MATHEMATICS OF COMPUTATION
Volume 72, Number 241, Pages 435–458
S 0025-5718(02)01422-9
Article electronically published on May 3, 2002

CONSTRUCTING HYPERELLIPTIC CURVES OF GENUS 2 SUITABLE FOR CRYPTOGRAPHY

ANNEGRET WENG

Abstract. In this article we show how to generalize the CM-method for elliptic curves to genus two. We describe the algorithm in detail and discuss the results of our implementation.

1. Introduction

In 1986 Atkin [1] proposed an algorithm for primality proving using elliptic curves. An important part of his algorithm deals with the construction of elliptic curves with given group order. It is based on the theory of complex multiplication and was investigated in detail by Atkin and Morain in [2]. The complex multiplication method (short: CM-method) turned out to be a very efficient algorithm for producing elliptic curves used for cryptosystems.

Although point counting on randomly chosen elliptic curves has been improved over the years and is now sufficiently fast, the CM-method is still attractive. If the class number is not too large (say ≤ 1000), the class polynomial can easily be factored. In this case the CM-method is faster than point counting. Also, the curves are constructed so as to have a suitable group order.

Koblitz [8] suggested the use of Jacobians of hyperelliptic curves for cryptography to provide a larger class of curves. For general hyperelliptic curves of small genus (say $g \leq 3$) the discrete logarithm problem in the Jacobian of a hyperelliptic curve is thought to be hard. Though the scalar multiplication is slower than for elliptic curves, we are working over smaller fields, which has some advantages.

To ensure the security of a cryptosystem based on the discrete logarithm problem in a finite abelian group, we have to make sure that the group order contains a large prime factor [18]. More precisely, the group order should either be prime or a product of a prime and a small number. For hyperelliptic curves, finding the group order of the Jacobian seems to be a nontrivial task. Up to now there exists no point counting algorithm for randomly chosen hyperelliptic curves which reaches the group order suitable for cryptography (say 2^{160}). Gaudry and Harley have recently implemented a generalisation of Schoof-Atkin-Elkies and were able to determine the order of the Jacobian of a curve of genus two defined over $\mathbb{F}_p$ where $p = 10^{19} + 51$ [4].

Received by the editor January 19, 2001 and, in revised form, March 29, 2001.

2000 *Mathematics Subject Classification.* Primary 11Y16, 11Y40, 94A60; Secondary 14K22, 14H45.

This work was supported by the NRW Forschungsverbund Datensicherheit (see `www.datensicherheit.nrw.de`) and the DFG (Graduiertenkolleg).

In this paper we want to discuss one possible solution to the group order problem on hyperelliptic curves over finite fields. There exists a generalisation of the elliptic curve algorithm with complex multiplication by Frey and Spallek [21] in the case of genus two. Spallek gave two examples with class number one in her thesis. Wang [23] and Weber [24] suggested replacing the computation of Gröbner bases with an efficient algorithm by Mestre [12]. Based on Spallek's work, van Wamelen constructed all curves defined over $\mathbb{Q}$ having complex multiplication [22].

A complete description and implementation of the CM-method for $g = 2$ does not yet exist in the literature. In this paper we combine the ideas in [21, 23, 24, 22] to get an efficient algorithm. We discuss our implementation and give examples. We were able to compute hyperelliptic curves over prime fields whose Jacobians have complex multiplication by the maximal order in a CM-field up to class number 10. Finally we present statistics on the distribution of the group order of the Jacobian.

In Section 2 we recall some basic definitions about hyperelliptic curves over finite fields. The construction is restricted to hyperelliptic curves of genus 2 which are defined over a prime field $\mathbb{F}_p$ or a small extension of a prime field.

The rough idea of the algorithm goes as follows:

1. Fix a CM-field K and find a suitable prime p and a possible group order n.
2. List all principally polarized abelian varieties over $\mathbb{C}$ having complex multiplication by the maximal order $\mathcal{O}_K$. They are given by certain period matrices $\Omega_i \in \mathbb{H}_2$ where $\mathbb{H}_2 = \{z \in \mathbb{C}^{2\times 2}, z = z^t, \operatorname{Im} z > 0\}$ is the Siegel upper half plane (see Section 3).
3. Compute the ten theta constants up to a certain precision (see Section 4 and the Appendix, p. 456).
4. Compute Igusa's invariants j_1, j_2, j_3 from the theta constants (see Section 5). Reduce them modulo p.
5. Compute Mestre's invariants Q_{ij} and H_{ijk} from j_1, j_2, j_3 (see Section 6).
6. Apply Mestre's algorithm to get the equation of the hyperelliptic curve C (see Section 7).
7. Check whether the group order $\#J(C)$ is equal to n.

The complete algorithm is presented in Section 9. In Section 8 we show how to get good Weil numbers for $g = 2$. In Section 10 we give an analysis of the complexity of the algorithm, including a list of CM-fields suitable for our method. Section 11 lists several statistics. In Section 12 we give two examples. In Section 13 we discuss further improvements and generalisations and the limits of the CM-method.

2. Definitions

2.1. **The Jacobian of a hyperelliptic curve.** In this section we fix notations and give some basic definitions about hyperelliptic curves over finite fields and complex multiplication.

Let C be a hyperelliptic curve of genus 2 defined over a finite prime field $\mathbb{F}_p$ ($p \neq 2$). Then the curve can be given in the form

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

where $f(x) \in \mathbb{F}_p[x]$ has degree six and no multiple roots in $\overline{\mathbb{F}}_p$.

In cryptography we consider the abelian group formed by the $\mathbb{F}_p$-rational points on the Jacobian of C. The Jacobian is defined by

$$J_C = Div_0(C)/Princ(C)$$

where $Div_0(C)$ (resp. $Princ(C)$) denotes the group of degree 0 divisors (resp. principal divisors) (see [8]). We denote the group of $\mathbb{F}_p$-rational points on its Jacobian by $J_C(\mathbb{F}_p)$.

2.2. **The Frobenius of hyperelliptic curves of genus two over finite fields.** The isogeny

$$(x, y) \mapsto (x^p, y^p)$$

on the curve C induces an endomorphism π on the Jacobian J_C. The endomorphism π is called the Frobenius endomorphism. The characteristic polynomial of the Frobenius is a polynomial of degree 4. If the characteristic polynomial of π is irreducible, it defines a CM-field K of degree 4 over $\mathbb{Q}$. This means K is an imaginary quadratic extension over a real quadratic number field K_0.

Once we know the roots π_i of the characteristic polynomial we can determine the group order by

$$\#J(C) = \prod_{i=1}^{4}(1 - \pi_i).$$

We fix a CM-field K and consider an algebraic number $w_1 \in K$ such that

$$[\mathbb{Q}(w_1) : \mathbb{Q}] = 4 \quad \text{and} \quad w_1\overline{w_1} = p.$$

Its conjugates are given by w_i, $i = 2, \ldots, 4$.

Let $Tor(U)$ be the torsion group of units of K.

Now suppose we have a curve defined over $\mathbb{F}_p$ having complex multiplication by $\mathcal{O}_K$ (the maximal order in K). Then we have at most

$$\begin{cases} \#Tor(U) & \text{if } p \text{ is inert with respect to } K_0/\mathbb{Q} \text{ or } K \text{ is Galois,} \\ 2\,\#Tor(U) & \text{if } p \text{ splits completely in } K \text{ and } K \text{ is not Galois} \end{cases}$$

possibilities for the group order $\#J(\mathbb{F}_p)$.

From now on we assume that K does not contain a cyclotomic field. Then there are two, resp. four possibilities for the group order.

3. Complex multiplication

In this section we refer to the literature [19], [10], [9], [21]. We will only give the definitions that are necessary to understand the algorithm.

Every abelian variety of dimension n over $\mathbb{C}$ is isomorphic to $\mathbb{C}^n/L$ for some lattice L. Further, we know that there exists a nondegenerate Riemann form on the lattice L (for definitions and proofs, see [10], [21]). The Riemann form induces a polarization on L. If it is a principal polarization the lattice can be given by $\mathbb{Z}^n + \Omega\mathbb{Z}^n$, where Ω lies in the Siegel upper half plane $\mathbb{H}_n = \{z \in M_n(\mathbb{C}), z^t = z, \operatorname{Im} z \text{ positive definite}\}$. Every Jacobian variety has a principal polarization [14].

Let $End(A)$ be the endomorphism ring of a simple abelian variety over $\mathbb{C}$. The field $End(A) \otimes \mathbb{Q}$ is either a totally real number field or an imaginary quadratic extension of a totally real number field [19].

We concentrate on the case that

$$End(A) \otimes \mathbb{Q} = K \quad \text{and} \quad [K : \mathbb{Q}] = 2n$$

and there exists a subfield K_0 in K such that K_0 is totally real and $[K : K_0] = 2$. The field K is called a **CM-field**.

If $\{\sigma_1,\dots,\sigma_n\}$ are the real embeddings of K_0, then the embeddings of K into $\mathbb{C}$ are given by

$$\{\hat{\sigma}_1,\dots,\hat{\sigma}_n,\rho\hat{\sigma}_1,\dots,\rho\hat{\sigma}_n\}$$

where $\hat{\sigma}_i$ is an embedding with $\hat{\sigma}_i|K_0=\sigma_i$ and ρ denotes the complex conjugation.

We choose a subset $\Phi=(\varphi_1,\dots,\varphi_n)$ such that $\varphi_i\neq\varphi_j,\rho\varphi_j$. Then (K,Φ) is called a **CM-type**.

Let $\mathfrak{A}$ be an ideal in K and (K,Φ) a CM-type. Then

$$\Phi(\alpha):=(\varphi_1(\alpha),\dots,\varphi_n(\alpha))^t,\quad \alpha\in\mathfrak{A},$$

is a lattice in $\mathbb{C}^n$ having complex multiplication by $\mathcal{O}_K$, i.e., the matrix

$$S_\Phi(\gamma)=\begin{pmatrix}\varphi_1(\gamma) & & \\ & \dots & \\ & & \varphi_n(\gamma)\end{pmatrix},\quad \gamma\in\mathcal{O}_K,$$

leaves the lattice invariant (see [19]). The corresponding abelian variety is said to be an abelian variety of CM-type (K,Φ).

An abelian variety of CM-type (K,Φ) is simple iff the CM-type is primitive. There exists an easy criterion for whether a CM-type is primitive (see [19], [10], [9], [21]).

Now we adapt the theory to our situation:

Note that Jacobians of hyperelliptic curves of genus 2 are exactly the principally polarized abelian varieties of dimension 2 [13].

Let $K_0=\mathbb{Q}(\sqrt{d})$, $d\in\mathbb{N}$, be a real quadratic number field of class number one. Suppose $\alpha=a+b\sqrt{d}$ is squarefree and totally positive (i.e., $a\pm b\sqrt{d}>0$). Then $K=\mathbb{Q}(i\sqrt{\alpha})$ is a CM-field of degree 4 over $\mathbb{Q}$. A CM-type (K,Φ) is not primitive iff K is Galois with Galois group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Let ϵ be the fundamental unit of K_0. We consider the subgroup of units which consists of all totally positive units in K_0, and denote it by U^+. It has a subgroup U_N^+ that consists of all units which satisfy a relative norm equation with respect to K/K_0. Note that $U^+=U_N^+$ if the fundamental unit has negative norm.

Since K_0 has class number one, the ring of integers can be given in the form

$$\mathcal{O}_{K_0}+\gamma\mathcal{O}_{K_0},$$

where $\gamma\in\mathcal{O}_K$. Further, every ideal $\mathfrak{A}_j$ in $\mathcal{O}_K$ has a relative basis

$$\alpha_j\mathcal{O}_{K_0}+\beta_j\mathcal{O}_{K_0},\quad \alpha_j,\beta_j\in K.$$

The ideal $\mathfrak{A}_j$ is equivalent to an ideal of the form

$$\mathcal{O}_{K_0}+\tau_j\mathcal{O}_{K_0},\quad \tau_j=\frac{\alpha_j}{\beta_j}\in\mathcal{O}_K,$$

where $\operatorname{Im}\tau_j>0$. If $\epsilon\notin U^+$, we will assume that $N_{K/K_0}(\tau_j)$ is always totally positive.

We can define two continuations of the real conjugation in K_0 to K. We set

$$\hat{\sigma}(i\sqrt{\alpha}^+)=i\sqrt{\sigma(\alpha)}^+\quad\text{and}\quad \rho\hat{\sigma}(i\sqrt{\alpha}^+)=-i\sqrt{\sigma(\alpha)}^+,$$

where $\sqrt{a}^+$ denotes the positive square root of $a\in\mathbb{R}$.

Spallek [21] proved the following theorem:

Theorem 3.1. *Let K be a CM-field as above and K either not Galois or Galois with Galois group $\mathbb{Z}/4\mathbb{Z}$. Let $K_0 = \mathbb{Z}+\mathbb{Z}w$ be the real subfield, σ the real conjugation and $\varphi = \rho\hat{\sigma}$.*

1. *A complete system of simple principally polarized abelian varieties (up to isomorphism) having complex multiplication by $\mathcal{O}_K$ is given by $\mathcal{K} = \mathcal{K}_{1,\varphi} \cup \mathcal{K}_{1,\overline{\varphi}}$, where*

$$\mathcal{K}_{1,\varphi} = \begin{cases} \{(\tau_j, \tau_j^{\varphi}) : N_{K/K_0}(\tau_j) \text{ totally pos.}\}, & \epsilon \in U_N^+, \\ \{(\tau_j, \tau_j^{\varphi}), (\epsilon\tau_j, \epsilon\tau_j^{\varphi}) : N_{K/K_0}(\tau_j) \text{ totally pos.}\}, & \epsilon \in U^+ - U_N^+, \\ \{(\tau_j, \tau_j^{\varphi}) : N_{K/K_0}(\tau_j) \text{ totally pos.}\}, & \text{otherwise}, \end{cases}$$

$$\mathcal{K}_{1,\overline{\varphi}} = \begin{cases} \emptyset, & \text{if } K \text{ is Galois}, \\ \{(\tau_j, (\tau_j)^{\rho\varphi}) : N_{K/K_0}(\tau_j) \text{ not totally pos.}\}, & \epsilon \in U_N^+, \\ \{(\tau_j, \tau_j^{\rho\varphi}), (\epsilon\tau_j, \epsilon\tau_j^{\rho\varphi}) : N_{K/K_0}(\tau_j) \text{ totally pos.}\}, & \epsilon \in U^+ - U_N^+, \\ \{(\epsilon\tau_j, (\epsilon\tau_j)^{\rho\varphi}) : N_{K/K_0}(\tau_j) \text{totally pos.}\}, & \text{otherwise}. \end{cases}$$

2. *Given a principally polarized abelian variety of type $(K, \{1, \psi\})$ of the form (s_j, s_j^{ψ}), the corresponding period matrix is given by*

$$\Omega_{s_j, s_j^{\psi}} = \frac{1}{w - w^{\sigma}} \begin{pmatrix} w^2 s_j - (w^{\psi})^2 s_j^{\psi} & w s_j - w^{\psi} s_j^{\psi} \\ w s_j - w^{\psi} s_j^{\psi} & s_j - s_j^{\psi} \end{pmatrix}.$$

4. Computing the theta constants

Once we have a period matrix Ω, we want to compute the invariants of the curves corresponding to the Jacobian represented by Ω. For this we use the theta constants

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega, 0) = \sum_{n \in \mathbb{Z}^2} \exp(\pi i (n + \frac{1}{2}\delta)^t \Omega (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (\frac{1}{2}\epsilon)), \tag{1}$$

where $\delta, \epsilon \in \{0, 1\}^2$. It can easily be shown that

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega, 0) = 0$$

if $\delta\epsilon^t = 1 \mod 2$. Thus we concentrate on the 10 even theta constants

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega, 0), \quad \delta^t \epsilon \equiv 0 \mod 2.$$

They are given by

$$\theta_1 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{0}{0} \end{bmatrix}, \ \theta_2 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{1}{0} \end{bmatrix}, \ \theta_3 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{0}{1} \end{bmatrix}, \ \theta_4 := \theta \begin{bmatrix} \binom{0}{0} \\ \binom{1}{1} \end{bmatrix}, \ \theta_5 := \theta \begin{bmatrix} \binom{1}{0} \\ \binom{0}{0} \end{bmatrix},$$
$$\theta_6 := \theta \begin{bmatrix} \binom{1}{0} \\ \binom{0}{1} \end{bmatrix}, \ \theta_7 := \theta \begin{bmatrix} \binom{0}{1} \\ \binom{0}{0} \end{bmatrix}, \ \theta_8 := \theta \begin{bmatrix} \binom{0}{1} \\ \binom{1}{0} \end{bmatrix}, \ \theta_9 := \theta \begin{bmatrix} \binom{1}{1} \\ \binom{0}{0} \end{bmatrix}, \ \theta_{10} := \theta \begin{bmatrix} \binom{1}{1} \\ \binom{1}{1} \end{bmatrix}.$$

Suppose we would like to compute the theta constants up to the precision 10^{-s} for some integer s. Note that the absolute value of a summand in (1) depends only on

$$\left| \exp(-\pi (n + \frac{1}{2}\delta)^t \operatorname{Im} \Omega (n + \frac{1}{2}\delta)) \right|.$$

Thus we need an algorithm which computes all $n \in \mathbb{Z}^2$ such that

$$(n+\frac{1}{2}\delta)^t \operatorname{Im}\Omega(n+\frac{1}{2}\delta) \leq C.$$

Such an algorithm is given in the Appendix.

Now we have to find the value C such that

$$\left| \sum_{\substack{n\in\mathbb{Z}^2 \\ (n+\frac{1}{2}\delta)^t \operatorname{Im}\Omega(n+\frac{1}{2}\delta)>C}} \exp(\pi i((n+\frac{1}{2}\delta)^t\Omega(n+\frac{1}{2}\delta)+2(n+\frac{1}{2}\delta)^t(\frac{1}{2}\epsilon))) \right| \leq 10^{-s}.$$

We have

$$\begin{aligned} &\left| \sum_{\substack{n\in\mathbb{Z}^2 \\ (n+\frac{1}{2}\delta)^t \operatorname{Im}\Omega(n+\frac{1}{2}\delta)>C}} \exp(\pi i((n+\frac{1}{2}\delta)^t\Omega(n+\frac{1}{2}\delta)+2(n+\frac{1}{2}\delta)^t(z+\frac{1}{2}\epsilon))) \right| \\ &\quad \leq \sum_{\substack{n\in\mathbb{Z}^2 \\ (n+\frac{1}{2}\delta)^t \operatorname{Im}\Omega(n+\frac{1}{2}\delta)>C}} \left| \exp(-\pi(n+\frac{1}{2}\delta)^t \operatorname{Im}\Omega(n+\frac{1}{2}\delta)) \right| \\ &\quad \leq \sum_{m=C}^{\infty} \mu(m)\exp(-\pi m), \end{aligned}$$

where

$$\mu(m) = \#\{n \in \mathbb{Z}^2 : m < (n+\frac{1}{2}\delta)^t \operatorname{Im}\Omega(n+\frac{1}{2}\delta) \leq m+1\}.$$

To approximate the size of $\mu(m)$ we make use of the volume heuristics

$$\mu(m) \approx \frac{\text{Vol }(K_2(m))}{(\min\Omega)^2},$$

where $K_2(m) = \{z \in \mathbb{C}^2 : m \leq \|z\| \leq m+1\}$ and $\min\Omega = \min_{g\in\mathbb{Z}^2}\{g^t(\operatorname{Im}\Omega)g\}$. As a rough estimate we get

$$\text{Vol }(K_2(m)) \leq 7m.$$

Now we have

$$\sum_{m=C}^{\infty} \mu(m)\exp(-\pi m) \approx \frac{7}{(\min\Omega)^2} \sum_{m=C}^{\infty} mx^{-m}, \quad \text{where } x = \exp(\pi).$$

Since the function $f(x) = x\exp(-\pi x)$ is strictly decreasing for a variable $x > 1$, we have

$$\sum_{m=C}^{\infty} mx^{-m} \leq \int_{C-1}^{\infty} mx^{-m}dm.$$

Setting $x = \exp(\pi)$ gives us the following estimate:

$$\begin{aligned}
&\frac{7}{(\min\Omega)^2}\sum_{m=C}^{\infty} mx^{-m} \\
&\quad\le \frac{7}{(\min\Omega)^2}\int_{m=C-1}^{\infty} mx^{-m}dm \\
&\quad= \frac{7}{(\min\Omega)^2}\left((C-1)\frac{\exp(-\pi(C-1))}{\pi} + \frac{1}{\pi^2}\exp(-\pi(C-1)\right) \\
&\quad< \frac{7}{(\min\Omega)^2}\left(\frac{C}{\pi}\exp(-\pi(C-1))\right) < \frac{2.3}{(\min\Omega)^2}\exp(-\frac{3}{4}\pi C).
\end{aligned}$$

The last step uses the inequality

$$C\exp(-\pi(C-1)) < \exp(-\frac{3\pi}{4}C) \quad \text{for } C \ge 7.$$

We get the following condition on C:

$$C > (s + 0.35 - 2\log_{10}(\min\Omega))$$

and

$$C > \frac{1}{2}(s + 0.35 - 2\log_{10}(\min\Omega)) \quad \text{if } C \ge 75.$$

It is clear that a formula for C will always depend on the first successive minima of Ω.

5. From theta constants to Igusa's invariants

Given the value of the 10 even theta characteristics evaluated at the period matrix Ω, we can compute the three j-invariants of the corresponding hyperelliptic curve.

First we define the values h_4, h_{10}, h_{12} and h_{16} coming from modular forms of weight 4, 10, 12 and 16:

$$\begin{aligned}
h_4 &:= \sum_{i=1}^{10}\theta_i^8, \\
h_{10} &:= \prod_{i=1}^{10}\theta_i^2, \\
h_{12} &:= (\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10})^4 + (\theta_1\theta_2\theta_9\theta_6\theta_8\theta_3)^4 + (\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_7)^4 + (\theta_5\theta_2\theta_6\theta_8\theta_3\theta_7)^4 \\
&\quad + (\theta_1\theta_5\theta_2\theta_{10}\theta_3\theta_7)^4 + (\theta_1\theta_9\theta_8\theta_{10}\theta_3\theta_7)^4 + (\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_4)^4 + (\theta_1\theta_5\theta_9\theta_8\theta_3\theta_4)^4 \\
&\quad + (\theta_5\theta_9\theta_6\theta_{10}\theta_3\theta_4)^4 + (\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + (\theta_1\theta_2\theta_9\theta_6\theta_7\theta_4)^4 + (\theta_1\theta_5\theta_6\theta_8\theta_7\theta_4)^4 \\
&\quad + (\theta_2\theta_9\theta_8\theta_{10}\theta_7\theta_4)^4 + (\theta_5\theta_2\theta_9\theta_3\theta_7\theta_4)^4 + (\theta_1\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4,
\end{aligned}$$

$$
\begin{aligned}
h_{16} := {} & \theta_8^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_8\theta_{10})^4 + \theta_5^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_8\theta_3)^4 + \theta_{10}^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_3)^4 \\
& + \theta_3^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_3)^4 + \theta_1^4(\theta_1\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_7)^4 + \theta_2^4(\theta_5\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_7)^4 \\
& + \theta_1^4(\theta_1\theta_5\theta_2\theta_6\theta_8\theta_3\theta_7)^4 + \theta_9^4(\theta_5\theta_2\theta_9\theta_6\theta_8\theta_3\theta_7)^4 + \theta_9^4(\theta_1\theta_5\theta_2\theta_9\theta_{10}\theta_3\theta_7)^4 \\
& + \theta_6^4(\theta_1\theta_5\theta_2\theta_6\theta_{10}\theta_3\theta_7)^4 + \theta_5^4(\theta_1\theta_5\theta_9\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_2^4(\theta_1\theta_2\theta_9\theta_8\theta_{10}\theta_3\theta_7)^4 \\
& + \theta_6^4(\theta_1\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_8^4(\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_{10}^4(\theta_5\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_7)^4 \\
& + \theta_3^4(\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_7)^4 + \theta_7^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_7)^4 + \theta_7^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_3\theta_7)^4 \\
& + \theta_9^4(\theta_1\theta_5\theta_2\theta_9\theta_8\theta_{10}\theta_4)^4 + \theta_6^4(\theta_1\theta_5\theta_2\theta_6\theta_8\theta_{10}\theta_4)^4 + \theta_2^4(\theta_1\theta_5\theta_2\theta_9\theta_8\theta_3\theta_4)^4 \\
& + \theta_6^4(\theta_1\theta_5\theta_9\theta_6\theta_8\theta_3\theta_4)^4 + \theta_1^4(\theta_1\theta_5\theta_9\theta_6\theta_{10}\theta_3\theta_4)^4 + \theta_2^4(\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_3\theta_4)^4 \\
& + \theta_1^4(\theta_1\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_5^4(\theta_5\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_9^4(\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 \\
& + \theta_8^4(\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_{10}^4(\theta_1\theta_5\theta_9\theta_8\theta_{10}\theta_3\theta_4)^4 + \theta_3^4(\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_3\theta_4)^4 \\
& + \theta_5^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_7\theta_4)^4 + \theta_2^4(\theta_1\theta_5\theta_2\theta_6\theta_8\theta_7\theta_4)^4 + \theta_9^4(\theta_1\theta_5\theta_9\theta_6\theta_8\theta_7\theta_4)^4 \\
& + \theta_8^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_7\theta_4)^4 + \theta_1^4(\theta_1\theta_2\theta_9\theta_8\theta_{10}\theta_7\theta_4)^4 + \theta_5^4(\theta_5\theta_2\theta_9\theta_8\theta_{10}\theta_7\theta_4)^4 \\
& + \theta_6^4(\theta_2\theta_9\theta_6\theta_8\theta_{10}\theta_7\theta_4)^4 + \theta_{10}^4(\theta_1\theta_2\theta_9\theta_6\theta_{10}\theta_7\theta_4)^4 + \theta_{10}^4(\theta_1\theta_5\theta_6\theta_8\theta_{10}\theta_7\theta_4)^4 \\
& + \theta_1^4(\theta_1\theta_5\theta_2\theta_9\theta_3\theta_7\theta_4)^4 + \theta_6^4(\theta_5\theta_2\theta_9\theta_6\theta_3\theta_7\theta_4)^4 + \theta_8^4(\theta_5\theta_2\theta_9\theta_8\theta_3\theta_7\theta_4)^4 \\
& + \theta_5^4(\theta_1\theta_5\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_2^4(\theta_1\theta_2\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_9^4(\theta_1\theta_9\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4 \\
& + \theta_8^4(\theta_1\theta_6\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_{10}^4(\theta_5\theta_2\theta_9\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_3^4(\theta_1\theta_2\theta_9\theta_6\theta_3\theta_7\theta_4)^4 \\
& + \theta_3^4(\theta_1\theta_5\theta_6\theta_8\theta_3\theta_7\theta_4)^4 + \theta_3^4(\theta_2\theta_9\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_7^4(\theta_1\theta_5\theta_2\theta_8\theta_{10}\theta_7\theta_4)^4 \\
& + \theta_7^4(\theta_1\theta_5\theta_9\theta_8\theta_3\theta_7\theta_4)^4 + \theta_7^4(\theta_5\theta_9\theta_6\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_7^4(\theta_2\theta_6\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4 \\
& + \theta_4^4(\theta_1\theta_5\theta_2\theta_9\theta_6\theta_{10}\theta_4)^4 + \theta_4^4(\theta_1\theta_2\theta_9\theta_6\theta_8\theta_3\theta_4)^4 + \theta_4^4(\theta_5\theta_9\theta_6\theta_8\theta_{10}\theta_7\theta_4)^4 \\
& + \theta_4^4(\theta_5\theta_2\theta_6\theta_8\theta_3\theta_7\theta_4)^4 + \theta_4^4(\theta_1\theta_5\theta_2\theta_{10}\theta_3\theta_7\theta_4)^4 + \theta_4^4(\theta_1\theta_9\theta_8\theta_{10}\theta_3\theta_7\theta_4)^4.
\end{aligned}
$$

Then we get four invariants I_2, I_4, I_6, I_{10} of weight 2,4,6 and 10:

$$I_2 := \frac{h_{12}}{h_{10}}, \quad I_4 := h_4, \quad I_6 := \frac{h_{16}}{h_{10}}, \quad I_{10} := h_{10}.$$

From these invariants we can deduce absolute invariants j_1, j_2 and j_3. The three j-invariants are rational generators of the field of absolute invariants. Two principally polarized abelian varieties of dimension two are isomorphic if and only if they have the same j-invariants [5]. These are given by

$$j_1 := \frac{I_2^5}{I_{10}}, \quad j_2 := \frac{I_4 I_2^3}{I_{10}}, \quad j_3 := \frac{I_6 I_2^2}{I_{10}}.$$

6. From Igusa's invariants to Mestre's invariants

Since the absolute Igusa invariants j_1, j_2, j_3 are rational generators of the field of invariants, we can write the invariants for Mestre's algorithm in terms of them. Mestre gives formulae (p. 319 of [12]) which make it possible to express the coefficients of the conic and the cubic. We follow Mestre's notation.

Set

$$j_1' = \frac{A^5}{D}, \quad j_2' = \frac{A^3 B}{D}, \quad j_3' = \frac{A^2 C}{D},$$

where A, B, C, D are invariants of degree 2, 4, 6 and 10 given by Mestre. Note that A, B, C, D are not the same as the Igusa invariants I_2, I_4, I_6, Δ. The absolute invariants j_1', j_2', j_3' are also rational generators of $\mathbb{Q}(j_1, j_2, j_3)$.

We obtain the following transformation formulae:

$$j_1' = -\frac{j_1}{120^5}, \quad j_2' = \frac{720 j_1'}{6750} - \frac{j_2}{120^3 \cdot 6750}, \quad j_3' = \frac{j_3}{120^2 \cdot 2025100} + \frac{1080 j_2'}{2025} - \frac{16 j_1'}{375}.$$

Since $\alpha = \frac{D}{\Delta}$ is an absolute invariant, we can find an expression for it in terms of the j_i':

$$\alpha = -\frac{1}{4556250}\left(\frac{1}{j_1'} + 62208\right) + \frac{16 j_2'}{75 j_1'} + \frac{16 j_3'}{45 j_1'} - 2\frac{{j_2'}^2}{3{j_1'}^2} - \frac{4 j_2' j_3'}{3{j_1'}^2}.$$

We normalize Mestre's invariants Q_{ij} and $H_{l_1,\dots,l_3}$ in such a way that they become absolute invariants. For simplicity denote j_i' by j_i. Then

$$\begin{aligned}
Q_{11}' &= \tfrac{Q_{11}}{A^3} = \tfrac{(2j_3 + \frac{1}{3} j_2)}{j_1}, \\
Q_{12}' &= \tfrac{Q_{12}}{A^4} = \tfrac{2}{3}\tfrac{j_2^2 + j_1 j_3}{j_1^2}, \\
Q_{13}' &= Q_{22}' = \tfrac{Q_{13}}{A^5} = \alpha, \\
Q_{23}' &= \tfrac{Q_{23}}{A^6} = \tfrac{1}{j_1^2}(\tfrac{j_2^3}{3j_1} + \tfrac{4 j_2 j_3}{9} + \tfrac{2 j_3^2}{3}), \\
Q_{33}' &= \tfrac{Q_{33}}{A^7} = \tfrac{1}{j_1^2}(\tfrac{j_1 j_2 \alpha}{2} + \tfrac{2 j_2^2 j_3}{9 j_1} + \tfrac{2 j_3^2}{9}), \\
H_{111}' &= \tfrac{H_{111}}{A^5} = \tfrac{2}{9}\tfrac{j_1^2 j_3 - 6 j_1 j_2 j_3 + 9 j_1^2}{j_1^2}, \\
H_{112}' &= \tfrac{H_{112}}{A^6} = \tfrac{1}{9}\tfrac{2 j_2^3 + 4 j_1 j_2 j_3 + 12 j_1 j_3^2 + 3 j_1^2}{j_1^3}, \\
H_{113}' = H_{122}' &= \tfrac{H_{113}}{A^7} = \tfrac{1}{9}\tfrac{j_2^3 + 4/3 j_1 j_2 j_3 + 4 j_2^2 j_3 + 6 j_1 j_3^2 + 3 j_1 j_2}{j_1^3}, \\
H_{123}' &= \tfrac{H_{123}}{A^6} = \tfrac{1}{18 j_1^3} 2\tfrac{j_2^4}{j_1} + 4 j_2^2 j_3 + \tfrac{4 j_1 j_3^2}{3} + 4 j_2 j_3^2 + 3 j_1 j_2 + 12 j_1 j_3, \\
H_{133}' &= \tfrac{H_{133}}{A^7} = \tfrac{1}{18 j_1^3}(\tfrac{j_2^4}{j_1} + \tfrac{4 j_2^2 j_3}{3} + \tfrac{16 j_2^3 j_3}{3 j_1} + \tfrac{26 j_2 j_3^2}{3} + 8 j_3^3 + 3 j_2^2 + 2 j_1 j_3), \\
H_{222}' &= \tfrac{H_{222}}{A^6} = \tfrac{1}{9 j_1^3}(3\tfrac{j_2^4}{j_1} + 6 j_2^2 j_3 + \tfrac{8}{3} j_1 j_3^2 + 2 j_2 j_3^2 - 3 j_1 j_3), \\
H_{223}' &= \tfrac{H_{223}}{A^7} = \tfrac{1}{18 j_1^3}(-\tfrac{2 j_2^3 j_3}{3 j_1} - \tfrac{4 j_2 j_3^2}{3} - 4 j_3^3 + 9 j_2^2 + 8 j_1 j_3), \\
H_{233}' &= \tfrac{H_{233}}{A^8} = \tfrac{1}{18 j_1^3}(\tfrac{j_2^5}{j_1^2} + 2\tfrac{j_2^3 j_3}{j_1} + \tfrac{8}{9} j_2 j_3^2 + \tfrac{2 j_2^2 j_3^2}{3 j_1} - j_2 j_3 + 9 j_1), \\
H_{333}' &= \tfrac{H_{333}}{A^9} = \tfrac{1}{36 j_1^3}(-2\tfrac{j_2^4 j_3}{j_1^2} - 4\tfrac{j_2^2 j_3^2}{j_1} - \tfrac{16}{9} j_3^3 - \tfrac{4 j_2 j_3^3}{j_1} + 9\tfrac{j_2^3}{j_1} + 12 j_2 j_3 + 20 j_3^2).
\end{aligned}$$

From now on, we write Q_{ij} and H_{ijk} instead of Q_{ij}' and H_{ijk}'.

7. Mestre's algorithm for finite prime fields

For the idea of the algorithm and its correctness for an arbitrary field K, see Mestre's article [12].

We give here an explicit formulation if K is a finite prime field.

Suppose we have the three j-invariants $\tilde{j}_1, \tilde{j}_2, \tilde{j}_3$ modulo p. Then we get Mestre's invariants

$$Q_{11}, Q_{12}, Q_{13} = Q_{22}, Q_{23}, Q_{33}$$

and

$$H_{111}, H_{112}, H_{113}, H_{123}, H_{133}, H_{222}, H_{223}, H_{233}, H_{333},$$

which are the coefficients of a conic

$$\sum_{1\le i\le j\le 3} Q_{ij}x_ix_j,$$

resp. a cubic

$$\sum_{1\le i\le j\le k\le 3} H_{ijk}x_ix_jx_k.$$

We would like to parametrize the conic so that the set of solutions is given by

$$(f_1(t), f_2(t), f_3(t)).$$

For this we transform the conic into a normal form

$$Q'_{11}x_1^2 + Q'_{22}x_2^2 + Q'_{33}x_3^2. \tag{2}$$

We can then parametrize the new conic Q' and finally get a parametrization $(f_1(t), f_2(t), f_3(t))$ of the conic Q itself.

We plug the solution into the cubic

$$\sum_{i\le j\le k} H_{ijk}f_i(t)f_j(t)f_k(t)$$

to get the model of the hyperelliptic curve

$$y^2 = \sum_{i\le j\le k} H_{ijk}f_i(t)f_j(t)f_k(t) =: f(t).$$

The polynomial $f(t)$ has degree six. Suppose we would like to apply Cantor's algorithm. Then we need a monic polynomial of degree 5. The hyperelliptic function field given by

$$C_f : y^2 = f(t), \quad \deg f = 6,$$

has a model defined over $\mathbb{F}_p$

$$C_g : y^2 = g(t), \quad \deg g = 5,$$

if and only if the curve C_f has an $\mathbb{F}_p$-rational Weierstrass point. Simply speaking this means that $f(t)$ has a zero in $\mathbb{F}_p$. By a projective transformation we move the $\mathbb{F}_p$-rational Weierstrass point to infinity and obtain a polynomial of degree five.

We can compute the probability that a polynomial of degree 6 whose discriminant is not equal to zero has an $\mathbb{F}_p$-rational point. It is given by

$$\frac{-24p - 3p^3 + 10p^2 + 91p^6 + 43p^4 - 117p^5}{144(p^6 - p^5)}.$$

The complete algorithm is now given as follows:

Computing the curve from its j-invariants

Input: $j_1, j_2, j_3 \in \mathbb{F}_p$

Output: A hyperelliptic curve of the form $y^2 = f(t)$, where $f(t) \in \mathbb{F}_p[t]$, $\deg(f) =$ 5 or 6.

1: Compute Mestre's invariants Q_{ij}, H_{ijk} from the j-invariants $j_i, i = 1, 2, 3$.
2: Parametrize the conic (Q_{ij}) by $f_1(t), f_2(t), f_3(t)$.
3: Obtain $f(t) := \sum_{i\le j\le k} H_{ijk}f_i(t)f_j(t)f_k(t) \in \mathbb{F}_p[t]$.

4: Transform f into a polynomial of degree 5 if possible.
5: Return $y^2 = f(t)$.

8. Good Weil numbers

In this section we describe how to find a suitable prime p such that

$$w\overline{w} = p, \tag{3}$$

for $w \in \mathcal{O}_K$. The equation (3) is a relative norm equation with respect to the relative field extension K/K_0. Thus we could choose random primes and try to solve the relative norm equation by applying the function <bnfisintnorm> provided by the PARI library to p^2. The primes so found are of the most general form, but the method needs heavier machinery (e.g., class groups) and is more difficult to implement than the algorithm we discuss in this section. Our method finds only two possibilities for the group order. For applications this is sufficient.

We assume that the Frobenius w is an element in $\mathcal{O} = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$, where $\eta = i\sqrt{a + b\sqrt{d}}$, resp. $\eta = i\sqrt{a + b(\frac{-1+\sqrt{d}}{2})}$. The order $\mathcal{O}$ might not be the maximal order $\mathcal{O}_K$. Let D be the discriminant of K_0.

First we consider $D \equiv 0 \mod 4$. Set $p = w\overline{w}$ and

$$w = c_1 + c_2\sqrt{d} + (c_3 + c_4\sqrt{d})i\sqrt{a + b\sqrt{d}}.$$

We obtain two equations for c_1, c_2, c_3 und c_4:

$$\begin{aligned} c_1^2 + c_2^2 d + c_3^2 a + c_4^2 ad + 2c_3c_4bd &= p, \\ 2c_1c_2 + 2c_3c_4a + c_3^2 b + c_4^2 bd &= 0. \end{aligned}$$

From this we deduce the following algorithm:

Good Weil numbers, $D \equiv 0 \mod 4$

Input: CM-field $K = \mathbb{Q}(i\sqrt{a + b\sqrt{d}})$.
Output: A prime p that satisfies a relative norm equation and the two possible group orders.

1: Choose c_3, c_4 at random,[1] $(c_3, c_4) = 1$.
2: **if** $c_3^2 b - c_4^2 db \not\equiv 0 \mod 2$ **then**
3: Start again.
4: **end if**
5: Set $2n := -2c_3c_4a - c_3^2 b - c_4^2 bd$.
6: Set $c_1 := q$ where $q \mid n$.
7: $c_2 := n/q$;
8: $p := c_1^2 + c_2^2 d + c_3^2 a + c_4^2 da + 2c_3c_4bd$;
9: **if** p is not prime **then**
10: Start again.
11: **end if**
12: Set possible group order $(p+1)^2 \pm 4(p+1)c_1 + 4(c_1^2 - c_2^2 d)$.

The algorithm for $D \equiv 1 \mod 4$ is based on the same idea.

[1] If c_3, c_4 have approximately n digits then p will have around $2n$ digits.

Good Weil numbers, $D \equiv 1 \mod 4$

Input: CM-field $K = \mathbb{Q}(i\sqrt{a + b(\frac{-1+\sqrt{d}}{2})})$.

Output: A prime p that satisfies a relative norm equation and the two possible group orders.

1: Choose c_3, c_4 at random, $(c_3, c_4) = 1$.
2: $n := 2c_3c_4a - c_4^2a + c_3^2b - 2c_3c_4b + (\frac{d+3}{4})bc_4^2$;
3: **if** $n \mod 4 \equiv 2$ **then**
4: Start again.
5: **end if**
6: **if** n even **then**
7: $c_2 :=$ even factor of n;
8: **else**
9: $c_2 :=$ odd factor of n;
10: **end if**
11: $c_1 := \frac{1}{2}(-\frac{n}{c_2} + c_2)$;
12: $p := c_1^2 + c_2^2(\frac{d-1}{4}) + c_3^2a + c_4^2a(\frac{d-1}{4}) + 2c_3c_4b(\frac{d-1}{4}) - bc_4^2(\frac{d-1}{4})$;
13: **if** p is not prime **then**
14: Start again.
15: **end if**
16: Set possible group order $(p+1)^2 \pm (p+1)(4c_1 - 2c_2) + 4(c_1^2 - c_1c_2 + c_2^2(\frac{1-d}{4}))$.

Note that this elementary method needs the factorization of an integer in step 6. It is not advisable to factor the integer completely. Much faster is a trial factorization up to a fixed bound. Table 1 shows the time (in seconds) to find 1000 primes of size approximately 2^{80} satisfying a relative norm equation.

TABLE 1.

CM-field	elementary programm	use of <bnfisintnorm>
$\mathbb{Q}(i\sqrt{2+\sqrt{2}})$	247	296
$\mathbb{Q}(i\sqrt{3+\sqrt{2}})$	256	371
$\mathbb{Q}(i\sqrt{4+\sqrt{2}})$	252	394
$\mathbb{Q}(i\sqrt{29+6\sqrt{23}})$	302	403
$\mathbb{Q}(i\sqrt{3+\frac{-1+\sqrt{5}}{2}})$	243	328
$\mathbb{Q}(i\sqrt{4+\frac{-1+\sqrt{5}}{2}})$	241	424
$\mathbb{Q}(i\sqrt{5+\frac{-1+\sqrt{5}}{2}})$	240	429
$\mathbb{Q}(i\sqrt{55+4\frac{-1+\sqrt{53}}{2}})$	285	378
$\mathbb{Q}(i\sqrt{6+\frac{-1+\sqrt{73}}{2}})$	263	424
$\mathbb{Q}(i\sqrt{6+\frac{-1+\sqrt{89}}{2}})$	268	197
$\mathbb{Q}(i\sqrt{7+\frac{-1+\sqrt{101}}{2}})$	257	303
$\mathbb{Q}(i\sqrt{6+\frac{-1+\sqrt{113}}{2}})$	266	435
$\mathbb{Q}(i\sqrt{9+\frac{-1+\sqrt{141}}{2}})$	292	356

9. The complete algorithm

Now we are able to give the complete algorithm.

Before starting with the construction of a hyperelliptic curve we have to fix a CM-field, and we have to find a suitable prime field $\mathbb{F}_p$.

Precomputations for the group order

1: Choose a CM-field $K = \mathbb{Q}\left(i\sqrt{a+b\sqrt{d}}\right)$.
2: Find a prime p such that there exists $w \in K$ with $w\overline{w} = p$.
3: Compute the two (resp. four) possible group orders n_1, n_2 (n_3, n_4) depending on p and $\mathcal{O}_K$.
4: **if** n_1 and n_2 (resp. n_3 and n_4) have no large prime factor **then**
5: Go to 2.
6: **else**
7: Return K, p, n_1 and n_2.
8: **end if**

Once we have found a CM-field K and a suitable prime p, we are left with the task of finding a hyperelliptic curve defined over $\mathbb{F}_p$ having complex multiplication by the order $\mathcal{O}_K$.

Construction of hyperelliptic curves suitable for cryptography

Input: CM-field K, $h_{K_0} = 1$, prime p and the two (sometimes four) possible group orders n_1 and n_2 (resp. n_3, n_4).

Output: A hyperelliptic curve of the form $y^2 = f(t)$, where $f(t) \in \mathbb{F}_p[t]$, $\deg(f) =$ 5 or 6.

1: Choose a complete set (up to isomorphism) of period matrices Ω_i of all simple principally polarized abelian varieties having complex multiplication by $\mathcal{O}_K$ (see Section 3). Let s be the size of the set of isomorphism classes.
2: Compute all even theta constants

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (\Omega_i, 0) = \sum_{n \in \mathbb{Z}^2} \exp(\pi i (n + \frac{1}{2}\delta)^t \Omega_i (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^t (\frac{1}{2}\epsilon)).$$

See Section 4.
3: Compute the $3s$ generating j-invariants

$$j_1^{(i)},\ j_2^{(i)},\ j_3^{(i)}, \quad i = 1, \ldots, s.$$

4: Compute the class polynomials

$$H_1(X) = \prod_{i=1}^{s} (X - j_1^{(i)}), \quad H_2(X) = \prod_{i=1}^{s} (X - j_2^{(i)}), \quad H_3(X) = \prod_{i=1}^{s} (X - j_3^{(i)}).$$

5: Find the denominator (see Remark 9.1) and get the polynomials $H_i'(X) \in \mathbb{Z}[X]$.
6: **for** all (a_1, a_2, a_3), a_i zero of $H_i'(X) \mod p$ **do**
7: Set

$$j_1 := a_1; \quad j_2 := a_2; \quad j_3 := a_3.$$

8: Compute Mestre's invariants (see Section 6).
9: Apply Mestre's algorithm to get a curve

$$C : y^2 = f(t), \quad f(t) \in \mathbb{F}_p[t], \quad \deg f(t) = 6.$$

10: **if** $\#J(C) = n_1$ or n_2 **then**
11: Return C;

12: **end if**
13: **end for**

Remark 9.1. 1. The algorithm is restricted to CM-fields whose real subfield has class number one. This ensures that the ideals in $\mathcal{O}_K$ have a relative integer basis with respect to $\mathcal{O}_{K_0}$. Therefore it is possible to give period matrices of the principally polarized abelian varieties with complex multiplication by $\mathcal{O}_K$ (see Theorem 3.1).

2. For step 5 of the algorithm we applied the continued fraction algorithm to the second highest coefficient of the polynomial to obtain a possible denominator $d_{K,H_i(X)}$. This method gives us almost always a polynomial in $\mathbb{Z}$ which is not necessarily primitive.

   There exist exceptions, e.g.,

$$K = \mathbb{Q}\left(i\sqrt{5 + \frac{-1+\sqrt{13}}{2}}\right),$$

   where the denominator of the polynomial $H_1(X)$ contains an additional power of three, i.e., 3^2.

3. In contrast to elliptic curves, where the class polynomial always splits into linear factors, the class polynomials $H_i(X)$ do not have to split into linear factors even when p satisfies a relative norm equation. For the correctness of our method it is only important that $H_i(X)$ have a linear factor modulo p. This is a consequence from class field theory.

   It is even more efficient to take primes which do not split completely, since the for-loop in step 6 takes fewer rounds in this case.

Example 9.2. Consider the CM-field $\mathbb{Q}(i\sqrt{3+\sqrt{2}})$ and the prime

$$p = 907978164842524484436193557995633106029.$$

Each of the class polynomials $H_1(X)$, $H_2(X)$ and $H_3(X)$ splits into one factor of degree two and two factors of degree one.

The two linear factors give us hyperelliptic curves defined over $\mathbb{F}_p$, and the irreducible factor of degree two leads to curves defined over $\mathbb{F}_{p^2}$.

10. Complexity of the algorithm

10.1. **Analysis.** The algorithm falls into two parts:

1. Computation of the class polynomial.
2. Mestre's algorithm.

The running time of the first part is dominated by the computation of the theta constants. In Section 4 we saw that the computation of the theta constants depends on the value of the first successive minima of the period matrix. An exact analysis is therefore rather difficult.

However, since we cannot compute up to arbitrarily high precision, the number of CM-fields we consider is restricted (see also Section 13). In principle we could compute all possible class polynomials in advance.

Table 2 will give an idea about the complexity of the computation of the class polynomials. The first three columns describe the CM-field K

$$\mathbb{Q}\left(i\sqrt{a+b\sqrt{d}}\right), \quad d=\frac{D}{4}, \qquad \text{if } D\equiv 0 \mod 4,$$

$$\mathbb{Q}\left(i\sqrt{a+b\frac{-1+\sqrt{d}}{2}}\right), \quad d=D, \qquad \text{if } D\equiv 1 \mod 4.$$

The fourth column gives the class number of K and the fifth the number of possible polarizations. Note that in all these cases h_K (#Pol) is the degree of the class polynomial.

Recall that the monic class polynomial has rational coefficients. The sixth column gives the number of decimal digits of the denominator of the second highest coefficient of the class polynomial. The seventh column gives the precision which is necessary for the computations to get the right result. The eighth column gives the time in seconds.

Some of the CM-fields are taken from the tables in [15] and [11]. We were able to compute the class polynomial of a CM-fields of class number 10.

The second part is the application of Mestre's algorithm. First we have to factor the class polynomial. There exists an efficient probabilistic algorithm [3] which takes

$$O(n^{2+\epsilon}+n\log p)$$

operations in $\mathbb{F}_p$, where n is the degree of the polynomial. In our situation the degree of the polynomial is bounded and small. So we can estimate the number of operations in $\mathbb{F}_p$ by $O(\log p)$. Note that we have to apply Mestre's algorithm s^3 times, where s is the degree of the class polynomial. In most cases s equals $2h_K$. Especially we have to compute s^3 scalar multiplications on a hyperelliptic Jacobian. Every scalar multiplication takes

$$O(g^2\log p)$$

field operations (see [16] for the complexity of a single composition on a hyperelliptic Jacobian). Thus as an overall complexity (once the class polynomial is computed) we get

$$O((2h_K)^3\log p)$$

operations in $\mathbb{F}_p$.

TABLE 2.

CM-field							
D	**a**	**b**	h_K	# pol.	denom. dec. digits	prec.	time (in s.)
5	3	1	1	1	1	20	1
5	4	1	2	2	11	50	1
5	7	1	1	2	1	20	1
5	6	2	2	1	13	100	1
5	8	1	4	2	23	100	18

TABLE 2. (Continued)

CM-field							
D	**a**	**b**	h_K	# pol.	denom. dec. digits	prec.	time (in s.)
5	16	7	4	2	59	200	52
5	23	5	1	2	52	100	3
5	91	52	2	1	50	150	3
5	35	8	5	2	29	400	81
5	18	6	4	1	73	400	35
8	2	1	1	1	1	20	1
8	3	1	2	2	3	50	1
8	6	1	4	2	17	200	23
8	13	4	2	2	42	200	7
8	13	6	3	2	4	100	2
8	15	4	5	2	4	300	71
8	23	8	7	2	22	500	568
12	11	4	4	2	4	100	8
13	3	1	2	2	1	50	1
13	6	2	2	2	16	150	9
13	8	3	1	1	1	20	1
13	16	3	1	2	30	100	1
17	9	1	4	1	22	100	6
17	6	1	4	2	38	200	16
21	5	1	4	2	45	300	51
24	17	6	6	2	16	600	401
28	7	2	4	2	12	150	10
29	7	2	4	2	24	200	31
29	24	7	4	2	7	150	20
33	95	28	4	2	40	200	27
37	19	5	3	2	9	100	16
37	26	7	3	2	33	200	90
41	10	2	4	2	8	150	14
44	67	20	4	2	22	200	26
53	55	4	1	1	33	100	1
56	53	14	2	2	33	100	3
57	9	2	2	2	6	100	3
61	9	2	2	2	30	100	2
69	5	1	4	2	21	200	292
73	6	1	4	2	13	150	20
73	5	1	1	2	11	50	1
76	279	64	4	2	8	150	152
88	5	1	2	2	37	150	4
89	11	2	4	2	25	300	83
92	29	6	4	2	26	200	216
92	77	16	2	2	31	200	20
97	8	1	3	2	11	100	8
101	7	1	3	2	1	100	7
109	9	1	1	2	5	20	1
124	39	7	4	2	40	200	310
124	23	4	2	2	19	150	3
129	13	2	4	2	37	200	82
137	10	1	4	2	33	300	532
141	9	1	2	2	35	300	44
233	10	1	1	2	27	50	1
389	114	11	1	2	50	100	2

10.2. **Notes on implementation.** The two parts of the algorithm differ not only in the complexity but also in the difficulty of the implementation.

For the first part we need a library that supports computations in relative number fields. Most suitable for this task is the C-library PARI (`ftp://megrez.math.u-bordeaux.fr/pub/pari/`).

The second part is easier to implement. It requires efficient polynomial arithmetic. We used the library NTL written in C++ (`http://www.shoup.net/ntl/`).

11. Statistics

11.1. **Primes interesting for implementations.** Some primes are especially well suited for implementions (see [6], [20]). In Table 3 we give a list of Mersenne primes and generalized Mersenne primes. We tested whether they split in a given CM-field or not, and whether the corresponding group order contains a large prime factor.

Table 3.

D	a	b	prime	k, group order equals $k \cdot q, q$ prime
5	6	2	$2^{89}-1$	580
			$2^{130}-5$	4
5	16	7	$2^{150}-3$	64
5	18	7	$2^{192}-2^{64}-1$	1
			$2^{224}-2^{96}+1$	1
5	11	1	$2^{96}-2^{32}+1$	151
			$2^{116}-3$	59
			$2^{113}-3$	11
5	19	4	$2^{107}-1$	16
5	23	5	$2^{224}-2^{96}+1$	109
			$2^{127}-1$	1
8	5	2	$2^{89}-1$	188
8	6	3	$2^{96}-2^{32}+1$	32
8	13	6	$2^{116}-3$	4
8	19	8	$2^{213}-3$	167
13	5	1	$2^{192}-2^{64}-1$	816
13	6	2	$2^{150}-3$	16
13	11	4	$2^{116}-3$	13
13	75	20	$2^{127}-1$	859
17	3	1	$2^{107}-1$	64
17	27	8	$2^{107}-1$	1
21	15	4	$2^{118}-3$	1, 67
24	3	1	$2^{174}-3$	800
28	7	2	$2^{127}-1$	300
29	15	4	$2^{107}-1$	647
37	19	5	$2^{107}-1$	747
37	26	7	$2^{96}-2^{32}+1$	511

TABLE 3. (Continued)

D	a	b	prime	k, group order equals $k \cdot q, q$ prime
41	6	1	$2^{174}-3$	100
44	4	1	$2^{94}-3$	16
			$2^{174}-3$	280
44	7	2	$2^{94}-3$	14
53	7	1	$2^{192}-2^{64}-1$	1
61	67	12	$2^{94}-3$	25
89	6	1	$2^{127}-1$	136
129	13	2	$2^{96}-2^{32}+1$	20
149	7	1	$2^{192}-2^{64}-1$	7
269	9	1	$2^{94}-3$	16

11.2. **Probability of the group order's being almost prime.** For every CM-field given in Table 4 we chose 5001 primes of the size 2^{80} that satisfy a relative norm equation, and determined the two corresponding group orders.

We counted the number of group orders which are of the form

$$k \cdot q_{prime}$$

where $k = 1, \ldots, 9$, $k \leq 1000$ and $k > 1000$. The first column gives the parameter D, a, b of the CM-field.

The CM-field imposes some divisibility conditions on the group order. In the case where $\mathcal{O}_K = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0}$ with a purely imaginary element $\eta \in \mathcal{O}_K$, the group order can easily be seen to be a multiple of 4.

It is possible to generalize the heuristics from [7], p. 162, on the probability of prime group order to hyperelliptic curves with complex multiplication. This requires more theoretical background, and will be covered by the author in a forthcoming paper.

TABLE 4.

CM-field	1	2	3	4	5	6	7	8	9	10	$11-1000$	>1000
5, 6, 2	0	0	0	130	0	0	0	0	0	0	431	9439
5, 35, 8	135	0	0	0	94	0	0	0	0	0	421	9350
8, 3, 1	0	0	0	0	0	0	0	93	0	0	374	9533
8, 5, 2	0	0	0	147	0	0	0	0	0	0	431	9424
8, 6, 1	0	0	0	149	0	0	0	0	0	0	438	9458
13, 3, 1	0	0	0	52	0	0	0	0	0	0	365	9583
13, 8, 3	47	0	0	0	0	0	0	0	106	0	397	9450
13, 5, 1	55	0	99		0	0	0	0	75	0	360	9411
13, 7, 1	0	0	0	62	0	0	0	0	0	0	407	9531
13, 75, 20	170	0	0	0	0	0	0	0	37	0	448	9345
13, 16, 6	0	0	0	237	0	0	0	0	0	0	464	9299
13, 11, 4	57	0	90	0	0	0	0	0	71	0	378	9404
17, 11, 4	0	0	0	60	0	0	0	67	0	0	427	9446
17, 6, 1	0	0	0	0	0	0	0	108	0	0	436	9458
17, 147, 56	183	0	0	139	0	0	0	0	0	0	441	9237

TABLE 4. (Continued)

CM-field	1	2	3	4	5	6	7	8	9	10	$11-1000$	>1000
$21,5,1$	0	0	0	59	0	0	0	0	0	0	423	9520
$21,7,1$	34	0	52	0	24	0	11	0	42	0	394	9443
$21,22,7$	60	0	81	0	15	0	0	0	85	0	369	9390
$21,15,4$	112	0	0	0	78	0	39	0	9	0	395	9367
$28,7,2$	0	33	0	24	0	24	0	14	0	0	421	9484
$29,7,2$	0	0	0	55	0	0	0	0	0	0	328	9617
$29,5,1$	92	0	0	0	51	0	31	0	0	14	441	9373
$29,17,5$	160	0	0	0	0	0	105	0	0	0	406	9329
$29,24,7$	70	0	0	0	50	0	55	0	0	0	392	9433
$29,12,3$	76	0	0	0	51	0	31	0	7	0	390	9447
$29,4,1$	0	0	0	163	0	0	0	0	0	0	405	9434
$33,7,2$	0	0	0	0	0	0	0	116	0	0	325	9559
$33,95,28$	0	0	0	31	0	0	0	41	0	0	392	9538
$37,43,12$	134	0	0	0	0	0	97	0	36	0	401	9332
$44,67,20$	0	0	0	125	0	0	0	0	0	0	383	9492

12. EXAMPLES

12.1. **Complex multiplication by $\mathbb{Q}\left(i\sqrt{8+\frac{-1+\sqrt{5}}{2}}\right)$.** We would like to construct a hyperelliptic curve whose Jacobian has complex multiplication by

$$K = \mathbb{Q}\left(i\sqrt{8+\frac{-1+\sqrt{5}}{2}}\right).$$

Note that K is not Galois and has class number four. The fundamental unit of the real quadratic subfield $K_0 = \mathbb{Q}(\sqrt{5})$ has negative norm.

A relative integral basis for the elements in the class group is given by

$$\begin{aligned}
\mathfrak{A}_1 &= \mathcal{O}_K = \mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0},\\
\mathfrak{A}_2 &= (-3 + (\frac{-1+\sqrt{5}}{2})\eta)\mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0},\\
\mathfrak{A}_3 &= (-2 + (1 + \frac{-1+\sqrt{5}}{2})\eta)\mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0},\\
\mathfrak{A}_4 &= (-6 + (3 + \frac{-1+\sqrt{5}}{2})\eta)\mathcal{O}_{K_0} + \eta\mathcal{O}_{K_0},
\end{aligned}$$

where

$$\eta = i\sqrt{8+\frac{-1+\sqrt{5}}{2}}.$$

We get a representation system of eight principally polarized abelian varieties of dimension two. For each period matrix we compute the theta constants and the invariants. All computations are done with a precision of 300 decimal digits.

We obtain the class polynomials $H_1(X), H_2(X), H_3(X)$. The three denominators are

$$3^5 \cdot 11^6 \cdot 13^{12}, \quad 3^3 \cdot 11^4 \cdot 13^8, \quad 3^4 \cdot 11^4 \cdot 13^8.$$

We find the polynomials in $\mathbb{Z}[x]$ (due to the size of the coefficients of the first class polynomial we resrict ourselves to giving only the second and third polynomial):

$$\mathbf{H_2}(\mathbf{X})=3^{12}11^{14}13^{16}X^8-27779096536726653818950674601921971890292396045107400000X^7$$
$$+34672003697016486452063399964783605302100193177232773160239750\cdot10^8\,X^6$$
$$-32393589217364753187070921239998417329427407217352309430460575015087 5\cdot10^{12}\,X^5$$
$$-20937218837950194113220127645766807032084298552951292629623998156594664062 5\cdot10^{13}\,X^4$$
$$+60328862534042250738888759108177266596764793474073820503982476246403251953125\cdot10^{18}\,X^3$$
$$-23401670525368589438056194761028013754319187493140282305720285857951319396972656 25\cdot10^{20}\,X^2$$
$$+10534734530981451514686210390116015034972538307090387952047745813541389450073242187 5\cdot10^{24}X$$
$$-2^{24}5^{45}89^2\cdot641^3\cdot12430422901047449^3\cdot8731^3,$$

$$\mathbf{H_3}(\mathbf{X})=3^{16}11^{14}13^{16}X^8-72949208300907821495446956308249521633137016239813170400 0X^7$$
$$+23524716248435960582740582773938197268249860704648447505445184960000 00X^6$$
$$-71218305684149496286946881803653284792882757196034826882826448665436742400000000 0X^5$$
$$-25267786282031848740770903958680953436532962430224953814936073275890940167 04\cdot10^{12}\,X^4$$
$$+14941533087767712082498571768065821556986226021420177995979460702475204327304 96\cdot10^{16}\,X^3$$
$$-15876116697434291742784135808288779379055520791250608382580754703680686073542464\cdot10^{21}\,X^2$$
$$+23164020191801095074104651385789073435984564596801530594058579619355152605422172 16\cdot10^{24}\,X$$
$$-23012781609506842725673828687577347694671831242090585258325545018791489860135799168\cdot10^{27}.$$

A suitable prime is given by $p = 1298992167307454227473799805 09$. It will give us the two possible group orders:

$$168738065072611715566249610176939686572799166162350239634 76$$

and

$$168738065072611715532456868031381666107802482769488055355 16.$$

Note that

$$\begin{aligned} n &= 168738065072611715566249610176939686572799166162350239634 76 \\ &= 4 \cdot q_{prime}, \end{aligned}$$

where q_{prime} is a prime number.

Applying Mestre's algorithm, we find the following curve C over $\mathbb{F}_p$:

$$\begin{aligned} C : y^2 = t^5 &+ 1108540658589940613910785602 11t^4 \\ &+ 52690279977948565928475983553t^3 \\ &+ 81016668528840831602117585943t^2 \\ &+ 43842353021798749401773327333t \\ &+ 84554758087342364918400819975. \end{aligned}$$

The Jacobian of C has exactly n elements.

12.2. **Complex multiplication by $\mathbb{Q}\left(i\sqrt{3+\sqrt{7}}\right)$.** We consider the CM-field $\mathbb{Q}\left(i\sqrt{3+\sqrt{7}}\right)$, which has class number two and two polarizations.

The class polynomials $H_1(X)$, $H_2(X)$ and $H_3(X)$ are given by

$$\begin{aligned}
\mathbf{H_1(X)}&=X^4-2130771672X^3+19850297943250 5408X^2\\
&\quad+67287241032943472939335 68X-53021793091704 99300715659264,\\
\mathbf{H_2(X)}&=4X^4-236549430X^3+1322300792925225X^2\\
&\quad-10889814068091756720 00X-63020475598926822336 0000,\\
\mathbf{H_3(X)}&=64X^4-1045893528X^3+1368605510700597X^2\\
&\quad+25217643676092277219 2X+10734474282651295628544.
\end{aligned}$$

A suitable prime is given by $p = 58094331481464218131068859646359 3$. It will give us the two possible group orders:

$$n_1 = 337495135027824453733283789094149750817279621391373902756574895952,$$
$$n_2 = 337495135027824453733281165453395182011292833807497899521740278848.$$

Note that

$$n_1 = 16 \cdot q_{prime},$$

where q_{prime} is a prime number.

The curve which corresponds to the group order n is given by

$$\begin{aligned}
C : y^2 = t^5 &+ 47472759658621103428440184585078 5t^4\\
&+ 31474823459647441873958033995764 8t^3\\
&+ 31474076653298434619192952799340 9t^2\\
&+ 57439798836119065894404356378001 8t\\
&+ 54622869385947037941877059359468 7.
\end{aligned}$$

13. Discussion

In this section we discuss some further improvements and generalizations of the CM-method, as well as the computational limits.

First we would like to mention an idea of van Wamelen to speed up the computation of the theta constants. He suggests in [22] to apply generators of the group $Sp_2(\mathbb{Z})$ to the period matrix Ω_i in order to maximize the first successive minima of Ω_i.

We would like to mention that our method does not work for fields of small characteristic. Let C be a hyperelliptic curve defined over a finite field whose absolute invariants lie in $\mathbb{F}_q$ where $q = p^n$. Now suppose C has complex multication by $\mathcal{O}_K$ and $\mathcal{O}_K$ has two polarizations. It can easily be seen that $n \leq 2h_K$. Thus in order to get a large extension degree we need a large class number, which is not possible. But we can use the algorithm for fields where $n > 1$ is small.

A strong limitation of the CM-method is the fact that in general the invariants are not integers. As a consequence the class polynomial has rational coefficients. If the parameters chosen are not too big, the denominator can be found. This is the reason why our method works at all. But the denominators increase with the discriminant of the CM-field. It turns out that this makes our method infeasible if the class number gets too large.

TABLE 5.

D	a	b	degree	denominator
5	12	1	12	$13^8 19^8 23^8 47^8 71^8 103^8$
5	12	2	12	$2^2 7^8 13^8 23^8 59^8 83^8$
5	14	6	12	$3^1 917^{12} 59^{12}$
5	20	1	12	$3^5 5^6 7^8 11^8 31^8 37^8 41^8 47^8 101^8$
8	13	1	12	$23^8 43^8 59^8 71^8 79^8 83^8$
29	13	1	10	$17^{12} 19^{12} 29^{12} 47^{12} 61^{12}$

For demonstration we list a few CM-fields with class number 5 and 6 and the denominator of $H_1(X)$ in Table 5.

APPENDIX

This algorithm is a generalization of (3.15) in [17].

Given a symmetric matrix $A \in \mathbb{R}^{k^2}$, a fixed vector $\epsilon \in (\mathbb{R}^+)^k$ and a constant $C \in \mathbb{R}$, it finds the set of vectors $x \in \mathbb{Z}^k$ such that

$$(x+\epsilon)^t A(x+\epsilon) \leq C. \tag{4}$$

First we compute an upper triangular matrix $(q_{ij}) \in \mathbb{R}^{k^2}$ with the property

$$x^t A x = \sum_{i=1}^{k} q_{ii} \left(x_i + \sum_{j=i+1}^{k} q_{ij} x_j \right)^2$$

for all $x \in \mathbb{R}^k$. For this algorithm, see [17].

For all $x \in \mathbb{Z}^k$ which satisfy the condition (4) we have, for $k \geq i \geq 1$,

$$\begin{aligned} & q_{ii}((x_i+\epsilon_i) + \sum_{j=i+1}^{k} q_{ij}(x_j+\epsilon_j))^2 \\ & \quad \leq C - \sum_{\nu=i+1}^{k} q_{\nu\nu}((x_\nu+\epsilon_\nu) + \sum_{j=\nu+1}^{k} q_{\nu j}(x_j+\epsilon_j))^2 =: T_i. \end{aligned}$$

Thus for $x_k \in \mathbb{Z}$ with

$$\begin{aligned} |x_k| &\leq (c/q_{kk})^{\frac{1}{2}} - \epsilon_k, \text{ if } x_k \text{ is positive,} \\ |x_k| &\leq (c/q_{kk})^{\frac{1}{2}} + \epsilon_k, \text{ if } x_k \text{ is negative,} \end{aligned}$$

we try to find all possiblities for x_{k-1}.

For a fixed $x_{i+1}, \ldots, x_k \in \mathbb{Z}$, where

$$\sum_{\nu=i+1}^{k} q_{\nu\nu}(x_\nu + \epsilon_\nu) + \sum_{j=\nu+1}^{k} (q_{\nu j}(x_j + \epsilon_j))^2 \leq T_{i+1},$$

we obtain all possiblities for x_i by

$$-(T_i/q_{ii})^{\frac{1}{2}} - U_i - \epsilon_i \leq x_i \leq (T_i/q_{ii})^{\frac{1}{2}} - U_i - \epsilon_i,$$
$$\text{where } U_i := \sum_{j=i+1}^{k} q_{ij}x_j \text{ for } k-1 \geq i \geq 1.$$

We get the following algorithm:

Finding all solutions $x \in \mathbb{Z}^k$ to $Q(\mathbf{x}+\epsilon) \leq C$

Input: Matrix (q_{ij}), constant C, vector $\epsilon \in (\mathbb{R}^+)^k$.
Output: $\mathbf{x} \in \mathbb{Z}^k$, $\mathbf{x} \neq 0$, where $Q(\mathbf{x}+\epsilon) \leq C$

Let T_i, U_i, x_i and $OS(x_i)$ be vectors of dimension k.
$i := k; T_i := C; U_i := 0;$
while $i \leq k$ **do**
  bool_value := TRUE;
  $Z := (T_i/q_{ii})^{\frac{1}{2}}$;
  $OS(x_i) := \lfloor Z - U_i - \epsilon_i \rfloor$;
  $x_i := \lceil -Z - U_i - \epsilon_i \rceil - 1$;
  while bool_value = TRUE AND $i \leq$k **do**
    $x_i := x_i + 1$;
    if $(x_i \leq OS(x_i))$ **then**
      if i=1 **then**
        Output x;
      else
        $i := i - 1$;
        $U_i := \sum_{j=i+1}^{k} q_{ij}(x_j + \epsilon_j)$;
        $T_i := T_{i-1} - q_{i+1,i+1}(x_{i+1} + \epsilon_{i+1} + U_{i+1})$;
        bool_value := FALSE;
      end if
    else
      $i := i + 1$;
    end if
  end while
end while

Acknowledgments

I thank my supervisor Professor G. Frey for his support, help and encouragement. This work is part of my PHD-thesis.

Further I would like to thank K. Belabas for answering all my email-questions concerning the Pari-Library. Also I would like to thank all the people who helped me by pointing out interesting questions and reading the preliminary versions: S. Galbraith, A. Menezes, K. Nguyen, H.-G. Rück, T. Schmidt, A. Stein.

I am grateful to the NRW Verbundsprojekt Datensicherheit and the DFG (Graduiertenkolleg), who gave me the financial support making this work possible. I thank the Center for Applied Cryptographic Research in Waterloo, Ontario, for their hospitality.

References

1. A.O.L. Atkin, *The number of points on an elliptic curve modulo a prime*, unpublished manuscript, 1991.
2. A.O.L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68. MR **93m:**11136
3. J. von zur Gathen and Victor Shoup, *Computing Frobenius maps and factoring polynomials*, Comput. Complexity **2** (1992), 187–224. MR **94d:**12011
4. P. Gaudry and R. Harley, *Counting points on hyperelliptic curves over finite fields*, ANTS IV (2000), 313–332.
5. J.I.. Igusa, *Arithmetic variety of moduli of genus two*, Ann. of Math. **72** (1960), 612–649. MR **22:**5637
6. D.E. Knuth, *The art of computer programming vol.2, seminumerical algorithms*, Addison-Weseley, 1981. MR **83i:**68003
7. N. Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), 157–165. MR **89h:**11023
8. ———, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139–150. MR **90k:**11165
9. S. Lang, *Introduction to algebraic and abelian functions*, 2nd ed., Springer-Verlag, 1982. MR **84m:**14032
10. ———, *Complex multiplication*, Springer-Verlag, 1983. MR **85f:**11042
11. S. Louboutin and R. Okazaki, *Determination of all non-normal quartic cm-fields and of all non-abelian normal octic cm-fields with class number one*, Acta Arith. (1994), 47–62. MR **95g:**11107
12. J.-F. Mestre, *Construction des courbes de genre 2 a partir de leurs modules*, Effective Methods in Algebraic Geometry (Castiglioncello, 1990), Prog. Math., Birkhäuser **94** (1991), 313–334. MR **92g:**14022
13. D. Mumford, *Tata lecture on theta*, vol. 1, Birkhäuser, 1983. MR **85h:**14026
14. ———, *Tata lecture on theta*, vol. 2, Birkhäuser, 1984. MR **86b:**14017
15. R. Okazaki, *On evaluation of L-functions over real quadratic fields*, J. Math. Kyoto Univ. **31-4** (1991), 1125–1153. MR **93b:**11154
16. S. Paulus and A. Stein, *Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves*, ANTS III, LNCS **1423** (1998), 576–591. MR **2000i:**11098
17. E. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989. MR **92b:**11074
18. S. Pohlig and M. Hellmann, *An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance*, IEEE Trans. Inform. Theory **IT-24** (1978), 106–110.
19. G. Shimura, *Abelian varieties with complex multiplication and modular functions*, revised ed., Princeton University Press, 1998. MR **99e:**11076
20. J.A. Solinas, *Generalized Mersenne numbers*, Technical Reports, CACR, Waterloo (1999).
21. 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.
22. P. van Wamelen, *Examples of genus two cm curves defined over the rationals*, Math. Comp. **68** (1999), 307–320. MR **99c:**11079
23. X. Wang, *2-dimensional simple factors of $J_0(N)$*, Manuscripta Math. **87** (1995), 179–197. MR **96h:**11059
24. H.J. Weber, *Hyperelliptic simple factors of $J_0(N)$ with dimension at least 3*, Experiment. Math. **6** (1997), 273–287. MR **99e:**14054

Institute for Experimental Mathematics, University of Essen, D-45326 Essen, Germany

E-mail address: weng@exp-math.uni-essen.de