LARGE CYCLIC SUBGROUPS OF JACOBIANS OF HYPERELLIPTIC CURVES

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. In this paper we obtain conditions on the divisors of the group order of the Jacobian of a hyperelliptic genus 2 curve, generated by the complex multiplication method described by Weng (2003) and Gaudry *et al* (2005). Examples, where these conditions imply that the Jacobian has a large cyclic subgroup, are given.

1. Introduction

In elliptic curve cryptography it is essential to know the number of points on the curve. Cryptographically we are interested in curves with large cyclic subgroups. Such elliptic curves can be constructed. The construction is based on the theory of complex multiplication, studied in detail by Atkin and Morain (1993). It is referred to as the *CM method*.

Koblitz (1989) suggested the use of hyperelliptic curves to provide larger group orders. Therefore constructions of hyperelliptic curves are interesting. The CM method for elliptic curves has been generalized to hyperelliptic curves of genus 2 by Spallek (1994), and efficient algorithms have been proposed by Weng (2003) and Gaudry *et al* (2005).

Both algorithms take as input a primitive, quartic CM field K, and give as output a hyperelliptic genus 2 curve C over a prime field $\mathbb{F}_p$. A prime number p is chosen such that $p = \omega\overline{\omega}$ for a number $\omega \in \mathfrak{O}_K$, where $\mathfrak{O}_K$ is the ring of integers of K. We have $K = \mathbb{Q}(\eta)$ and $K \cap \mathbb{R} = \mathbb{Q}(\sqrt{D})$, where $\eta = i\sqrt{a + b\xi}$ and

$$\xi = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

Write $\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta$, $c_i \in \mathbb{Z}$. Let C be a hyperelliptic curve of genus 2 over $\mathbb{F}_p$ with $\mathrm{End}(C) \simeq \mathfrak{O}_K$. The Jacobian $\mathfrak{J}_C(\mathbb{F}_p)$ is isomorphic to

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z} \times \mathbb{Z}/n_4\mathbb{Z}, \tag{1}$$

where $n_i \mid n_{i+1}$ and $n_2 \mid p - 1$. In this paper, conditions on the prime divisors of the number n_2 are obtained, and examples, where these conditions imply that the Jacobian $\mathfrak{J}_C(\mathbb{F}_p)$ has a large cyclic subgroup, are given. The conditions on the prime divisors are given by the following theorem.

Date: March 16, 2007. The author is a Ph.D.-student at the Department of Mathematical Sciences, Faculty of Science, University of Aarhus.

2000 *Mathematics Subject Classification.* Primary 14H40; Secondary 11G15, 14Q05, 94A60.

Key words and phrases. Jacobians, hyperelliptic curves, complex multiplication, cryptography.

Research supported in part by a Ph.D. grant from CRYPTOMAThIC.

Theorem 1. *Let $C/\mathbb{F}_p$ be a hyperelliptic curve of genus 2 with $\mathrm{End}(C) \simeq \mathfrak{O}_K$, where K is a primitive, quartic CM field. Assume that the structure of $\mathcal{J}_C(\mathbb{F}_p)$ is given by (1). Let $\ell \mid n_2$ be an odd prime number. Then $\ell \leq Q$, where*

$$Q = \max\{a, D, a^2 - b^2 D\},$$

if $D \equiv 2, 3 \pmod 4$, and

$$Q = \max\{a, D, 4a(a+b) - b^2(D-1), aD + 2b(D-1)\},$$

if $D \equiv 1 \pmod 4$. If $\ell > D$, then $c_1 \equiv 1 \pmod \ell$ and $c_2 \equiv 0 \pmod \ell$.

Remark 2. Since the number $n_2 \mid p-1$ and $\ell \mid n_2$, it follows that $\ell \neq p$.

2. Hyperelliptic curves

A hyperelliptic curve is a smooth, projective curve $C \subseteq \mathbb{P}^n$ of genus $g \geq 2$ with a separable, degree 2 morphism $\phi : C \to \mathbb{P}^1$. Let C be a hyperelliptic curve of genus $g = 2$ defined over a prime field $\mathbb{F}_p$, where $\mathbb{F}_p$ is of characteristic $p > 2$. By the Riemann-Roch theorem there exist an embedding $\psi : C \to \mathbb{P}^2$, mapping C to a curve given by an equation of the form

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

where $f \in \mathbb{F}_p[x]$ is of degree $\deg(f) = 6$ and have no multiple roots (see Cassels and Flynn, 1996, chapter 1).

The set of principal divisors $\mathcal{P}(C)$ on C constitutes a subgroup of the degree 0 divisors $\mathrm{Div}_0(C)$. The Jacobian $\mathcal{J}_C$ of C is defined as the quotient

$$\mathcal{J}_C = \mathrm{Div}_0(C)/\mathcal{P}(C).$$

Let $\ell \neq p$ be a prime number. The ℓ^n-torsion subgroup $\mathcal{J}_C[\ell^n] < \mathcal{J}_C$ of elements of order dividing ℓ^n is then by (Lang, 1959, theorem 6, p. 109)

$$\mathcal{J}_C[\ell^n] \simeq \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}.$$

An endomorphism $\varphi : \mathcal{J}_C \to \mathcal{J}_C$ induces a $\mathbb{Z}_\ell$-linear map

$$\varphi_\ell : T_\ell(\mathcal{J}_C) \to T_\ell(\mathcal{J}_C)$$

on the ℓ-adic Tate-module $T_\ell(\mathcal{J}_C)$ of $\mathcal{J}_C$ (Lang, 1959, chapter VII, §1). Hence φ is represented on $\mathcal{J}_C[\ell]$ by a matrix $M \in \mathrm{Mat}_{4\times 4}(\mathbb{Z}/\ell\mathbb{Z})$. Let $P(X) \in \mathbb{Z}[X]$ be the characteristic polynomial of φ (see Lang, 1959, pp. 109–110) and $P_M(X) \in (\mathbb{Z}/\ell\mathbb{Z})[X]$ the characteristic polynomial of M. Then (Lang, 1959, theorem 3, p. 186)

$$P(X) \equiv P_M(X) \pmod \ell. \tag{2}$$

Since C is defined over $\mathbb{F}_p$, the mapping $(x, y) \mapsto (x^p, y^p)$ is an isogeny on C. This isogeny induces an endomorphism φ on the Jacobian $\mathcal{J}_C$, the Frobenius endomorphism. The characteristic polynomial $P(X)$ of φ is of degree 4 (Tate, 1966, theorem 2, p. 140). Theorem 1 will be established by using the identity (2) on the Frobenius.

3. CM fields

An elliptic curve E with $\mathbb{Z} \neq \mathrm{End}(E)$ is said to have *CM*. Let K be an imaginary, quadratic number field with ring of integers $\mathfrak{O}_K$. K is a *CM field.* If $\mathrm{End}(E) \simeq \mathfrak{O}_K$, then E is said to have *CM by* $\mathfrak{O}_K$. More generally a CM field is defined as follows.

Definition 3 (CM field)**.** A number field K is a CM field, if K is a totally imaginary, quadratic extension of a totally real number field K_0.

In this paper only CM fields of degree $[K : \mathbb{Q}] = 4$ are considered. Such a field is called a *quartic* CM field. Let $K_0 = K \cap \mathbb{R}$. Then K_0 is a real, quadratic number field, $K_0 = \mathbb{Q}(\sqrt{D})$. Since K is a totally imaginary, quadratic extension of K_0, a number $\eta \in K$ exists, such that $K = K_0(\eta)$, $\eta^2 \in K_0$. The number η is totally imaginary, and we may assume $\eta = i\eta_0$, $\eta_0 \in \mathbb{R}$, and that $-\eta^2$ is totally positive.

Let C be a hyperelliptic curve of genus $g = 2$. Then C is said to have CM by $\mathfrak{O}_K$, if $\mathrm{End}(C) \simeq \mathfrak{O}_K$. The structure of K determines whether C is irreducible. More precisely, the following theorem holds.

Theorem 4. *Let C be a hyperelliptic curve of genus 2 with CM by $\mathfrak{O}_K$, where K is a quartic CM field. Then C is reducible if, and only if, $K/\mathbb{Q}$ is Galois with Galois group* $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. (Shimura, 1998, proposition 26, p. 61). □

Theorem 4 motivates the following definition.

Definition 5 (Primitive, quartic CM field)**.** A quartic CM field K is called primitive if either $K/\mathbb{Q}$ is not Galois, or $K/\mathbb{Q}$ is Galois with cyclic Galois group.

4. The CM method for genus 2

The CM method for genus 2 is described in detail by Weng (2003) and Gaudry *et al* (2005). In short, the CM method is based on the construction of the class polynomials of the number field K. The prime number p has to be chosen such that

$$p = \omega\overline{\omega} \tag{3}$$

for a number $\omega \in \mathfrak{O}_K$. There are 2 approaches to choose such a prime number p. Either pick a random prime number p, and try to solve the complex norm equation (3) in $\mathfrak{O}_K$, or generate a number $\omega \in \mathfrak{O}_K$, such that $\omega\overline{\omega}$ is a prime number. The first approach needs deep theory, e.g. class groups. The second can be implemented in a short algorithm, and is based on elementary theory. Moreover, empirical results indicate that the elementary method is the faster of the two approaches (Weng, 2003, table 1). Thus the elementary method is preferable. The algorithm is given in figure 1 for $D \equiv 2, 3 \pmod 4$. The algorithm for $D \equiv 1 \pmod 4$ is similar (Weng, 2003, section 8).

Remark 6. In either way we get an $\omega \in \mathfrak{O}_K$ with $\omega\overline{\omega} = p$. We may assume that ω fulfils the additional condition $\gcd(c_3, c_4) = 1$, where the numbers c_3 and c_4 are given by equation (4) in section 5. In the first approach, if ω does not fulfil this condition, we can just pick another prime number p. In the elementary method we can incorporate this condition in the algorithm.

Input: CM-field $K = \mathbb{Q}\left(i\sqrt{a+b\sqrt{D}}\right)$.
Output: Prime $p = \omega\overline{\omega}$ and $\omega \in \mathfrak{O}_K$.

1. Choose random numbers $c_3, c_4 \in \mathbb{Z}$ such that $\gcd(c_3, c_4) = 1$ and $c_3^2 b - c_4^2 bD \equiv 0 \pmod 2$.
2. Set $2n := -2c_3c_4a - c_3^2b - c_4^2bD$.
3. Choose c_1 at random as a divisor of n.
4. Set $c_2 := n/c_1$.
5. Set $p := c_1^2 + c_2^2D + c_3^2a + c_4^2aD + 2c_3c_4bD$. If p is not a prime number, start again.
6. Set $\omega := c_1 + c_2\sqrt{D} + (c_3 + c_4\sqrt{D})i\sqrt{a+b\sqrt{D}}$.

FIGURE 1. Elementary method to choose a prime number $p = \omega\overline{\omega}$ in the case $D \equiv 2, 3 \pmod 4$.

5. Properties of $\mathcal{J}_C(\mathbb{F}_p)$

Let K be a primitive, quartic CM field with real subfield $K_0 = \mathbb{Q}(\sqrt{D})$ of class number $h(K_0) = 1$. Write $K = \mathbb{Q}(\eta)$, where $\eta = i\sqrt{a + b\xi}$ and

$$\xi = \begin{cases} \frac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \pmod 4, \\ \sqrt{D}, & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

We may assume that $a \pm b\sqrt{D}, a + b\frac{1\pm\sqrt{D}}{2} > 0$, cf. section 3. Let p be a prime number such that

$$p = \omega\overline{\omega}$$

for a number $\omega \in \mathfrak{O} = \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$. Since $h(K_0) = 1$, we can write

$$\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta, \quad c_i \in \mathbb{Z}. \tag{4}$$

We may assume $\gcd(c_3, c_4) = 1$, cf. remark 6. Let $C/\mathbb{F}_p$ be a hyperelliptic curve of genus 2 with CM by $\mathfrak{O}_K$. Write

$$\mathcal{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z} \times \mathbb{Z}/n_4\mathbb{Z}, \tag{5}$$

where $n_i \mid n_{i+1}$ and $n_2 \mid p - 1$ (see Frey and Lange, 2006, proposition 5.78, p. 111). Depending on the remainder of D modulo 4, we obtain conditions on the prime divisors of the number n_2.

Theorem 7. *Let $C/\mathbb{F}_p$ be a hyperelliptic curve of genus 2 with CM by $\mathfrak{O}_K$. Assume that the structure of $\mathcal{J}_C(\mathbb{F}_p)$ is given by (5). Let $\ell \mid n_2$ be an odd prime number. Then $\ell \leq Q$, where*

$$Q = \max\{a, D, a^2 - b^2D\},$$

if $D \equiv 2, 3 \pmod 4$, and

$$Q = \max\{a, D, 4a(a+b) - b^2(D-1), aD + 2b(D-1)\},$$

if $D \equiv 1 \pmod 4$. If $\ell > D$, then $c_1 \equiv 1 \pmod \ell$ and $c_2 \equiv 0 \pmod \ell$.

Proof. Assume $D \equiv 2, 3 \pmod 4$. Since $\omega\overline{\omega} = p$ we find that

$$p = c_1^2 + c_2^2D + c_3^2a + c_4^2aD + 2c_3c_4bD, \tag{6}$$

$$0 = 2c_1c_2 + c_3^2b + c_4^2bD + 2c_3c_4a. \tag{7}$$

Let $P(X)$ be the characteristic polynomial of the Frobenius φ.

$$P(X) = \prod_{i=1}^{4}(X-\omega_i) = X^4 - 4c_1X^3 + (2p + 4(c_1^2 - c_2^2D))X^2 - 4c_1pX + p^2.$$

Here ω_i are the roots of $P(X)$.

Let $\ell \mid n_2$ be an odd prime number. Then by equation (5) the Jacobian $\mathfrak{J}_C(\mathbb{F}_p)$ contains a subgroup $U \simeq (\mathbb{Z}/\ell\mathbb{Z})^3$. As

$$(\mathbb{Z}/\ell\mathbb{Z})^3 < \mathfrak{J}_C(\mathbb{F}_p)[\ell] < \mathfrak{J}_C[\ell],$$

the Frobenius φ is represented on $\mathfrak{J}_C[\ell]$ by a matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & m_1 \\ 0 & 1 & 0 & m_2 \\ 0 & 0 & 1 & m_3 \\ 0 & 0 & 0 & m_4 \end{bmatrix}$$

Notice that $m_4 = \det(M) \equiv \deg(\varphi) = p^2 \pmod{\ell}$. Since $p \equiv 1 \pmod{\ell}$, M has the characteristic polynomial

$$P_M(X) \equiv (X-1)^4 = X^4 - 4X^3 + 6X^2 - 4X + 1 \pmod{\ell}.$$

Now $P(X) \equiv P_M(X) \pmod{\ell}$. Thus

$$c_1 \equiv c_1^2 - c_2^2D \equiv 1 \pmod{\ell},$$

since $\ell \neq 2$.

Assume $\ell > D$. Then

$$c_1 \equiv 1 \pmod{\ell}, \quad c_2 \equiv 0 \pmod{\ell}. \tag{8}$$

By the equations (6) and (7), we get

$$c_1^2 + c_2^2D + c_3^2a + c_4^2aD + 2c_3c_4bD \equiv 1 \pmod{\ell},$$
$$2c_1c_2 + c_3^2b + c_4^2bD + 2c_3c_4a \equiv 0 \pmod{\ell}.$$

Therefore, by equation (8), the following holds.

$$\begin{aligned} c_3^2a + c_4^2aD + 2c_3c_4bD &\equiv 0 \pmod{\ell}, \\ c_3^2b + c_4^2bD + 2c_3c_4a &\equiv 0 \pmod{\ell}. \end{aligned} \tag{9}$$

It follows that

$$c_3c_4(a^2 - b^2D) \equiv 0 \pmod{\ell}.$$

Here $a^2 - b^2D = (a+b\sqrt{D})(a-b\sqrt{D}) > 0$, since $a \pm b\sqrt{D} > 0$. Assume $\ell > a^2 - b^2D$. Then we get $c_3c_4 \equiv 0 \pmod{\ell}$. Thus either $c_3 \equiv 0 \pmod{\ell}$ or $c_4 \equiv 0 \pmod{\ell}$.

Assume $\ell > a$. If $c_3 \equiv 0 \pmod{\ell}$, then $c_4^2aD \equiv 0 \pmod{\ell}$ by equation (9), i.e. $c_4 \equiv 0 \pmod{\ell}$. On the other hand if $c_4 \equiv 0 \pmod{\ell}$, then $c_3^2a \equiv 0 \pmod{\ell}$, i.e. $c_3 \equiv 0 \pmod{\ell}$.

Summing up, $c_3 \equiv c_4 \equiv 0 \pmod{\ell}$ if $\ell > \max\{a, D, a^2 - b^2D\}$. But this contradicts $\gcd(c_3, c_4) = 1$. Therefore $\ell \leq \max\{a, D, a^2 - b^2D\}$, and the case $D \equiv 2, 3 \pmod{4}$ is established.

Now consider the case $D \equiv 1 \pmod 4$. Since $\omega\overline{\omega} = p$, we now find that

$$\begin{aligned} p &= c_1^2 + c_1c_2 + \frac{1}{4}c_2^2(1+D) + c_3^2\Big(a + \frac{1}{2}b\Big) + c_3c_4\Big(\frac{1}{2}b(D+1) + a\Big) \\ &\quad + c_4^2\Big(\frac{1}{8}b(3D+1) + \frac{1}{4}a(D+1)\Big), \\ 0 &= c_1c_2 + \frac{1}{2}c_2^2 + \frac{1}{2}c_3^2b + c_3c_4(a+b) + c_4^2\Big(\frac{1}{8}b(D+3) + \frac{1}{2}a\Big). \end{aligned}$$

The characteristic polynomial of the Frobenius φ is given by

$$\begin{aligned} P(X) &= X^4 - (4c_1 + 2c_2)X^3 + (2p + (2c_1 + c_2)^2 - c_2^2D)X^2 \\ &\quad - (4c_1 + 2c_2)pX + p^2. \end{aligned}$$

Let $\ell \mid n_2$ be an odd prime number. As in the case $D \equiv 2, 3 \pmod 4$, the Frobenius φ is represented on $\mathcal{J}_C[\ell]$ by a matrix M with the characteristic polynomial

$$P_M(X) \equiv X^4 - 4X^3 + 6X^2 - 4X + 1 \pmod \ell.$$

Since $P(X) \equiv P_M(X) \pmod \ell$, it follows that

$$4c_1 + 2c_2 \equiv (2c_1 + c_2)^2 - c_2^2D \equiv 4 \pmod \ell.$$

Assume $\ell > D$. Then

$$c_1 \equiv 1 \pmod \ell, \quad c_2 \equiv 0 \pmod \ell.$$

Now

$$\begin{aligned} &c_3^2(8a + 4b) + c_3c_4\left(4b(D+1) + 8a\right) \\ &\qquad + c_4^2\left(b(3D+1) + 2a(D+1)\right) \equiv 0 \pmod \ell \\ &4c_3^2b + 8c_3c_4(a+b) + c_4^2\left(b(D+3) + 4a\right) \equiv 0 \pmod \ell. \end{aligned}$$

Therefore

$$\begin{aligned} &4c_3^2a + 2c_3c_4b(D-1) + c_4^2(a+b)(D-1) \equiv 0 \pmod \ell, \\ &4c_3^2b + 8c_3c_4(a+b) + c_4^2\left(b(D+3) + 4a\right) \equiv 0 \pmod \ell. \end{aligned} \tag{10}$$

It follows that

$$(b^2(D-1) - 4a(a+b))(2c_3c_4 - c_4^2) \equiv 0 \pmod \ell.$$

Notice that

$$4a(a+b) - b^2(D-1) = 4\left(a + b\frac{1+\sqrt{D}}{2}\right)\left(a + b\frac{1-\sqrt{D}}{2}\right) > 0.$$

Now assume $\ell > 4a(a+b) - b^2(D-1)$. Then

$$2c_3c_4 - c_4^2 \equiv 0 \pmod \ell.$$

Thus either $c_4 \equiv 0 \pmod \ell$ or $c_4 \equiv 2c_3 \pmod \ell$.

Assume $\ell > a$. If $c_4 \equiv 0 \pmod \ell$, then $c_3^2 \equiv 0 \pmod \ell$ by equation (10), i.e. $c_3 \equiv 0 \pmod \ell$. This contradicts $\gcd(c_3, c_4) = 0$. So $c_4 \not\equiv 0 \pmod \ell$. Then $c_4 \equiv 2c_3 \pmod \ell$. From equation (10) it follows that

$$c_4^2(2b(D-1) + aD) \equiv 0 \pmod \ell,$$

i.e. $c_4 \equiv 0 \pmod \ell$ if $\ell > 2b(D-1) + aD$. But then $c_3 \equiv c_4 \equiv 0 \pmod \ell$, a contradiction. $\square$

Remark 8. The condition $\gcd(c_3, c_4) = 1$ may be relaxed. In the proof of theorem 7, we only need $\ell \nmid \gcd(c_3, c_4)$.

6. Examples

By theorem 7, large prime divisors of the order $N = |\mathfrak{J}_C(\mathbb{F}_p)|$ will not divide the divisor n_2 of N. This is useful if we want to determine the possible cyclic subgroups of $\mathfrak{J}_C(\mathbb{F}_p)$.

Example 1. In $K = \mathbb{Q}\left(i\sqrt{2+\sqrt{2}}\right)$, the prime number

$$p = 1531403392215282623743624735925933 4919$$

is the complex norm of the number

$$\begin{aligned}\omega = {} & 3913314953099587393 - 31\sqrt{2} \\ & + (4483312578 + 6978049007\sqrt{2})i\sqrt{2+\sqrt{2}}.\end{aligned}$$

The CM method yields a hyperelliptic genus 2 curve C with Jacobian of order

$$N = 234519634968847474692278544362349582158321382804023011720188699330496198748.$$

Since $N = 2^2 \cdot 7^3 \cdot 17 \cdot 23 \cdot 4993 \cdot r$, where

$$r = 875561738089195201633298616759897394332430403735970748570971 40343$$

is a prime number, either

$$\mathfrak{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/N\mathbb{Z} \quad \text{or} \quad \mathfrak{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_3\mathbb{Z} \times \mathbb{Z}/n_4\mathbb{Z},$$

where $n_3 \in \{2, 7, 14\}$.

Example 2. In $K = \mathbb{Q}\left(i\sqrt{7+\sqrt{5}}\right)$, the prime number

$$p = 143041070968789403308931 23933$$

is the complex norm of the number

$$\begin{aligned}\omega = {} & -119599766860084 + 5279155\sqrt{5} \\ & + \left(13860963299 + 4898901569\sqrt{5}\right) i\sqrt{7+\sqrt{5}}.\end{aligned}$$

The CM method yields a hyperelliptic genus 2 curve C with Jacobian of order

$$N = 20460747983898930953674814829733355744711104697658908 8984.$$

Since $N = 2^3 \cdot 7^3 \cdot 71 \cdot r$, where

$$r = 1050217015557576630891205130257738047915611254140091$$

is a prime number, either

$$\mathfrak{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/n_3\mathbb{Z} \times \mathbb{Z}/n_4\mathbb{Z},$$

where $n_3 \in \{1, 2, 7, 14\}$, or

$$\mathfrak{J}_C(\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n_3\mathbb{Z} \times \mathbb{Z}/n_4\mathbb{Z},$$

where $n_3 \in \{2, 14\}$.

References

A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, vol. 61, pp. 29–68, 1993.

J.W.S. Cassels and E.V. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2. London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.

G. Frey and T. Lange. Varieties over Special Fields. In H. Cohen and G. Frey, editors, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, pp. 87–113. Chapman & Hall/CRC, 2006.

P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng. The p-adic CM-Method for Genus 2. 2005. `http://arxiv.org`.

N. Koblitz. Hyperelliptic cryptosystems. *J. Cryptology*, vol. 1, pp. 139–150, 1989.

S. Lang. *Abelian Varieties*. Interscience, 1959.

G. Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 1998.

A.-M. Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-Key-Kryptosystemen*. Ph.D. thesis, Institut für Experimentelle Mathematik, Universität GH Essen, 1994.

J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, vol. 2, pp. 134–144, 1966.

A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, vol. 72, pp. 435–458, 2003.

Department of Mathematical Sciences, Faculty of Science, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C

E-mail address: `cr@imf.au.dk`