UNIVERSITY OF AARHUS
DEPARTMENT OF MATHEMATICS

ISSN: 1397–4076

p-TORSION OF GENUS TWO CURVES OVER PRIME FIELDS OF CHARACTERISTIC p

by Christian Robenhagen Ravnshøj

Preprint Series No.: 6

May 2007

2007/05/29

Ny Munkegade, Bldg. 1530
DK-8000 Aarhus C, Denmark

http://www.imf.au.dk
institut@imf.au.dk

p-TORSION OF GENUS TWO CURVES OVER PRIME FIELDS OF CHARACTERISTIC p

CHRISTIAN ROBENHAGEN RAVNSHØJ

Abstract. Consider the Jacobian of a hyperelliptic genus two curve defined over a prime field of characteristic p and with complex multiplication. In this paper we show that the p-Sylow subgroup of the Jacobian is either trivial or of order p.

1. Introduction

In elliptic curve cryptography it is essential to know the number of points on the curve. Cryptographically we are interested in elliptic 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 two 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 (see section 3 for the definition of a CM field), and give as output a hyperelliptic genus two curve C defined over a prime field $\mathbb{F}_p$. A prime number p is chosen such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_K$, 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

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

In this paper, the following theorem is established.

Theorem 1. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$. Assume that* $\mathrm{End}(C) \simeq \mathfrak{O}_K$*, where K is a primitive, quartic CM field as defined in definition 5, and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as above. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

2. Hyperelliptic curves

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

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

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 PhD grant from CRYPTOMAThIC.

where $f \in \mathbb{F}_p[x]$ is of degree six 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

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

Since C is defined over $\mathbb{F}_p$, the mapping $(x, y) \mapsto (x^p, y^p)$ is a morphism on C. This morphism induces the p-power Frobenius endomorphism φ on the Jacobian $\mathcal{J}_C$. The characteristic polynomial $P(X)$ of φ is of degree four (Tate, 1966, Theorem 2, p. 140), and by the definition of $P(X)$ (see Lang, 1959, pp. 109–110),

$$|\mathcal{J}_C(\mathbb{F}_p)| = P(1),$$

i.e. the number of $\mathbb{F}_p$-rational points on the Jacobian is determined by $P(X)$.

3. CM fields

An elliptic curve E with $\mathbb{Z} \neq \mathrm{End}(E)$ is said to have *complex multiplication*. Let K be an imaginary, quadratic number field with ring of integers $\mathfrak{O}_K$. K is a *CM field*, and 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 2 (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.

Remark 3. Consider a quartic CM field K. Let $K_0 = K \cap \mathbb{R}$ be the real subfield of K. Then K_0 is a real, quadratic number field, $K_0 = \mathbb{Q}(\sqrt{D})$. By a basic result on quadratic number fields, the ring of integers of K_0 is given by $\mathfrak{O}_{K_0} = \mathbb{Z} + \xi\mathbb{Z}$, where

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

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 that $\eta = i\eta_0$, $\eta_0 \in \mathbb{R}$. Furthermore we may assume that $\eta^2 \in \mathfrak{O}_{K_0}$; so $\eta = i\sqrt{a + b\xi}$, where $a, b \in \mathbb{Z}$.

Let C be a hyperelliptic curve of genus two. 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 two with* $\mathrm{End}(C) \simeq \mathfrak{O}_K$*, 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.

The CM method for constructing curves of genus two with prescribed endomorphism ring 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 a primitive, quartic CM field K with real subfield K_0 of class number $h(K_0) = 1$. The prime number p has to be chosen such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_K$. By Weng (2003) we may assume that $x \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$.

4. The p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$

Let K be a primitive, quartic CM field with real subfield $K_0 = \mathbb{Q}(\sqrt{D})$ of class number $h(K_0) = 1$. Cf. Remark 3 we may write $K = \mathbb{Q}(\eta)$, where $\eta = i\sqrt{a + b\xi}$ and

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

Let p be a prime number such that $p = x\overline{x}$ for a number $x \in \mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$. Let C be a hyperelliptic curve of genus two defined over $\mathbb{F}_p$ with $\mathrm{End}(C) \simeq \mathfrak{O}_K$. Assume that the p-power Frobenius under this isomorphism is given by the number

$$\omega = c_1 + c_2\xi + (c_3 + c_4\xi)\eta, \quad c_i \in \mathbb{Z}. \tag{1}$$

Since the p-power Frobenius is of degree p, we know that $\omega\overline{\omega} = p$.

Remark 6. If $c_2 = 0$ in (1), then $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and K is not primitive. So $c_2 \neq 0$.

The characteristic polynomial $P(X)$ of the Frobenius is given by

$$P(X) = \prod_{i=1}^{4}(X - \omega_i),$$

where ω_i are the conjugates of ω. Since the conjugates of ω are given by $\omega_1 = \omega$, $\omega_2 = \overline{\omega}_1$, ω_3 and $\omega_4 = \overline{\omega}_3$, where $\omega_3 = c_1 + c_2\xi' + (c_3 + c_4\xi')\eta'$, $\eta' = i\sqrt{a + b\xi'}$ and

$$\xi' = \begin{cases} -\sqrt{D}, & \text{if } D \equiv 2, 3 \mod 4 \\ \frac{1-\sqrt{D}}{2}, & \text{if } D \equiv 2, 3 \mod 4 \end{cases}$$

it follows that

$$P(X) = X^4 - 4c_1X^3 + (2p + 4(c_1^2 - c_2^2D))X^2 - 4c_1pX + p^2,$$

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

$$P(X) = X^4 - 2cX^3 + (2p + c^2 - c_2^2D)X^2 - 2cpX + p^2,$$

if $D \equiv 1 \mod 4$. Here, $c = 2c_1 + c_2$. We notice that $4 \mid P(1) = |\mathfrak{J}_C(\mathbb{F}_p)|$. This observation leads to the following lemma.

Lemma 7. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$ of characteristic $p > 5$. Assume that $\mathrm{End}(C) \simeq \mathfrak{O}_K$ and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as in remark 3. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

Proof. Assume $p^2 \mid N = |\mathfrak{J}_C(\mathbb{F}_p)|$. Since $|\omega_i| = \sqrt{p}$, we know that

$$N = P(1) = \prod_{i=1}^{4}(1 - \omega_i) \leq (1 + \sqrt{p})^4 = p^2 + 4p\sqrt{p} + 6p + 4\sqrt{p} + 1.$$

Hence, $\frac{N}{p^2} < 4$ for $p > 5$. But then $4 \nmid N$, a contradiction. So $p^2 \nmid N$, i.e. the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is of order at most p. $\square$

Now consider the case $p \leq 5$. Assume at first that $D \equiv 2, 3 \mod 4$. Since $\omega_1\overline{\omega}_1 = \omega_2\overline{\omega}_2 = p$, we know that $|c_1 \pm c_2\sqrt{D}| \leq \sqrt{p}$. Thus,

$$\begin{aligned} |c_2\sqrt{D}| &= \frac{1}{2}\left|c_1 + c_2\sqrt{D} - \left(c_1 - c_2\sqrt{D}\right)\right| \\ &\leq \frac{1}{2}\left(\left|c_1 + c_2\sqrt{D}\right| + \left|c_1 - c_2\sqrt{D}\right|\right) \\ &\leq \sqrt{p}. \end{aligned}$$

Similarly we see that $|c_1| \leq \sqrt{p}$. Assume that $D > 5$. Then $|c_2| \leq \sqrt{\frac{p}{D}} < 1$. So $c_2 = 0$, since $c_2 \in \mathbb{Z}$. This contradicts remark 6, i.e. $D \leq 5$. Now assume that $D = 2$. Then $c_2 \leq \sqrt{\frac{p}{2}} \leq \sqrt{\frac{5}{2}}$, i.e. $c_2 \in \{0, \pm 1\}$. Therefore it follows by calculating N for each of the possible values of c_1 and c_2, that if $p^2 \mid N$, then $c_2 = 0$. This is again a contradiction. So if $D = 2$, then $p^2 \nmid N$. Similar it follows that if $D = 3$, then $p^2 \nmid N$.

Finally assume that $D \equiv 1 \pmod 4$. Then it follows from $\omega_1\overline{\omega}_1 = \omega_2\overline{\omega}_2 = p$ that $|c_1 + c_2\frac{1\pm\sqrt{D}}{2}| \leq \sqrt{p}$. Thus, $|c_2\sqrt{D}| \leq 2\sqrt{p}$ and $|2c_1 - c_2| \leq 2\sqrt{p}$. Assume that $D > 20$. Then $|c_2| < 2\sqrt{\frac{5}{20}} = 1$, i.e. $c_2 = 0$, a contradiction. So $D \leq 20$. By calculating N for each of the possible values of p, D, c and c_2 it follows that $p^2 \nmid N$ also in this case. Hence the following lemma is established.

Lemma 8. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$ of characteristic $p \leq 5$. Assume that* $\mathrm{End}(C) \simeq \mathfrak{O}_K$ *and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as in remark 3. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

Summing up, the following theorem holds.

Theorem 9. *Let C be a hyperelliptic curve of genus two defined over a prime field $\mathbb{F}_p$. Assume that* $\mathrm{End}(C) \simeq \mathfrak{O}_K$ *and that the p-power Frobenius under this isomorphism is given by a number in $\mathfrak{O}_{K_0} + \eta\mathfrak{O}_{K_0}$, where η is given as in remark 3. Then the p-Sylow subgroup of $\mathfrak{J}_C(\mathbb{F}_p)$ is either trivial or of order p.*

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.

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.* PhD 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, University of Aarhus, Ny Munkegade, Building 1530, DK-8000 Aarhus C

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