi) > 0$ then $p(x)$ divides N_ϕ. So we need to determine which prime divisors D, lying above $p(x)$, are in the support of $\mathrm{div}\phi$ and to what multiplicity.

Lemma 17. *Let D_1 and D_2 denote two distinct prime divisors lying above the prime $p(x) \in \mathbb{F}_q[x]$. Let $a(x), b(x)$ denote two coprime elements of $\mathbb{F}_q[x]$.*

1. *There is at most one prime divisor $D \in \{D_1, D_2\}$ such that*

$$\mathrm{ord}_D(a(x) + b(x)y) > \max\{e_1, e_2\}\mathrm{ord}_{p(x)}(y_1^{(k)} - y_2^{(l)}) \tag{6}$$

where $D_i = (p(x), r_i(x,y))$, $y_i \in \overline{\mathbb{F}_q(x)}$ is any root in y of the polynomial $r_i(x,y) \mod p(x)$. The index k (resp. l) is arbitrarily chosen from the set $\{1, \ldots, \deg_y r_1(x,y)\}$ (resp. $\{1, \ldots, \deg_y r_2(x,y)\}$).

2. *If (6) holds for $D = D_i$ and $e_i > 1$ or $f_i > 1$ then*

$$\mathrm{ord}_{D_i}(a(x) + b(x)y) \leq e_i \mathrm{ord}_{p(x)}(y_i^{(k)} - y_i^{(l)}).$$

where k and l are arbitrarily chosen from the set $\{1, \ldots, \deg_y r_i(x,y)\}$.

Proof. We write $\mathrm{div}(a(x) + b(x)y) = v_1 D_1 + v_2 D_2 + E - m\infty$ where $v_i \geq 0$ and E is an effective divisor such that $\{D_1, D_2\} \cap \mathrm{Supp}(E) = \emptyset$. To prove the first statement we need to show

$$\min\{v_1, v_2\} \leq \max\{e_1, e_2\}\mathrm{ord}_{p(x)}(y_1^{(k)} - y_2^{(l)}),$$

the second statement will follow in a similar way. We have

$$\frac{\min\{v_1,v_2\}}{\max\{e_1,e_2\}}. \leq \frac{v_i}{e_i} \leq \frac{1}{e_i}\mathrm{ord}_{D_i}(\phi) = \mathrm{ord}_{p(x)}(a(x)+b(x)y_i^{(k)}).$$

Hence

$$\begin{aligned}\frac{\min\{v_1,v_2\}}{\max\{e_1,e_2\}} &\leq \min\left(\mathrm{ord}_{p(x)}(a(x)+b(x)y_i^{(k)}), \mathrm{ord}_{p(x)}(a(x)+b(x)y_j^{(l)})\right)\\ &\leq \mathrm{ord}_{p(x)}\left(b(x)(y_1^{(k)}-y_2^{(l)})\right)\end{aligned}$$

Now if $b(x) \equiv 0 \pmod{p(x)}$ then, since $a(x)$ and $b(x)$ are coprime, we would have $p(x)$ does not divide N_ϕ and so $v_1 = v_2 = 0$ and we are done. Hence assume $p(x)$ does not divide $b(x)$ but then

$$\min\{v_1,v_2\} \leq \max\{e_1,e_2\}\mathrm{ord}_{p(x)}(y_1^{(k)}-y_2^{(l)})$$

as required. □

If we define $\mathcal{D}$ to be the discriminant of $C(x,y)$ with respect to y, then we obtain:

Corollary 2. *If $p(x)$ is a prime of $\mathbb{F}_q[x]$ which does not divide the discriminant $\mathcal{D}$ then there is at most one prime divisor, D_i, lying above $p(x)$ such that $\mathrm{ord}_{D_i}(\phi) > 0$ and it satisfies $e_i = f_i = 1$.*

Proof. If $p(x)$ is a prime as described and D_i is a prime divisor lying above $p(x)$ then $e_i = 1$. So if $f_i > 1$ then we have, by the above Lemma, that $\mathrm{ord}_{p(x)}(\phi) \leq 0$. □

Hence decomposing $\phi = a(x) + b(x)y$ is trivial: We suppose that $p(x)^t$ exactly divides N_ϕ.

If $p(x)$ is a prime of $\mathbb{F}_q[x]$ which does not divide $\mathcal{D}$ we see that there is only one prime divisor, D, lying above $p(x)$ in the support of ϕ. We set

$$r(x,y) = y - \frac{a(x)}{b(x)} \pmod{p(x)}.$$

This last definition will make sense because since $a(x)$ and $b(x)$ are coprime we cannot have $p(x)$ dividing $b(x)$. We then put $D = (p(x), r(x,y))$, so D is a prime divisor of residue class degree equal to one and $\mathrm{ord}_D(\phi) = t$.

If $p(x)$ divides $\mathcal{D}$ and there is one prime divisor, D, lying above $p(x)$ then we have $\mathrm{ord}_D(\phi) = et/f$, where e and f are the ramification and residue degrees of D.

For hyper- and super- elliptic curves these last two cases exhaust all possibilities. For other curves any additional cases when $p(x)$ divides $\mathcal{D}$ can be handled on an ad hoc basis.

9.2. **The Main Algorithm.** We are now in a position to describe the main algorithm for solving discrete logarithm problems in the divisor class group of our curve. We assume we are given two reduced divisors D_1 and D_2 representing classes in $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$. We are asked to solve the equation

$$D_1 \equiv \lambda D_2.$$

We let $a = 1/\sqrt{2\log q}$ and let $b = 1/\sqrt{\log q}$, we then set

$$\begin{aligned} S_1 &= a(\delta\log\delta)^{1/2},\\ S_2 &= b(\delta\log\delta)^{1/2}.\end{aligned}$$

The algorithm we shall describe will be an index calculus type method, so the first thing we shall need to do is to construct a factor base, $\mathcal{F}$.

We shall place into $\mathcal{F}$

1. all prime divisors which lie above primes of $\mathbb{F}_q[x]$ which divide $\mathcal{D}$,
2. all prime divisors which are in the support of D_1 and D_2.
3. all unramified prime divisors of residue class degree equal to one which lie above a prime $p(x) \in \mathbb{F}_q[x]$ of norm less than or equal to q^{S_1}.

We expect the size of $\mathcal{F}$ to be roughly equal to the number of irreducible polynomials of degree less than or equal to S_1. So we have

$$\#\mathcal{F} \leq q^{S_1} = L_{e^\delta}(1/2, c_1)$$

where $c_1 = \sqrt{\frac{\log q}{2}}$. As long as $S_1 \geq d$ (which is true for sufficiently large δ) then, by Theorem 14, $\mathcal{F}$ will generate the group $\mathrm{Pic}^0_{\mathbb{F}_q}(C)$.

Our first task is to find some relations linking D_1 and D_2 to the elements of $\mathcal{F}$. To do this we will possibly enlarge $\mathcal{F}$ a little. We generate random numbers t and compute

$$D_1 + tD_2 \equiv D_3$$

where D_3 is an effective reduced divisor equivalent to $D_1 + tD_2$ in the divisor class group. If the support of D_3 consists of prime divisors of residue class degree one only, we enlarge the factor base, $\mathcal{F}$, by these divisors if necessary and store the relation between D_1, D_2 and $\mathcal{F}$ in a matrix. This step is carried out a number of times until we have a small set, ≈ 5, such relations between D_1, D_2 and the rest of $\mathcal{F}$.

We do not expect such a method to take too long since the degree of D_3 will be less than or equal to g. Suppose the x-coordinates in the support of the divisor D_3 over the algebraic closure act like the roots of a random polynomial of degree g with coefficients in F_q. Then we expect, with probability roughly $1/g$, that the x-coordinates are the roots of an irreducible polynomial of degree g. In such a situation the divisor D_3 will be prime and have residue class degree one. So, on average, we expect to try at most g such random values of t until we find a suitable D_3. One problem which arises is that the factor base will now include some 'large' primes. We shall see that this is not a problem later.

We now need to construct relations on the factor base. There are a number of relations which come for free, for example the decomposition of the ramified primes of $\mathbb{F}_q[x]$ gives relations, as does the decomposition of primes in $\mathbb{F}_q[x]$ of degree less than S_1 which split completely into prime divisors in K of residue class degree one.

The other relations we require are created using 'random' values of $a(x)$ and $b(x)$ of degree less than S_2 and then determining the prime divisors in the support of the function

$$\phi = a(x) + b(x)y.$$

If all such prime divisors lie in $\mathcal{F}$, which mainly depends on whether the polynomial N_ϕ has all its irreducible factors having degree less than S_1, we can store the relation and continue.

This last step can be speeded up using techniques from factoring algorithms such as lattice sieving, see [21] for details in the context of the current paper. Lattice sieving will allow us to hopefully force any rogue factor base element into a relation and hence using lattice sieving increases the chances of getting a relation matrix of full rank. Indeed it is using lattice sieving which allows us to deduce relations on the 'large' primes in the factor base which we produced above.

At this stage we meet with a problem, since the full relation lattice may not be generated by elements in the function field of the specific form

$$\phi = a(x) + b(x)y.$$

This could cause our algorithm to fail to terminate and leads to one of the reasons why our analysis below is only heuristic. However, in practice this can be overcome. We choose many elements $\theta \in K(C)$, whose minimal polynomial, $C_\theta(x, \theta)$ over $\mathbb{F}_q[x]$ is non-singular. Each such θ can be expressed as a polynomial in y and we can use the curve defined by $C_\theta(x, \theta)$ to find more relations of the form

$$a + b\theta.$$

One would expect that if enough such θ were chosen we would eventually cover the entire relation lattice. Another advantage of this approach is to provide an inherent parallelism for the computation. If the algorithm was to be distributed over a network of workstations each workstation could sieve with a different polynomial $C_\theta(x, \theta)$.

To simplify the complexity analysis below we shall, however, assume that $a(x)$ and $b(x)$ are random polynomials of degree less than or equal to S_2. Since factoring polynomials over finite fields (and hence factoring N_ϕ) can be accomplished in random polynomial time, see [3] and the discussion in [2], this is no theoretical barrier to our method.

We will need to produce a little over $\#\mathcal{F}$ such relations. However once this has been accomplished the discrete logarithm problem can be solved using standard matrix techniques. Given that our matrices will be sparse we can even apply sparse matrix techniques. Since this step is common to all index calculus methods we shall not explain it further here but see [5].

9.3. **The Overall Complexity.** We let $N_q(r, s)$ denote the number of monic polynomials of degree less than or equal to r over $\mathbb{F}_q$ which have all their irreducible factors of degree less than or equal to s. The complexity will depend heavily on the following result of Lovorn-Bender and Pomerance [14]

Theorem 18 (Lovorn-Bender and Pomerance). *Let $u = r/s$ and assume that $1 \leq s \leq r$. Then, uniformly for all prime powers such that $q \geq (r \log^2 r)^{1/s}$, we have*

$$N_q(r, s) = q^r / u^{(1+o(1))u}$$

as $s \to \infty$ and $u \to \infty$.

We use this to analyse the probability that a randomly chosen pair of polynomials, $a(x)$ and $b(x)$, of degree less than S_2 give rise to a relation as above. In our situation this is given by taking $r = \delta + nS_2$ and $s = S_1$ in the above theorem. Since $n = O(\delta)$ we see that

$$\frac{1}{s}(\log r + \log^3 r) \approx \frac{\log \delta}{a(\delta \log \delta)^{1/2}} = \left(\frac{2 \log q \log \delta}{\delta}\right)^{1/2}.$$

Hence the requirement that $q \geq (r \log^2 r)^{1/s}$ in our situation becomes, approximately,

$$\log q \geq \frac{2 \log \delta}{\delta}.$$

In such a situation the probability of attaining a relation is approximately given by

$$P = \left(\frac{S_1}{r}\right)^{(1+o(1))r/S_1}.$$

But we will need to generate roughly q^{S_1} relations so this will require approximately $T = q^{S_1}P^{-1}$ different random choices of $a(x)$ and $b(x)$. We notice that

$$\begin{aligned} \log T &\approx S_1 \log q + (1+o(1))\frac{\delta}{S_1}\log\frac{\delta}{S_1} \\ &\le a(\delta\log\delta)^{1/2}\log q + (1+o(1))\frac{(\delta\log\delta)^{1/2}}{2a} \\ &= (\delta\log\delta)^{1/2}\left(a\log q + \frac{1}{2a} + o(1)\right) \\ &= (\sqrt{2\log q} + o(1))(\delta\log\delta)^{1/2} \end{aligned}$$

To ensure we have enough random choices of $a(x)$ and $b(x)$ we will require that $q^{2S_2} > T$ which means that

$$2b(\delta\log\delta)^{1/2}\log q > \log T.$$

And so, approximately,

$$b > \frac{\sqrt{2\log q} + o(1)}{2\log q} \approx \frac{1}{\sqrt{2\log q}},$$

which certainly holds with the above choice of b. Since the time needed to factor the polynomials N_ϕ over $\mathbb{F}_q[x]$ can be discounted the complexity of determining enough relations is

$$O\left(L_{e^\delta}(1/2, \sqrt{2\log q} + o(1))\right).$$

All that remains is to estimate the time needed to perform the matrix step. If w denotes the number of rows of a matrix then we let k denote the exponent such that w^k is the roughly proportional to the time needed to perform the matrix step. Since our matrices are sparse we should be able to achieve $k = 2$, but for completeness we let k be variable.

Our matrix has roughly q^{S_1} rows and so the matrix step should take roughly q^{kS_1} steps, which is

$$O\left(L_{e^\delta}(1/2, kc_1)\right).$$

Hence our overall complexity estimate is

$$O\left(L_{e^\delta}(1/2, c)\right),$$

where c is given by

$$\max\left(\sqrt{2\log q} + o(1), k\sqrt{\frac{\log q}{2}}\right).$$

So if sparse matrix techniques are used and $k = 2$ we obtain $c = \sqrt{2\log q} + o(1)$.

References

[1] L. Adleman, J. De Marrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In *ANTS-1 : Algorithmic Number Theory*, L. Adleman and M.-D. Huang, editors. Springer-Verlag, LNCS 877, 1994.

[2] E. Bach and J. Shallit. *Algorithmic Number Theory. Volume 1 : Efficient Algorithms.* MIT Press, 1996.

[3] E.R. Berlekamp. Factoring polynomials over large finite fields. *Math. Comp.*, **24**, 713–715, 1970.

[4] J. Buchmann and S. Paulus. A one-way function based on ideal arithmetic in number fields. In *Advances in Cryptology, CRYPTO 97*, Editor B. Kaliski, Springer Verlag, LNCS 1294, 385–394, 1997.

[5] J. Buchmann, D. Squirrel and P. Theobald. Computing the HNF of sparse integer matrices. Preprint, 1998.

[6] D.G. Cantor. Computing in the Jacobian of a hyper-elliptic curve. *Math. Comp.*, Vol 48, 95–101, 1987.

[7] J. Coates. Construction of rational functions on a curve. *Proc. Cam. Phil. Soc.*, Vol. 68, 105–123, 1970.

[8] H. Cohen. *A Course In Computational Algebraic Number Theory.* Springer-Verlag, GTM 138, 1993.

[9] R. Flassenberg and S. Paulus. Sieving in function fields. *Preprint*, 1997.

[10] G. Frey and H.-G. Rück. A remark concerning m-divisibility and the discrete logarithm problem in the divisor class group of curves. *Math. Comp.*, **62**, 865-874, 1994.

[11] A. Frölich and M. J. Taylor. *Algebraic number theory.* Cambridge studies in advanced mathematics 27, Cambridge 1991.

[12] W. Fulton. *Algebraic curves.* Benjamin (1969)

[13] M.-D. Huang, D. Ieradi. Efficient algorithms for the Riemann-Roch problem and for addition in the jacobian of a curve. *J. Symbolic Comp.*, Vol. 18, 519–539, 1994.

[14] R. Lovorn Bender and C. Pomerance. Rigourous discrete logarithm computations in finite fields via smooth polynomials. In *Computational Perspectives on Number Theory. Proc. of a Conference in honor of A.O.L. Atkin* Vol 7 of AMS/International Press Studies in Advanced Mathematics, Providence 1998.

[15] K. Mahler. *An analogue to Minkowski's geometry of numbers in a field of series.* Ann. Math. **42** No. 2. 1941. pp. 488 – 522.

[16] V. Müller, A. Stein and C. Thiel. Computing discrete logarithms in real quadratic function fields of large genus. Preprint 1997.

[17] S. Paulus. An algorithm of sub-exponential type computing the class group of quadratic orders over principal ideal domains. In *ANTS-2 : Algorithmic Number Theory*, H. Cohen, editor. Springer-Verlag, LNCS 1122, pp 243–257, 1996.

[18] S. Paulus. Lattice basis reduction in function fields. In *ANTS-3 : Algorithmic Number Theory*, J. Buhler, editor. Springer-Verlag, LNCS 1423, pp 567–575, 1998.

[19] S. Paulus, H.-G. Rück. Real and imaginary quadratic representations of hyperelliptic function fields. *To appear in Math. Comp.*

[20] M. Pohst, M. Schörning. *On integral bsis reduction in global function fields.* In *ANTS-2 : Algorithmic Number Theory*, H. Cohen, editor. Springer-Verlag, LNCS 1122, pp 273–283, 1996.

[21] N.P. Smart. Experiments using an analogue of the Number Field Sieve algorithm to solve the discrete logarithm problem in the Jacobians of hyperelliptic curves. *HP-Labs Technical Report*, HPL-97-130, 1997.

[22] H. Stichtenoth. *Algebraic function fields and codes.* Springer Universitext, Springer, 1993.

[23] E. J. Volcheck. Computing in the Jacobian of a plane algebraic curve. In *ANTS-1 : Algorithmic Number Theory*, L. Adleman and M.-D. Huang, editors. Springer-Verlag, LNCS 877, pp 221–233, 1994.

[24] R. J. Walker. *Algebraic curves.* New York: Springer 1978.

Mathematics Department, Royal Holloway University of London, Egham, Surrey TW20 0EX, U.K.

E-mail address: stevenga@dcs.rhbnc.ac.uk

Technische Universitt Darmstadt, Fachbereich 20 - Informatik Alexanderstr. 10, 64283 Darmstadt, Germany.
E-mail address: sachar@cdc.informatik.th-darmstadt.de

Hewlett-Packard Laboratories,Filton Road, Stoke Gifford, Bristol, BS12 6QZ, U.K.
E-mail address: nsma@hplb.hpl.hp.com