International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373/doi:10.14445/22315373/IJMTT-V67I10P506
Volume 67 Issue 10, 67-71, October, 2021

Original Article

Some Results For Computation Theory In Hyperelliptic Curves Type

Tran Duy Hung[1], Dao Viet Cuong[2], Ngo Tien Hung[3] and Pham Tien Huy[4]

[1]*Faculty of Information Technology, Hanoi Open University, Nguyen Hien St, Hai Ba Trung, Hanoi, Vietnam*
[2]*Faculty of Basic Sciences,University of Transport and Communications, Cau Giay St, Hanoi, Vietnam*
[3]*High School for Gifted Students, Ha Noi National University of Education, Hanoi, Vietnam*
[4]*Faculty of Electronic Telecommunication and Information Technology, Hanoi Open University, Nguyen Hien St, Hai Ba Trung, Hanoi, Vietnam*

Abstract *- In this paper we consider a reduction algorithm and computation in the Jacobian of a hyperelliptic curve type as forms* $y^2 = P_n(x), n \geq 3$*, which is generalized of a usual elliptic curve.*

Keywords *- Cryptosystems, Elliptic curve, Hyperelliptic curve type.*

I. INTRODUCTION

So far in a finite abelian goup, the discrete logarithm problem (DLP) is finding the integer that was multiplied by the base to get the element. Whenever we have a finite abelian group for which the DLP appears to be intractable, we can construct various public key cryptosystem in which taking large multiples of a group element is the trap-door function. Such cryptosystems were first constructured from the multiplicative group of a finite field. However, because certain special techniques are available for attacking the discrete log problem in that case it is worth while to study other sources of finite abelian groups. A number of improvements have since occoured, and new algorithms using the class group have appeared.
More recently, one has shown how tho use the group of points on an elliptic curve, defined over a finite field, in a factorization algorithms. Elliptic curves can be equipped with an efficiently computable group law, so that they are suited for implementing the cryptographic schemes as suggested first in Koblitz, Miller and Enge [1,2,6,7]. They are particularly appealing because they achieve the same level of security as a finite field based cryptosystem with much shorter key lengths, which results in a faster encryption and decryption process. For the elliptic curve discrete logarithm problem, there are some particular cases where a solution can be found with a complexity better than $O(\sqrt{n})$ [2],[3]. Similar cases were discovered for hyperelliptic curves [4]. However they are very particular and can be easily avoided when designing a cryptosystem.
The use of hyperelliptic curves in public-key cryptography was first proposed by Koblitz in 1989 [4]. It appears as an alternative to the use of elliptic curves [5], with the advantage that it uses a smaller base field for the same level of security. Several authors have given ways to build hyperelliptic cryptosystems efficiently. The security of such systems relies on the difficulty of solving the discrete logarithm problem in the Jacobian of hyperelliptic curves.
The purpose of the present article is to discuss similarly situation about hyperelliptic curves type which has form

$$y^2 = P_n(x),$$

where $P_n(x)$ is a polynomial of degree $n \geq 3$, $n \in \mathbb{N}$. Elliptic curves are the special case of the hyperelliptic curves type. So we specialise all results to the case of hyperelliptic type curves, where many of them can be proved by explicit computations or more elementary arguments than in the general case. In particular, our reduction procedure will use the Euclidean algorithm and be faster than the classical reduction procedure due to Gauss. A modification of it can be used for computation in the class group of an algebraic nuber field.

II. BASIC DEFINITIONS AND KNOWLEDGE

A. Discriminant of quadratic forms

Let n be an odd natural number. Without generality, we assume $n = -1 \, mod \, 4$. Let $\boldsymbol{QF_{-n}}$ be the set of positive binary integer primitive quadratic forms $aX^2 + bXY + cY^2$, $a, b, c \in \mathbb{Z}$, $a > 0$ and which are pairs of primes togetger with discriminant $b^2 - 4ac$. Note that, $\boldsymbol{QF_{-n}}$ is nonempty if and only if $n = 0$ or $n = -1 \, mod \, 4$.
Two forms (a, b, c) and (a', b', c') are called equivalent if and only if there is a 2×2-matrix $A \in SL_2(\mathbb{Z})$ with determinant 1 such that

$$\begin{pmatrix} \frac{b'}{2} & c' \\ a' & \frac{b'}{2} \end{pmatrix} = A^T \begin{pmatrix} \frac{b}{2} & c \\ a & \frac{b}{2} \end{pmatrix} A \, . \qquad (2.1)$$

For $f \in \boldsymbol{QF_{-n}}$ let $[f]$ be its $SL_2(\mathbb{Z})$-equivalence class and let C_{-n} be the set of equivalence classes in $\boldsymbol{QF_{-n}}$. C_{-n} is a finite abelian group with respect to an operation called "composition" defined as follows (see [3])

$$[(a_1, b_1, c_1)].[(a_2, b_2, c_2)] = [(a_3, b_3, c_3)],$$

where

$$a_3 = \frac{a_1 a_2}{d^2}\ ;\ b_3 = b_2 + 2.\frac{a_2}{d}.R\ ;\ c_3 = \frac{b_3^2 + n}{4a_3}$$

with d, R such that

$$d = \lambda a_2 + \mu a_1 + \nu\frac{b_1 + b_2}{2}$$
$$R = \lambda.\frac{b_1 - b_2}{2} - \nu c_2$$
$$\lambda, \mu, \nu \in \mathbb{Z}.$$

The group C_{-n} is called the class group, its cardinality h_{-n} is called the class number of the discriminant $-n$.

B. Field characteristic

Let K is a field with the unit element e, if for some $n > 0$ we have

$$\underbrace{e + e + \cdots + e}_{n\ times} = ne = 0,$$

then the smallest such n is a prime number, it is called the characteristic of K. If there are no such number n, then one says that characteristic of K is 0. For instance, the fields $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers) has characteristic 0, for p a prime, the finite field $GF(p^n)$ has characteristic p. If H is a subfield of K, then H and K have the same characteristic.

C. The groups

Let K be an arbitrary field of characteristic $\neq 2$, and let $\overline{K}$ denote its algebraic closure. We define a hyperelliptic curve type C of genus n over K to be an equation of the form

$$v^2 = f(u), \tag{2.2}$$

where $f(u)$ is a polynomial of degree $n \geq 3, n \in \mathbb{N}$, with all roots distinct and with coefficients in K. We require that the curve have no singular points (u, v), i.e., in the Weierstrass equation form, its discriminant is zero (see [1]).

Let F be a set containing K. By an F-point $P \in C$, we mean either the symbol ∞ or else a solution $u = x \in F$, $v = y \in F$ of the equation (2.2), and the solution of (2.2) is called a "finite" point and is denoted by $P_{x,y}$. If σ is an automorphism of F over K, we let P^σ denote $P_{\sigma(x),\sigma(y)}$ and set $\infty^\sigma = \infty$.

We define a divisor is a finite form in $\overline{K}$ as follows

$$D = \sum_i m_i P_i$$

and the degree of D is $\sum_i m_i$.

Since $v^2 = f(u)$ on the curve C, consider a polynomial $p = p(u, v)$ in the form

$$p = a_0 + a_1 v + a_2 v^2 + \cdots + a_k v^k + \cdots$$

we have

$$v^2 = f(u),$$
$$v^3 = v.v^2 = v.f(u),$$
$$v^4 = v^2.v^2 = f^2(u), \ldots$$

Therefore, any polynomial $p = p(u, v)$ when consider as a function on C, can be written in the following form

$$p = a + bv, \tag{2.3}$$

where $a = a(u)$ and $b = b(u)$ are polynomials respect to variable u.

From (2.3), if $a + bv = 0$, then $v = -\frac{a}{b}$ and $v^2 = f = \frac{a^2}{b^2}$, this leads $a^2 - b^2 f = 0$. Therefore, if p vanishes at the point (x, y) (this implies $y^2 = f(x)$), then the order of the zero of p is the exponent of the highest power of $(u - x)$ which devides $a^2 - b^2 f$.

Suppose now $p = p(u, v)$ and $q = q(u, v)$ are polynomials in $K[u, v]$ such that $q(u, v)$ is not divisible by $v^2 - f(u)$. Then $h = \frac{p}{q}$ can defined on C, and the function h has a finite number of zeros and poles on C. From Laurent series expansion for the function h, we can associate h with its divisor $(h) = \sum_i m_i P_i$, where P_i are zeros and poles of h on C with coefficients m_i (m_i are possitves if P_i of h and negative if it is a pole). A divisor of a nozero function, such as (h) is called principal, a principal divisor has degree 0. The divisors form an additive group D under additive form

$$\sum_i m_i P_i + \sum_i n_i P_i = \sum_i (m_i + n_i) P_i$$

and the divisors of degree 0 form is a subgroup denoted by D_0.

We define $GCD(\sum_i m_i P_i, \sum_i n_i P_i)$ to be $\sum_i \min(m_i, n_i)P_i$. The principal divisors form a subgroup P of D_0 and Jacobian of C is defined by the quotient group $Jaco(C) = D_0/P$. If D_1 and D_2 are principal divisors and D_1 is equivalent to D_2 in $Jaco(C)$, then we write $D_1 = D_2(mod\ P)$ or $D_1 \sim D_2$, that means $D_1 - D_2 \in P$.
Given a finite point $P = P(x, y) \in C$, we define its "opposite" $\tilde{P}$ to be $\tilde{P} = (x, -y)$. If $P = \infty$ then we define $\tilde{P} = \infty$. If $P = P(x, y)$ is a point on the curve C, then we have $P - \infty = -(\tilde{P} - \infty)$, therefore, the point P and $\tilde{P}$ are zeros of the function $(u - x)$, which has a double pole at ∞. Thus the divisor $P + \tilde{P} - 2.\infty \equiv 0(mod\ P)$ or $\tilde{P} \equiv P - 2.\infty(mod\ P)$. It follows that each element of $Jaco(C)$ can be presented in the form

$$D = \sum_{i=1}^{r} P_i - r.\infty,$$

where $r = \sum_i m_i$ and if $P_i = (x_i, y_i)$ appears in D, then $\tilde{P}_i = (x_i, -y_i)$ does not appear as one of the P_j $(j \neq i)$. This implies, in particular, that points of the form $(x, 0)$ appear at most once in D, we call such a divisor semireduced. From the Riemann-Roch theorem [Lang], it follows that, each element of $Jaco(C)$ can be presented uniquely by such a divisor with restriction $r \leq n$. Such divisors to be called reduced. Any semereduced divisor D can be represented uniquely by a pair of polynomials $(a(u), b(u))$ satisfying $D = GCD((a), (b - v))$, where $a = a(u) = \prod(u - x_i)^{m_i}$ and $b = b(u)$ is the unique polynomial of degree less than $\deg(a)$ satisfying $b(x_i) = y_i, (1 \leq i \leq r)$ with appropriate multiplicity when the point P_i appears more than once in D. In the case P_i appears k times in D, $(b - y_i)$ must be divisible by $(u - x_i)^k$. This implies that $(b^2 - f)$ be divisible by a. We denote this divisor D by $\text{div}(a, b)$. Note that D is reduced if and only if $\deg(a) \leq n$. If we define $c = \frac{b^2 - f}{a}$, then the presentation (a, b, c) of D is analogous to the similar presentation of the quadratic form $aX^2 + 2bXY + cY^2$ with discriminant f.
If a and b have coefficients in K, we say that the divisor D rational over K. If K is compact, then D will be rational over K if and only if $D = D^\sigma$ for all automorphism σ of $\overline{K}$ over K.
In trivial case, if $n = 3$, then a is a linear polynomial $(u - x)$ and b is a constant y, in this case, $Jaco(C)$ is isomorphic to C, and the reduced divisor (a, b), considered as an element of $Jaco(C)$, corresponds to the point (x, y) on C (which is an elliptic curve). Hence, we will not distinguish between an element of $Jaco(C)$ and its reduced representative $\text{div}(a, b)$. In the case, to add two elements D_1=$\text{div}(a_1, b_1)$ and D_2=$\text{div}(a_2, b_2)$ of $Jaco(C)$, we consider as in the classical composition quadratic forms.

III. OVERVIEW OF THE ALGORITHM AND VERIFY ITS CORRECTNESS

Let K be a field with characteristic not equal to 2. From the Euclidean algorithm, we see that, if a, b and c are three polynomials in a variable u, then the notation $b = c(mod\ a)$ means that b equal to the residue of c modulo a, i.e., it is the unique polynomial b of degree $< \deg(a)$ such that a divides $(c - b)$.
The algorithm for adding divisors $D \in Jaco(C)$ consists of two steps. Given $D_1 = \text{div}(a_1, b_1)$ and $D_2 = \text{div}(a_2, b_2)$, we first find a semireduced divisor $D = \text{div}(a, b)$ such that $D \sim D_1 + D_2$. Next, we reduced D, that means, we find polynomials $a'(u)$ and $b'(u)$ such that $\deg(a') \leq n \text{ div } 2$, $\deg(b') \leq \deg(a')$, and $D \sim \text{div}(a', b')$. Thus we want to find the sum of $\text{div}(a_1, b_1)$ and $\text{div}(a_2, b_2)$ on $Jaco(C)$, (i.e., which satisfy $v^2 = f(u)$), where a_1, a_2, b_1, b_2 and f are all polynomial in u. Here, f has coefficients in K, and a_1, a_2, b_1, b_2 have coefficients in $\overline{K}$.
Step 1. Let $d = d(u)$ be the $GCD(a_1(u), a_2(u), b_1(u) + b_2(u))$ and choose $s_1(u), s_2(u)$ and $s_3(u)$ to be polynomials in u such that

$$d = s_1 a_1 + s_2 a_2 + s_3(b_1 + b_2). \tag{2.4}$$

Set

$$a = \frac{a_1 a_2}{d^2}$$

and

$$b = \frac{s_1 a_1 b_2 + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d}\ (mod\ a). \tag{2.5}$$

We have $\deg(b) < \deg(a)$, and $\text{div}(a, b)$ is semireduced.
We now verify correctness for (2.5). As usual, consider a polynomial $c = c(u)$ in variable u, we denote $ord_x(u)$ the largest integer r for which $(u - x)^r$ divides c. From (2.4), w have

$$b = \frac{b_2(d - s_2 a_2 - s_3(b_1 + b_2)) + s_2 a_2 b_1 + s_3(b_1 b_2 + f)}{d}.$$

This leads

$$b = b_2 + \frac{s_2 a_2 (b_1 - b_2)}{d} + \frac{s_3(f - b_2^2)}{d}. \tag{2.6}$$

Since $f - b_2^2 \equiv 0\ (mod\ a_2)$, the division in (2.4) is exact, so that b is a polynomial. We can multiply (2.6) by $(b_1 + b_2)$ and simplify to obtain

$$(b_1 + b_2)b = b_1 b_2 + f + \frac{s_1 a_1 (b_2^2 - f) + s_2 a_2 (b_1^2 - f)}{d}$$

or

$$\frac{b_1+b_2}{b-v}=(b_1-v)(b_2-v)+\frac{s_1a_1(b_2^2-f)+s_2a_2(b_1^2-f)}{d}.$$

There are following cases:

Case A. Suppose that the point $P=(x,y)$ has multiplicity $r_s\geq 0$ in D_s ; $s=1,2$, and if $y\neq 0$, then $\tilde{P}=(x,-y)$ does not occur in either, and we have

(i) $ord_x(a)=\begin{cases} r=r_1+r_2 & \text{if } y\neq 0\\ (r_1+r_2)(mod\ 2) & \text{if } y=0,\end{cases}$

(ii) $ord_x(b-y)\geq r$.

Case B. Suppose that $P=(x,y)$ has multiplicity $r_1>0$ in D_1 and $\tilde{P}=(x,-y)$ has multiplicity $r_2>0$ in D_2. Put $r=|r_1-r_2|$, we have

(i) $ord_x(a)=r$,

(ii) If $r_1\geq r_2$, then $ord_x(b-y)\geq r$ and $r_1\leq r_2$, then $ord_x(b+y)\geq r$.

In the case $r_1\leq r_2$, we have $ord_x(b_2-y)\geq r_2$, $ord_x(s_2a_2(b_1-b_2))=r_2$ and $ord_x(s_3(f-b_2^2)/d)\geq r_2-r_1$. Hence using (2.6), $ord_x(b-y)\geq r$.

(See more detail in [2])

Specical case, if a_1 and a_2 have no common factor, then $d=1$, we can take $s_3=0$, and so $a=a_1a_2$, $b=(s_1a_1b_2+s_2a_2b_1)(mod\ a)$.

Step 2. Given $D=\text{div}(a,b)$ with $\deg(a)>n$ div 2 (i.e., 5 div 2 = 2), the following procedure repalces D by $D'=\text{div}(a',b')$, where $\deg(a')<\deg(a)$. By successively applying the procedure, we obtain $D''=\text{div}(a'',b'')$ where $D\sim D''$ and $\deg(a'')\leq n$ div 2.

We set

$$a'=\frac{f-b^2}{a} \tag{2.7}$$

and then

$$b'=-b(mod\ a') \tag{2.8}$$

It is not difficult to show that $\text{div}(a',b')\sim\text{div}(a,b)$ and $\deg(a')<\deg(a)$. This concludes the description of the algorithm.

Remarks

(i) In the case $n=3$ (elliptic curves), the reduced divisors $D=\text{div}(u-x,y)$ are one-to-one correspondence with the point $P_{x,y}\in C$. The above algorithm is then easily seen to reduce to the usual formulas for the addition of points on an elliptics curve.

(ii) If classical algorithm are used, then the computation of the product of two polynomials of degree m and the computation of their GCD each take $O(m^2)$ field operations, while if the above algorithm is used, then the computation of their product takes $O(m\log m)$ operations and the computation of their GCD takes $O(m(\log m)^2)$ operations. It follows that the computation algorithm takes $O(n(\log n)^2)$ operations.

IV. CRYPTOSYSTEMS

Let K be a perfect field, and let L be an algebraic field extension of K. We let $Jaco(L)$ denote the set of L-points of $Jaco(C)$, i.e., the divisors D such that $D^\sigma=D$ for all automorphisms σ of $\bar{K}$ over L. Since this invariance propertiy is preserved under addition, $Jaco(L)$ is a subgroup of $Jaco(C)$. And then, an L-points of $Jaco(C)$ is simply an element $\text{div}(a,b)$ for which the polynomials a and b have coefficients in L.

We assume that $K=F_q$ is a finite field with q elements, we can see that the abelian group $Jaco(L)$ is finite for any extension $=F_{q^s}$.

The discrete logarithm problem on $Jaco(F_{q^s})$ is the problem: Given two divisors D_1 and D_2 defined over F_{q^s}, of determing an integer $m\in\mathbb{Z}$ such that $D_2\sim mD_1$ if such m exists.

According to the Diffie-Hellman phenomenon in [Hellman], this key change in the context of $Jaco(F_{q^s})$ works as follows: The finite F_{q^s} and the equation of C are publicly known, as is a fixed element $D_0\in Jaco(F_{q^s})$. Each user A chooses a large integer m_A, which is kept secret and computes and makes public the divisor mD_0. When two users A and B wish to have a key for use in some other cryptosystem, they use the divisor $m_Am_BD_0\in Jaco(F_{q^s})$. Here divisors are reduced to the form $\text{div}(a,b)$ with $\deg(b)<\deg(a)\leq n$ div 2, and some standard way is agreed upon, using the coefficients of a and b, to associate to $\text{div}(a,b)$ an integer which serves as the key.

Similarly, the ElGaml system [5] can be applied for the group $Jaco(F_{q^s})$, ofcourse, we are taking multiples of divisors rather than simply points.

In cryptosystems of this sort, we need to have a method of generating a "random" element of the group. In our case this means a divisor $D\in Jaco(F_{q^s})$. It suffies to show how to find a "random" point P on C with coordinates in F_{q^s}, after that, we can generate $D=\sum_i m_iP_i-(\sum_i m_i).\infty$ (with $m_i\geq 0$ and $\sum_i m_i\leq n$ div 2) by choosing points P with F_{q^s}-coordinates for small ($\leq n$ div 2) values of K and then setting D equal to a sum of divisors of the form

$$\sum_{\sigma \in Gal(F_{q^{sk}}/F_{q^s})} P^{\sigma} - k.\infty .$$

Without loss of generality we assume $s = 1$, i.e., we regrad C as defined over F_{q^s} and replace q^s by q. Let C have equation $v^2 = f(u)$, as before. Choose the coordinate $u = x \in F_q$ at random and attempt to solve $v^2 = f(u)$ for v, note that, there exists solution to this equation in any case. Thus, there exist efficient probabilistic algorithms for selecting random $D \in Jaco(F_{q^s})$.

We now computing multiples of divisors. A core factor in cryptosystems based on the discrete lograrithm problem (DLP) in an abelian group A is an efficient process for computing mD for $D \in A$ and for large integers m. Suppose the the group law in A is given explicity by an algorithm taking $\log^r(\sharp A)$ operations ($\sharp A$ is cardinality of A). Then the repeated-doubling method anables us to compute mD in $O(\log m.\log^r(\sharp A))$ operations.

V. CONSLUSSION

In this paper we present some results for hyperelliptic curves type, these results which similar in ellitptic curves and hyperelliptic curves. Special, in the case $n = 3$, its reduced to usual elliptic curves. From this, we expect that, we can also analyse our algorithm in the same model as for a function in the right-hand side defined in algebras with higher dimension.

ACKNOWLEDGMENT

The authors are also very grateful to the Science Foundation of Hanoi Open University for their support of the completion of this paper. The article is part of the MHN2021-01-21 scientific research.

REFERENCES

[1] Andreas Enge: Elliptie eurves and their applieations to eryptography – an Introduction. Kluwer Academic Publishers, (1999).
[2] DavidG., Cantor: Computing in the Jacobian of a Hyperelliptic Curve. Math. Com., 48(177) (1987) 95-101.
[3] Martin Seysen., A Probabilistic Factorization Algorithm with Quadratic Forms of Negative Discriminant. Mathematics of Computation, 48(178) (1987) 757-780.
[4] Neal Koblitz: HyperellipticCryptosystem. J. Cryptology., 1 (1989)139-150
[5] N. Koblitz: Elliptic curve cryptosystems, Math. Comp., 48 (1987) 203-209
[6] Serge Lang: Introduction to Algebraic Geometry. Interscience, New York, (1958).
[7] W. Diffie and M. Hetlman: New directions in cryptography, IEEE Trans. Inform. Theory, 22 (1976) 644-654.