A New Method for Computing the Inverse Ideal in a Coordinate Ring

Abdolali Basiri

Abstract—In this paper we present an efficient method for inverting an ideal in the ideal class group of a C_{ab} curve by extending the method which is presented in [3]. More precisely we introduce a useful generator for the inverse ideal as a $K[X]$-module.

Keywords—C_{ab} Curves, Ideal Class Group.

I. INTRODUCTION

THE first ideal class groups encountered in mathematics were part of the theory of quadratic forms: in the case of binary integral quadratic forms, as put into something like a final form by Gauss, a composition law was defined on certain equivalence classes of forms. This gave a finite abelian group, as was recognized at the time. Later Kummer was working towards a theory of cyclotomic fields. It had been realised (probably by several people) that failure to complete proofs in the general case of Fermat's last theorem by factorization using the roots of unity was for a very good reason: a failure of the fundamental theorem of arithmetic to hold, in the rings generated by those roots of unity, was a major obstacle. Out of Kummer's work for the first time came a study of the obstruction to the factorization. We now recognize this as part of the ideal class group: in fact Kummer had isolated the p-torsion in that group for the field of p-roots of unity, for any prime number p, as the reason for the failure of the standard method of attack on the Fermat problem (see regular prime). Somewhat later again Dedekind formulated the concept of ideal, Kummer having worked in a different way. At this point the existing examples could be unified. It was shown that while rings of algebraic integers do not always have unique factorization into primes (because they need not be principal ideal domains), they do have the property that every proper ideal admits a unique factorization as a product of prime ideals (that is, every ring of algebraic integers is a Dedekind domain). The ideal class group gives some answer to the question: which ideals are principal ideals? The answer comes in the form all of them, if and only if the ideal class group (which is a finite group) has just one element. Nowadays, an application of ideal class group is in cryptography. The success of elliptic curves in public key cryptography has created new interest in the arithmetic of more general algebraic curves such as hyperelliptic, superelliptic [4], C_{ab} [1] or C_A [2] curves. Unfortunately there is a heavy computational amount of addition in the Jacobian of such non-elliptic curves. The core of their arithmetic often consists of the reduction process, which is: transforming any group element into a reduced representative. But to compute such a reduced

School of Mathematics and Computer Science, Damghan University of Basic Sciences, Damghan, Iran, email: basiri@dubs.ac.ir

ideal, we need first to compute an inverse for the present ideal. In this paper, we give a useful generator as a $K[X]$-module for the inverse ideal of a typical ideal [3].

II. DEFINITIONS AND NOTATIONS

We begin with a basic definition and some notations.

Definition 1: For coprime positive integers a and b, coprime to the characteristic of the ground field K, a C_{ab} curve ([5], [6]) C is defined by a non-singular plan curve defined by the following form of polynomial F

$$F(X,Y) = Y^a + \sum_{ia+jb<ab} c_{ij}X^iY^j + X^b.$$

Let $K[F] = K[X,Y]/\langle F \rangle$ be a *coordinate ring* of a C_{ab} curve C which is defined by F and $K(F)$ be its *function field* (the field of fractions of $K[F]$). We will use three different representations of ideals:

- The notation $\mathrm{id}(f_1(X,Y),\cdots,f_m(X,Y))$ will represent the ideal
  $\{f_1(X,Y)g_1(X,Y) + \cdots + f_m(X,Y)g_m(X,Y) :$
  $g_1(X,Y),\cdots,g_m(X,Y) \in K[F]\}$.
- The notation $[f_1(X,Y),\cdots,f_m(X,Y)]_{K[X]}$ will represent the $K[X]$ module
  $\{f_1(X,Y)g_1(X) + \cdots + f_m(X,Y)g_m(X) :$
  $g_1(X),\cdots,g_m(X) \in K[X]\}$.
  Every ideal may be written in this form. However, it is not true that every such module is an ideal.
- The notation $[I : J]$ will represent the ideal
  $\{h \in R : hg \in I \quad \forall g \in J\}$
  where R is a ring and I and J two ideals of R. Specially $[f : J]$ denotes $[\mathrm{id}(f) : J]$ for every f in R.

III. MAIN THEOREM

We begin this section with two lemma and end it with the main theorem of this paper.

Lemma 2: Let $F(X,Y)$ be a monic polynomial w.r.t Y in $K[X,Y]$ and $v(X)$ a polynomial in $K[X]$, then $Y - v$ divides $F(X,Y) - F(X,v)$.

Proof: There are $F_0,\cdots,F_{a-1}$ in $K[X]$ such that

$$F(X,Y) \quad = \quad Y^a + \sum_{j=0}^{a-1} F_j(X)Y^j. \qquad (1)$$

Set

$$H = \sum_{j=0}^{a-1} Y^{a-1-j}v^j + \sum_{l=1}^{a-1} F_l \sum_{k=0}^{l-1} Y^{l-1-k}v^k,$$

World Academy of Science, Engineering and Technology
International Journal of Mathematical and Computational Sciences
Vol:1, No:11, 2007

we have then:

$$H(Y - v) = (Y^a - v^a) + \sum_{j=1}^{a-1} F_j(Y^j - v^j)$$

which is equal to $F(X, Y) - F(X, v)$. ∎

With above notations, H can be written as:

$$H = \sum_{i=0}^{a-1}(v^{a-1-i} + \sum_{k=i}^{a-2} F_{k+1}v^{k-i})Y^i. \qquad (2)$$

A generator set for the ideal $[u : \mathfrak{A}] \mod F$, can be computed as follows:

Lemma 3: Let $\mathfrak{A} = \mathrm{id}(u(X), Y - v(X))$ be a typical ideal, F a polynomial of the form (1) in $\mathfrak{A}$ and u divide $F(X, v)$, then

$[u : \mathfrak{A}] = \mathrm{id}(u, H) \mod F$.

Proof: There is a polynomial $w \in K[X]$ such that

$$F(X, v) = wu. \qquad (3)$$

Define

$\mathfrak{B} := [u : \mathfrak{A}] \mod F$

then

$$\mathfrak{B} = \{\mu \in K[X, Y] \mid \mu(Y - v) \in \mathrm{id}(u) \mod F\}. \qquad (4)$$

But by Lemma 2 and equation (3) we have

$$H(Y - v) = -wu \in \mathrm{id}(u) \mod F,$$

hence

$$\mathrm{id}(u, H) \subseteq \mathfrak{B} \mod F.$$

Now we show

$$\mathfrak{B} \subseteq \mathrm{id}(u, H) \mod F.$$

For this purpose let $\theta \in \mathfrak{B}$, it suffices to treat the special case:

$$\theta = \sum_{j=0}^{a-1} \theta_j Y^j, \qquad (5)$$

for some $\theta_0, ..., \theta_{a-1}$ in $K[X]$, because from equation (1) we have $Y^a + \mathfrak{B} = (\sum_{j=0}^{a-1} F_j Y^j) + \mathfrak{B}$. By equation (4),

$$\theta(Y - v) \in \mathrm{id}(u) \mod F.$$

There are so $\eta_{a-1}, ..., \eta_0, s \in K[X]$ such that

$$\theta(Y - v) = (\sum_{j=0}^{a-1} \eta_j Y^j)u + sF.$$

So from the equations (1) and (5) we have
$\theta_{a-1} Y^a + \sum_{j=1}^{a-1}(\theta_{j-1} - v\theta_j)Y^j - v\theta_0 =$
$sY^a + \sum_{j=1}^{a-1}(u\eta_j + sF_j)Y^j + u\eta_0 + sF_0$.

We have then $\theta_{a-1} = s$ and for $0 \le j \le a - 2$,

$$\begin{aligned}
\theta_j &= v\theta_{j+1} + u\eta_{j+1} + sF_{j+1} \\
&= (v^{a-j-1} + \sum_{l=j+1}^{a-1} v^{l-j-1}F_l)s \\
&\quad + (\sum_{l=j+1}^{a-1} v^{l-j-1}\eta_l)u
\end{aligned}$$

The later equations with (5) and (2) imply that:

$$\begin{aligned}
\theta &= s(H - \sum_{i=0}^{a-2}(v^{a-1-i} + \sum_{k=i}^{a-2} F_{k+1}v^{k-i})Y^i) \\
&\quad + \sum_{j=0}^{a-2}((v^{a-j-1} + \sum_{l=j+1}^{a-1} v^{l-j-1}F_l)s \\
&\quad + (\sum_{l=j+1}^{a-1} v^{l-j-1}\eta_l)u)Y^j \\
&= sH - s\sum_{j=0}^{a-2}(v^{a-1-j} + \sum_{l=j}^{a-2} F_{l+1}v^{l-j})Y^j \\
&\quad + \sum_{j=0}^{a-2}(v^{a-j-1} + \sum_{l=j}^{a-2} v^{l-j}F_{l+1})sY^j \\
&\quad + \sum_{j=0}^{a-2}\sum_{l=j+1}^{a-1} v^{l-j-1}\eta_l uY^j \\
&= sH + (\sum_{j=0}^{a-2}\sum_{l=j+1}^{a-1} v^{l-j-1}\eta_l Y^j)u,
\end{aligned}$$

which is an element of the ideal $\mathrm{id}(u, H) \mod F$, consequently

$$\mathfrak{B} = \mathrm{id}(u, H) \mod F.$$

∎

We now have all the ingredients needs to state and prove the main theorem which computes a generator set for the ideal

$$[u : \mathfrak{A}] \mod F,$$

as a $K[X]$-module.

Theorem 4: Let $\mathfrak{A} = \mathrm{id}(u(X), Y - v(X))$ be a typical ideal, F a polynomial of the form 1 in $\mathfrak{A}$, u divide $F(X, v)$ and $\mathfrak{B} = [u : \mathfrak{A}] \mod F$, then

$$\mathfrak{B} = [u, uY, ..., uY^{a-2}, H]_{K[X]} \mod F, \qquad (6)$$

i.e.,

$$\mathfrak{B} = \{\lambda F + \sum_{i=0}^{a-2} \theta_i uY^i + \theta_{a-1} H \mid \lambda \in K[X, Y], \ \theta_i \in K[X]\}.$$

Proof: Let

$$\mathfrak{C} := [u, uY, ..., uY^{a-2}, H] \mod F,$$

by Lemma 2 and equation (3) we have $YH = F - uw + vH$ which is an element of $\mathfrak{C}$, also

$$Y^2 H = YF + v(F + vH - uw) - wuY \in \mathfrak{C},$$

and by the same reason $Y^i H \in \mathfrak{C}$ for $i = 1, ..., a - 1$. Now from equation (1) for all $i \ge a$, there are $H_{i_0}, H_{i_1}, ..., H_{i_{a-1}} \in K[X]$ and $H_i \in K[X, Y]$ such that

$$Y^i = H_i F + \sum_{j=0}^{a-1} H_{i_j} Y^j \qquad (7)$$

hence $Y^i H = (H_i F + \sum_{j=0}^{a-1} H_{i_j} Y^j)H \in \mathfrak{C}$. On the other hand by equation 2 we have

$$
\begin{aligned}
Y^{a-1}u &= (H - \sum_{i=0}^{a-2}(v^{a-1-i} + \sum_{k=i}^{a-2} F_{k+1}v^{k-i})Y^i)u \\
&= uH - \sum_{i=0}^{a-2}(v^{a-1-i} + \sum_{k=i}^{a-2} F_{k+1}v^{k-i})uY^i,
\end{aligned}
$$

belongs to $\mathfrak{C}$. Also by equation (7), for all $i \geq a$ we result that $Y^i u = (H_i F + \sum_{j=0}^{a-1} H_{i_j} Y^j)u$ belongs to $\mathfrak{C}$. Consequently $\mathfrak{B} \subseteq \mathfrak{C}$, moreover, by the lemma 3 it is clear that $\mathfrak{C} \subseteq \mathfrak{B}$, and thus $\mathfrak{B} = \mathfrak{C}$. ∎

IV. AN EXAMPLE

In this section we give an example to explain how our theorem work.

Let C be a C_{35} curve in $\mathbb{Z}_{97}[x, y]$, defined by $F = y^3 + F_1 y + F_0$ where

$$F_0 = 24 + 89\,x + 51\,x^2 + 96\,x^3 + x^5, \quad F_1 = 62\,x^3 + 88\,x^2 + 27\,x + 26.$$

Consider the ideal $\mathfrak{A} = (u, y - v)$ where

$$u = 19 + 56\,x + 23\,x^3 + 24\,x^2 + 92\,x^5 + 3\,x^4 + x^8 + 87\,x^7 + 33\,x^6,$$

$$v = 28\,x^7 + 13\,x^6 + 86\,x^5 + 12\,x^4 + 25\,x^3 + 57\,x^2 + 27\,x + 53.$$

By applying explained procedure in previous section we can obtain that inverse ideal of $\mathfrak{A}$ modulo F is equal to:

$$\mathrm{id}(u, H) = [u, uy, H],$$

where
$H = y^2 + yH_1 + H_0,$
$H_1 = 28\,x^7 + 13\,x^6 + 86\,x^5 + 12\,x^4 + 25\,x^3 + 57\,x^2 + 27\,x + 53,$
$H_0 = 22 + 76\,x + 87\,x^{10} + 38\,x^{12} + 95\,x^{11} + 86\,x^9 + 51\,x^4 + 67\,x^3 + 69\,x^2 + 4\,x^5$
$+ 61\,x^6 + 49\,x^{13} + 66\,x^8 + 9\,x^7 + 8\,x^{14}.$

V. CONCLUSION

We presented an efficient method for inverting an ideal in the ideal class group of a C_{ab} curve which can be applied in cases of hyperelliptic and superelliptic curves and also can be used for computing the addition in the Jacobian of such non-elliptic curves.

ACKNOWLEDGMENT

REFERENCES

[1] S. Arita. Algorithms for computations in Jacobian group of C_{ab} curve and their application to discrete-log based public key cryptosystems. *IEICE Transactions*, J82-A(8):1291–1299, 1999. In Japanese. English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999.
[2] S. Arita, S. Miura, and T. Sekiguchi. An addition algorithm on the jacobian varieties of curves. *Journal of the Ramanujan Mathematical Society*, 19(4):235–251, December 2004.
[3] A. Basiri, A. Enge, J.-C. Faugère, and N. Gürel. The arithmetic of jacobian groups of superelliptic cubics. *Math. Comp.*, 74:389–410, 2005.
[4] S.-D. Galbraith, S. Paulus, and N.-P. Smart. Arithmetic on superelliptic curves. *Mathematics of Computation*, 71(237):393–405, 2002.
[5] S. Miura. Linear codes on affine algebraic curves. *IEICE Transactions*, J81-A:1398–1421, 1998. In Japanese. English summary by Ryutaroh Matsumoto available at *http://www.rmatsumoto.org/cab.html*.
[6] S. Miura and N. Kamiya. Geometric goppa codes on some maxima curves and their minimum distance. In *IEEE Worksop on Information Theory*, pages 85–86, Susono-shi, Japan, June 1993.
[7] Wikipedia encyclopedia. http://en.wikipedia.org/wiki/Mathematics

Abdolali Basiri is Assistant Professor at School of Mathematics and Computer Science, Damghan University of Basic Sciences, 3671641167, Damghan, Iran (phone/fax: +98 232 523 5316; e-mail: basiri@dubs.ac.ir).