Bjarki Holm

# Constructing Elliptic Curves with a Given Number of Points

*University of Cambridge*
*Hughes Hall*

*I declare that this essay is work done as part of the Part III Examination. It is the result of my own work, and except where stated otherwise, includes nothing which was performed in collaboration. No part of this essay has been submitted for a degree or any such qualification.*

Submitted: May 19, 2005
Signed:

# Constructing Elliptic Curves with a Given Number of Points

**Abstract**. We describe how the theory of complex multiplication can be used to construct elliptic curves over a finite field with a given number of rational points and illustrate how this method can be applied to primality testing.

# Contents

# 1 Introduction

The study of computational number theory has answered many fundamental questions on the theory of elliptic curves. In this essay we are concerned with the following question:

> Given a prime number $p$ and a positive integer $N$, how can we construct an elliptic curve defined over the finite field with $p$ elements, having $N$ rational points?

This problem was originally solved by Atkin and Morain [2] in the 1980s, in relation to the elliptic curve primality test of Goldwasser and Kilian. The method that they developed draws upon such rich subjects in number theory as the theory of complex multiplication and the class field theory of imaginary quadratic fields. Their basic idea was to look at a class of elliptic curves over the finite field $\mathbb{Z}/p\mathbb{Z}$, which can be constructed from certain class polynomials modulo the prime number $p$. The hardest part of this method is the construction of these class polynomials. In their original paper Atkin and Morain used direct construction over the complex numbers, using floating point precision, but in recent years some alternatives have been suggested. In 2000, Agashe et al. [1] proposed the use of a modified Chinese Remainder Theorem to compute a class polynomial modulo $p$ directly from a set of smaller polynomials. More recently, in 2004, Bröker and Stevenhagen [4] have presented an algorithm that works in a non-archimedean setting rather than over the complex numbers.

The main body of this essay is structured into five sections. In Section 2 we review the basics of quadratic forms, modular functions and imaginary quadratic fields. Section 3 presents some of the theory of elliptic curves relevant to our topic. We discuss general elliptic curves before turning our focus on curves over the field of complex numbers and over finite fields. This theory will be used in Section 4 when we derive the complex multiplication method for constructing elliptic curves. In Section 5 we discuss a few different ways of generating class polynomials, and lastly in section 6 we briefly describe how the complex multiplication method can be applied to primality testing.

A few numerical examples are provided in the text to illustrate some of the algorithms and procedures that we discuss. All non-trivial calculations were carried out by the author using the `PARI` computer algebra package [3].

**Notation.** We write $\mathbb{F}_q$ to denote the finite field with $q$ elements, where $q = p^a$ is a prime power. We denote by $\mathcal{H}$ the upper half complex plane, i.e. $\mathcal{H} = \{\alpha \in \mathbb{C} \mid \Im\alpha > 0\}$. If $K$ is a field then we let $\bar{K}$ be the algebraic closure of $K$.

# 2 The Modular Invariant $j$

In this section we recall some basic definitions of quadratic forms and modular functions. We start by looking at the $j$-invariant of a lattice in the complex plane, in terms of the Weierstrass $\wp$-function, which then leads to the definition of the elliptic $j$-function. Then we look at the imaginary quadratic extension $K = \mathbb{Q}(\sqrt{D})$, $D < 0$, and the relation with the set $Cl(D)$ of reduced binary quadratic forms. Lastly we present some important results about the Hilbert class field of $K$ and the associated class polynomial $H_D(X)$.

## 2.1 The Weierstrass $\wp$-Function

A *lattice* in the complex plane $\mathbb{C}$ is the set of all integral linear combinations of two complex numbers that are linearly independent over $\mathbb{R}$. We write $L[\omega_1, \omega_2]$ for the lattice $L$ generated by the complex numbers $\omega_1$ and $\omega_2$. The Weierstrass *$\wp$-function* of $L$ is defined by

$$\wp(z) = \wp(z; L) = \frac{1}{z^2} + \sum_{l \in L \setminus \{0\}} \left( \frac{1}{(z-1)^2} - \frac{1}{l^2} \right) \tag{1}$$

We know from Koblitz [9, Chapter I, Proposition 6] that the above sum converges absolutely and uniformly for $z$ in any compact subset of $\mathbb{C} - L$. The $\wp$-function is an important example of an *elliptic function*, i.e. a doubly periodic meromorphic function on $\mathbb{C}$. In fact, every elliptic function defined for a lattice $L$ can be expressed as a rational function in $\wp(z; L)$ and $\wp'(z; L)$ (see [10, §1.2]). Elliptic functions are closely related to elliptic curves, as we will see in §3.4. One can show that $\wp$ satisfies the differential equation [9, §6]

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L), \tag{2}$$

where $g_2(L) = 60 \sum_{\omega \in L \setminus \{0\}} \omega^{-4}$ and $g_3(L) = 140 \sum_{\omega \in L \setminus \{0\}} \omega^{-6}$ (and both sums converge under the same assumption as $\wp(z)$). Associated with the lattice $L$ is the *$j$-invariant* $j(L)$,

$$j(L) = 1728 \frac{g_2(L)^3}{g_2(L)^3 - 27 g_3(L)^2} = 1728 \frac{g_2(L)^3}{\Delta(L)}. \tag{3}$$

If $L$ is a lattice then $\Delta(L) \neq 0$, which means that the $j(L)$ is always well defined

[6, §10].

## 2.2 The $j$-Function

Let $\mathrm{SL}_2(\mathbb{Z})$ denote the group of integer coefficient 2-by-2 matrices of determinant 1, i.e.

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mid a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

An element of $\mathrm{SL}_2(\mathbb{Z})$ acts on a complex number $\tau$ by

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau = \tfrac{a\tau+b}{b\tau+d}.$$

A function $f$ is said to be a *modular form of weight* $2k$ if it is meromorphic everywhere in the upper half plane $\mathcal{H}$ and at infinity, and if for any $\tau$ in $\mathcal{H}$ it satisfies the relation

$$f\big(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\tau\big) = f(\tau) \text{ for all } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

A modular form of weight 0 is generally called a *modular function.*

Now let $L_\tau$ be a lattice generated by $1, \tau$, where $\tau$ a complex number in the upper half plane $\mathcal{H}$. The $j$-function $j(\tau)$ is then defined in terms of the $j$-invariant of $L_\tau$ by

$$j(\tau) = j(L_\tau) = j([1, \tau]).$$

The complex functions $g_2(\tau)$, $g_3(\tau)$ and the modular discriminant $\Delta(\tau)$ are defined in a similar manner. The main properties of the $j$-function are given by the following proposition [2, Proposition 3.1].

**Proposition 2.1.** *The $j$-function is a modular function, holomorphic in the upper half plane $\mathcal{H}$, and has a simple pole at infinity.*

Because the $j$-function is $\mathrm{SL}_2(\mathbb{Z})$-invariant, we have that

$$j(\tau + 1) = j\big(\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\tau\big) = j(\tau),$$

which shows that $j(\tau)$ is periodic of period 1. Hence it has a Fourier expansion which, if we write $q_\tau = e^{2\pi i\tau}$, is called the *$q$-expansion* of $j$. By Cox [6, Theorem

11.8], we can write the $q$-expansion as

$$j(\tau) = \frac{1}{q_\tau} + 744 + \sum_{m=1}^{\infty} c_m q_\tau^m,$$

where $\tau \in \mathcal{H}$ such that $0 < |q_\tau| < 1$ and the coefficients $c_m$ are positive integers for all $m \geq 1$. Instead of working directly with this series it is usually better to express $j(\tau)$ in terms of the Dedekind $\eta$-function, which is a modular form defined by

$$\eta(\tau) = q_\tau^{1/24} \prod_{m=1}^{\infty} (1 - q_\tau^m),$$

where, as before, $q_\tau = e^{2\pi i \tau}$. Because $0 < |q_\tau| < 1$, this product converges for any $\tau \in \mathcal{H}$. Using Euler's identity

$$\prod_{m=1}^{\infty} (1 - q^m) = \sum_{m=-\infty}^{\infty} q^{m(3m+1)/2},$$

this product can be expanded as [2, §3.5]

$$\eta(\tau) = q_\tau^{1/24}\left(1 + \sum_{m=1}^{\infty} (-1)^m (q_\tau^{m(3m-1)/2} + q_\tau^{m(3m+1)/2})\right). \tag{4}$$

The $\eta$-function satisfies the functional equations [6, Corollary 12.19]

$$\eta(\tau + 1) = \zeta_{24}\eta(\tau), \eta(-\tau^{-1}) = \sqrt{-i\tau}\eta(\tau), \tag{5}$$

where $\zeta_{24}$ is the 24th root of unity in $\mathbb{C}$. The modular discriminant of $L_\tau$ is related to $\eta$ by

$$\Delta(\tau) = (2\pi)^{12}\eta(\tau)^{24}. \tag{6}$$

This implies that, if we set $f(\tau) = \Delta(2\tau)/\Delta(\tau)$, we can compute $j$ in terms of $\eta$ by the formula

$$j(\tau) = \frac{(256f(\tau) + 1)^3}{f(\tau)}. \tag{7}$$

## 2.3 Quadratic Forms

An integral binary quadratic form $[a, b, c]$ is a polynomial $f(x, y) = ax^2 + bxy + cy^2$, where $a$, $b$, $c$ are integers. In this essay we will be working exclusively with integral binary quadratic forms and for simplicity we will write *quadratic form* to mean just that. The discriminant of the quadratic form $[a, b, c]$ is defined to be $D = b^2 - 4ac$. To each quadratic form $F = [a, b, c]$ we associate a matrix $M(F) = \left(\begin{smallmatrix} a & b/2 \\ b/2 & c \end{smallmatrix}\right)$. This allows us to define an equivalence relation: Two forms $F$ and $F'$ of the same discriminant are (properly) equivalent (written $F \sim F'$) if there exists $A$ in $\mathrm{SL}_2(\mathbb{Z})$ such that [6, §2]

$$M(F') = A^{-1}M(F)A.$$

A quadratic form $[a, b, c]$ is said to be *primitive* if $\gcd(a, b, c) = 1$ and *reduced* if it further satisifies

$$|b| \leq a \leq c \text{ and } b \geq 0 \text{ whenever } |b| = a \text{ or } a = c. \tag{8}$$

Following Cohen [5, §5.3.1] we can define a reduced quadratic form in an alternative manner: Let $f(x, y) = ax^2 + bxy + cy^2$ be a quadratic form and denote by $\tau$ the root of $f(x, 1)$ in the upper half plane $\mathcal{H}$, i.e.

$$\tau = \frac{-b + \sqrt{D}}{2a}. \tag{9}$$

Then the quadratic form $[a, b, c]$ is reduced if $\tau$ is in the domain

$$\mathcal{D} = \{\tau \in \mathcal{H} \mid \Re(\tau) \in [-\tfrac{1}{2}, \tfrac{1}{2}[, |\tau| > 1\} \cup \{\tau \in \mathcal{H} \mid \Re(\tau) \in [-\tfrac{1}{2}; 0], |\tau| = 1\}$$

As the complex number $\tau$ lies in the upper half plane $\mathcal{H}$, we see that $j(\tau)$ is well defined. When the context is clear, we write $j([a, b, c])$ to mean $j(\frac{-b+\sqrt{D}}{2a})$. For any quadratic number $\tau$ in $\mathcal{H}$ we define the *discriminant* of $\tau$ as the discriminant of the unique primitive positive definite quadratic form $[a, b, c]$ such that $\tau$ is a root of $ax^2 + bx + c = 0$.

Now let $Cl(D)$ denote the set of reduced quadratic forms of discriminant $D$ and let $h(D)$ be its order. It follows from (8) that $Cl(D)$ has finite order. The set $Cl(D)$ can be given the structure of an abelian group, under multiplication given by a composition of equivalence classes. The inverse of the class of $[a, b, c]$ in $Cl(D)$ is the class of $[a, -b, c]$ and we say that a form is *ambiguous* if it has order 2 in $Cl(D)$ [15]. It follows that an ambiguous binary quadratic is one among the types

$$[a, 0, c], [a, a, c], [a, b, a].$$

## 2.4 Hilbert Class Fields of Imaginary Quadratic Fields

An imaginary quadratic field is obtained by adjoining to the field of rationals the square root of a *fundamental* discriminant $D < 0$.

**Definition 2.1.** An integer $D$ is called a *fundamental discriminant* if $D \neq 1$ and either $D \equiv 1 \pmod 4$ and is square-free, or $D \equiv 0 \pmod 4$, $D/4$ is square-free and $D/4 \equiv 2, 3 \pmod 4$.

**Remark.** Unless otherwise noted, we henceforth write $D$ to mean a negative fundamental discriminant.

If $K = \mathbb{Q}(\sqrt{D})$ then $d_K$, the discriminant of the field $K$, is exactly equal to $D$. There is a one-to-one correspondence between $Cl(D)$ and the set of classes of fractional ideals of the unique quadratic field with discriminant $D$. Hence the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-D} = \mathbb{Q}(\sqrt{D})$ is equal to the order $h(D)$. An integral basis of $K$ is given by $(1, \omega)$, where $\omega = \frac{D+\sqrt{D}}{2}$. It follows that $K$ has ring of integers $\mathcal{O}_K = \mathbb{Z}[\omega]$ [2, §2.2]. The conjugates of $\sqrt{D}$ in $K$ are the two imaginary numbers $\pm\sqrt{D}$, hence $K$ has no real embeddings and one pair of complex embeddings into $\mathbb{C}$. It follows from Dirichlet's Unit Theorem that $\mathcal{O}_K^* \cong \mu(K)$, where $\mathcal{O}_K^*$ is the group of units in $K$ and $\mu(K)$ is the finite cyclic group of roots of unity in $K$. When $D = -3$ then $K$ contains $\zeta_6 = \frac{1+\sqrt{-3}}{2}$, a primitive sixth root of unity, and in the case $D = -4$, $K$ contains $\zeta_4 = \sqrt{-1}$. In the general case $D < -4$ the only roots of unity in $K$ are $\pm 1$. These results are summarised in the following Lemma.

**Lemma 2.2.** *Let $D < 0$ be a fundamental discriminant and let $\mathcal{O}_K$ be the ring of integers of $K = \mathbb{Q}(\sqrt{D})$. If we let $\varpi(D)$ denote the number of units in $\mathcal{O}_K$ then*

$$\varpi(D) = \begin{cases} 2 & \text{if } D < -4 \\ 4 & \text{if } D = -4 \\ 6 & \text{if } D = -3 \end{cases}$$

*and the group of units in $\mathcal{O}_K$ is equal to the $\varpi(D)^{\text{th}}$ roots of unity in $K$.*

**Remark.** This statement does in fact hold for an arbitrary order in $K$. Recall that an *order* $\mathcal{O}$ in the quadratic field $K$ is a subring of $K$, containing 1, which is a free $\mathbb{Z}$-module of rank 2. The ring of integers $\mathcal{O}_K$ is the maximal order in $K$ and the finite integer $f = [\mathcal{O}_K : \mathcal{O}]$ is called the *conductor* of $\mathcal{O}$. It is easy to show that the discriminant of $\mathcal{O}$ is $D' = f^2 d_K$, from which it follows that $\mathcal{O}_K$ is the unique order of discriminant $D$ in $K$. This implies, of course, that any order other than the maximal order can only have two units.

The Hilbert class field of $K$, which we denote by $H$, is the maximal unramified abelian extension of $K$, i.e. the composite of all the unramified abelian extensions. The following Proposition, which we state without proof, relates the Hilbert class field to values of the $j$-function at points in the upper half complex plane [2, Theorem 3.2].

**Theorem 2.3.** *Let $K = \mathbb{Q}(\sqrt{D})$, where $D$ is a negative fundamental discriminant. Then the Hilbert class field of $K$ can be obtained by adjoining to $K$ a value of $j([a,b,c])$, where $[a,b,c] \in Cl(D)$ is any one of the reduced quadratic forms of discriminant $D$. The minimal polynomial of the $j([a,b,c])$'s, denoted by $H_D(X)$, has integer coefficients. The Galois group Gal($H/K$) is isomorphic to $Cl(D)$, and if $f$ is an element of $Cl(D)$ then we write $\sigma_f$ to mean the corresponding element in Gal($H/K$). The action of $\sigma_f$ on $j$ is given by*

$$\sigma_f(j(\overline{f})) = j(f^{-1} \cdot \overline{f}).$$

The minimal polynomial $H_D(X)$ is called the *Hilbert class polynomial* and we refer to the equation $H_D(X) = 0$ as the *class equation.* The class polynomial can be expressed as

$$H_D(X) = \prod_{[a,b,c] \in Cl(D)} \left(X - j(\tfrac{-b+\sqrt{D}}{2a})\right) \in \mathbb{Z}[X]. \tag{10}$$

It then follows that if $\tau$ is any quadratic number of discriminant $D$ in $\mathcal{H}$, then $j(\tau)$ is an algebraic integer of degree exactly equal to $h(D)$. If the discriminant $D$ is not divisible by 3, then $j(\tau)$ is a cube in $H$, up to a multiplication by a unit in $K$ [5, §7.2.4]. Furthermore, the norm of any $j = j(\tau)$ in $H$, which is precisely the constant term of the class polynomial $H_D(X)$, is the cube of some rational integer [2, Proposition 7.1]. This property will become useful for checking the correctness of our calculations in §5.

**Remark.** The class polynomial can in general be defined for any integer $D'$ that occurs as the discriminant of some order $\mathcal{O}$ in $K$. Then the class polynomial of $\mathcal{O}$ is $H_{\mathcal{O}}(X) = \prod(X - j(\mathfrak{a}))$ where the product is over representatives $\mathfrak{a}$ of each ideal class of $\mathcal{O}$. We also write $H_{D'}(X)$ to mean $H_{\mathcal{O}}(X)$. Just as the zeroes of the Hilbert class polynomial generate the Hilbert class field of $K$, the roots of the class equation for an order of conductor $f$ in $K$ generate an abelian extension $K_f$ which is called the *ring class field* of $K$. In short, the ring class field $K_f$ is unramified outside $f$ and any prime ideal of $K$ not dividing $f$ is totally split if and only if it can be generated by an element which is in the congruence class of rationals modulo $f$ (see Cox [6]). The subject of ring class fields will be mostly ignored in this essay, as all the algorithms that we will consider are limited to the class of elliptic curves that have complex multiplication by the maximal order in some imaginary quadratic field.

We finish this section with an important theorem that describes the behaviour of certain rational primes in the Hilbert class field [2, Theorems 2.3 and 3.3].

**Theorem 2.4.** *Let $K = \mathbb{Q}(\sqrt{D})$ and let $H$ be the Hilbert class field of $K$. Then, if $p$ is a rational prime, the following statements are equivalent.*

*(i) $p$ is a norm in $K$.*

*(ii) $(p)$ splits completely in $H$.*

*(iii) $p$ splits as the product of two distinct elements in $\mathcal{O}_K$.*

*(iv) $H_D(X)$ modulo $p$ splits completely into linear factors with roots in $\mathbb{F}_p$.*

*(v) $4p = t^2 + s^2|D|$ has a solution in rational integers $(x, y)$.*

# 3 Elliptic Curves

In this section we introduce the basic theory of elliptic curves relevant to our topic. We start by recalling some definitions for curves given by Weierstrass equations and then go on to discuss the group law and complex multiplication over general fields. We then turn our attention to elliptic curves over the field of complex numbers and over finite fields. The theory of elliptic curves over $\mathbb{C}$ follows naturally from the discussion of lattices and the $\wp$-function in §2. Over finite fields we will focus on the case of 'ordinary' elliptic curves, which relate nicely to curves over $\mathbb{C}$. Finally, we review some of the work of Deuring concerning the reduction of elliptic curves, and state an important theorem that will provide a basis for our derivation of the complex multiplication method in §4.

This section is intended only as an overview of some of the rich theory of elliptic curves. For a more information on the subject, we refer to reader to Silverman [16] and Koblitz [9], or any of the other references given in the text.

## 3.1 Basic Definitions

Let $K$ be a field. An *elliptic curve* over $K$ (written $E/K$) is a non-singular projective plane cubic curve over $K$ together with a distinguished point $O_E$ with coordinates in $K$, called the "point at infinity". The set of projective points which are on the curve and have coordinates in $K$ will be called the set of $K$-rational points of $E$, denoted by $E(K)$.

In this essay we will be working with elliptic curves over a field $K$ of characteristic different from 2 and 3. Such a curve can always be given by an affine *Weierstrass equation* of the form

$$E : y^2 = x^3 + ax + b \qquad (a, b \in K), \tag{11}$$

the point $O_E$ taken over $K$ as the point $(x : y : z) = (0 : 1 : 0)$ in projective space [5, §7.1.4]. For an elliptic curve $E/K$ given by a Weierstrass equation, the set of $K$-rational points can be written $E(K) = \{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{O_E\}$. Associated with the Weierstrass equation are quantities

$$\Delta = -16(4a^3 + 27b^2), \quad j = -1728(4a)^3/\Delta, \tag{12}$$

called the *discriminant* and *j-invariant* of the elliptic curve, respectively. A curve

$E$ is said to be *singular* if and only if $\Delta(E) = 0$. By definition, elliptic curves are non-singular.

Now let $E(a, b)$ be shorthand notation for an elliptic curve with a Weierstrass equation given by (11).

**Theorem 3.1.** *Two elliptic curves $E(a, b)$ and $E(a', b')$ defined over $K$ are isomorphic (over $\bar{K}$) if and only if there exists a $c \in \bar{K}^*$ such that $a' = c^4 a$ and $b' = c^6 b$, the isomorphism being under the map*

$$(x, y) \mapsto (c^2 x, c^3 y).$$

*Proof.* See [16, III, Proposition 3.1(b)], which gives a proof for elliptic curves defined over general fields (whose characteristic may be 2 or 3). □

**Corollary.** *Two elliptic curves are isomorphic if and only if they have the same $j$-invariant.*

*Proof.* If $E(a, b)$ and $E(a', b')$ are isomorphic then it follows from formulas (12) and Theorem 3.1 that they have the same $j$-invariant. On the other hand, if the curves have the same $j$-invariant, we compute the relation $a^3 b'^2 = a'^3 b^2$ and verify (splitting into cases $a = 0$, $b = 0$ and $ab \neq 0$) that there always exists a $c \in \bar{K}^*$ that satisfies Theorem 3.1. □

**Remark.** From this corollary it is clear that the $j$-invariant of an elliptic curve is an invariant of the isomorphism class of that curve (hence the name).

## 3.2 The Group Law

The set of points on an elliptic curve can be given the structure of an abelian group, with a group law $\oplus$ defined by the following rule:

> Let $P$ and $Q$ be points on the projective curve $E$, and let $L$ be the line connecting $P$ and $Q$ (a tangent line if $P = Q$), which intersects the curve in a third point $R$. Then, if $O_E$ is the point at infinity on $E$, the sum $P \oplus Q$ is the point so that the line connecting $O_E$ and $R$ intersects $E$ in $O_E$, $R$ and $P \oplus Q$.

The group $E(K)$ has neutral element $O_E$. We note that the inverse of a point $P$ on $E$ is the point $\ominus P$, such that $P \oplus (\ominus P) = O_E$. For further properties of the group law we refer to Silverman [16, III]. For an integer $m$ and a point $P$ on $E$, we define multiplication by $m$ by

$$\begin{aligned} [m]P &= \underbrace{P \oplus P \oplus \ldots \oplus P}_{m \text{ terms}} && (m > 0) \\ [0]P &= O_E && \\ [m]P &= [-m](\ominus P) && (m < 0) \end{aligned}$$

Explicit formulas for the group law are given by the following Theorem.

**Theorem 3.2.** *Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. The inversion of a point $(x_0, y_0)$ on $E$ is the point $(x_0, -y_0)$, i.e. reflection in the x-axis. If $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ ar two points on $E$, then the sum $P_1 \oplus P_2 = (x_3, y_3)$ is given by*

$$\begin{aligned} x_3 &= \lambda^2 - x_1 - x_2 \\ y_3 &= \lambda(x_1 - x_3) - y_1 \end{aligned}$$

*where*

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{if } x_2 \neq x_1, \\ (3x_1^2 + a)(2y_1)^{-1} & \text{otherwise.} \end{cases}$$

*Proof.* Follows from direct manipulation of plane coordinates. □

## 3.3 Complex Multiplication

Let $E$ and $E'$ be elliptic curves defined over a field $K$. An *isogeny* from $E$ to $E'$ is a rational map from $E$ to $E'$, sending the point $O_E$ on $E$ to the point $O_{E'}$ on $E'$. If there exists a non-constant isogeny from $E$ to $E'$, then we say that the two curves are *isogenous.* The *endomorphism ring* of an elliptic curve $E$ over a field $K$ is defined to be

$$\mathrm{End}_K(E) = \{\text{isogenies } \phi : E \to E, \text{ over } K\}$$

It is a ring with multiplication given by the composition $(\phi\psi)(P) = \phi(\psi(P))$ and addition given by $(\phi + \psi)(P) = \phi(P) + \psi(P)$, where $\phi$ and $\psi$ are elements of $\mathrm{End}_K(E)$ and $P$ is a point on $E$. When $E$ is defined over $K$, we write $\mathrm{End}(E)$ to denote $\mathrm{End}_{\bar{K}}(E)$, where $\bar{K}$ is the algebraic closure of $K$. Fundamental to our study of the endomorphism ring is the multiplication-by-$m$ map, defined for any integer $m$ by

$$[m] : \begin{array}{l} E \to E \\ P \mapsto [m](P) \end{array} \tag{13}$$

where $[m](P)$ is defined as before. This map can be shown to be non-constant (see e.g. Silverman [16, p.72]). We see that the maps $[m]$ are elements of $\mathrm{End}(E)$, and we get an injection $\mathbb{Z} \hookrightarrow \mathrm{End}(E)$. In most cases these maps are the only elements, in which case $\mathrm{End}(E) \cong \mathbb{Z}$ because the maps are distinct. But if $\mathrm{End}(E)$ is strictly larger than $\mathbb{Z}$, then we say that $E$ has *complex multiplication.*

Let $\phi : E \to E'$ be a non-constant isogeny over $K$ and let $K(E)$ and $K(E')$ denote the function fields[1] of $E$ and $E'$ respectively. Then composition with $\phi$ induces an injection of function fields:

$$\phi^* : \begin{array}{l} K(E') \to K(E) \\ f \mapsto f \circ \phi \end{array} \tag{14}$$

We define the *degree* of $\phi$ as $\deg(\phi) = [K(E) : \phi^*(K(E'))]$ and we say that $\phi$ is separable if the extension $K(E)/\phi^*(K(E'))$ is separable. If $\phi : E \to E'$ is a non-constant isogeny of degree $m$ then there exists a unique isogeny $\hat{\phi} : E' \to E$ such that $\hat{\phi} \circ \phi = [m]$. We call $\hat{\phi}$ the *dual* of $\phi$ (for existence, see [16, III, Theorem 6.1(b)]).

To classify the endomorpism ring for elliptic curves with complex multiplication, we need to recall some definitions. Let $K$ be a number field and denote by $\mathcal{O}_K$ the ring of algebraic integers in $K$. By an *order* in $K$ we mean a subring of $\mathcal{O}_K$ whose dimension over $\mathbb{Z}$ equals $[K : \mathbb{Q}]$. We define a *quaternion algebra* over $K$ to be a central simple algebra of dimension four over $K$. We can now state:

**Proposition 3.3.** *The endomorphism ring of an elliptic curve is (isomorphic to) either $\mathbb{Z}$, an order in a quaternion algebra or an order in an imaginary quadratic field.*

*Proof.* See Silverman [16, §III.9]. □

[1] The function field of $E/K$ is the field of fractions of the coordinate ring $K[E] = K[X,Y]/(y^2 = x^3 + ax + b)$, assuming $\mathrm{char}(K) \neq 2, 3$.

## 3.4 Elliptic Curves Over $\mathbb{C}$

We observe that the Weierstrass equation (11) bears resemblance to the differential equation (2) for the Weierstrass $\wp$-function (in equation (11), set $y' = y/2$ and multiply through by 4 to get a similar form). This is no coincidence. We define a map from the complex torus $\mathbb{C}/L$ to the projective complex plane by

$$\begin{aligned} \psi\colon \quad & z \mapsto (\wp(z), \wp(z), 1) \quad (\text{if } z \neq 0) \\ & 0 \mapsto (0 : 1 : 0) \end{aligned} \tag{15}$$

We look at the equation $\wp(z) - x = 0$ and observe that it has (i) one solution for the roots of $4x^3 - g_2(L)x - g_3(L)$ and the point at infinity, and the corresponding $y$-coordinates are $y = \wp'(z) = 0$; (ii) two solutions in all other cases and the corresponding $y$-coordinates are $y = \pm(4\wp(z)^3 - g_2(L)\wp(z) - g_3(L))^{1/2}$.

In both cases a point $z$ is sent to a point on the elliptic curve $y^2 = 4x^3 - g_2(L)x - g_3(L)$ in the complex projective plane, and the map $\psi$ gives a one-to-one correspondence between the torus $\mathbb{C}/L$ and the curve. Moreover, because both $\wp$ and $\wp'$ are analytic functions, the $\psi$ is given by analytic functions near any point in $\mathbb{C}/L$ [9, §6]. We have sketched a proof of the following theorem.

**Theorem 3.4.** *Let $L$ be a lattice in $\mathbb{C}$. Then the map $\psi$ defines a one-to-one correspondence between $\mathbb{C}/L$ and the elliptic curve $E : y^2 = 4x^3 - g_2(L)x - g_3(L)$.*

Let $L$ be a lattice in $\mathbb{C}$ and define the set of complex numbers that stabilise $L$ as $M(L) = \{\alpha \in \mathbb{C} \mid \alpha L \subset L\}$. Clearly $M(L)$ contains $\mathbb{Z}$ and we say that $L$ has complex multiplication if $M(L)$ is strictly larger than $\mathbb{Z}$. If we let $E_\tau$ denote the elliptic curve over $\mathbb{C}$ that corresponds to the lattice $L_\tau = [1, \tau]$, then the endomorphism ring of $E_\tau$ is canonically isomorphic to $M(L_\tau)$ [6, §14.B]. Specifically, $E_\tau$ has complex multiplication if and only if $L_\tau$ does. By Theorem 3.4 we know that $E_\tau$ is defined by a Weierstrass equation $y^2 = 4x^3 - g_2(L_\tau)x - g_3(L_\tau)$. We observe that the $j$-invariant of the curve is $j(E_\tau) = 1728 g_2(L_\tau)^3/(g_2(L_\tau)^3 - 27g_3(L_\tau)^2) = j(\tau)$, where $j(\tau)$ is a complex value of the $j$-function, which we defined in §2.2. It follows from Theorem 2.3 that $j(E_\tau)$ is an algebraic integer of degree exactly equal to $h(D)$, where $D$ is the discriminant of $\tau$, and that $H_D(X)$ is the minimal polynomial of $j(E_\tau)$. The final theorem we will need about elliptic curves over $\mathbb{C}$ concerns the structure of the endomorphism ring.

**Theorem 3.5.** *Let $E$ be an elliptic curve defined over $\mathbb{C}$ and assume that $E$ has complex multiplication. Then* $\mathrm{End}_{\mathbb{C}}(E)$ *is an order in an imaginary quadratic field.*

*Proof.* An order in an imaginary quadratic field has the form $\mathbb{Z} + \tau\mathbb{Z}$, where $\tau \in \mathcal{H}$ is an algebraic integer of degree two. Let $E$ be an elliptic curve defined over $\mathbb{C}$. We know that $E \simeq \mathbb{C}/L$ where $L = L[\omega_1, \omega_2]$ is a lattice in $\mathbb{C}$. After division by one of its generators, say $\omega_1$, we can assume that $L = L_\tau$ for a certain $\tau \in \mathcal{H}$. For all $\alpha \in M(L)$ there exist integers $a, b, c$ and $d$ such that $\alpha = a + b\tau$ and $\alpha\tau = c + d\tau$. This implies that $\alpha$ is an eigenvalue of the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ (for eigenvector $[1\ \tau]^T$), i.e. $\alpha$ satisfies the equation $\lambda^2 - (a + d)\lambda + ad - bc$, and is therefore an algebraic integer of degreee two.

Now as we assume that $E$ has complex multiplication, it follows that the extension $K = \mathbb{Q}(\alpha) = \mathbb{Q}(\tau)$ is a quadratic imaginary extension of $\mathbb{Q}$ and $\mathrm{End}(E)$ is an order in $\mathcal{O}_K$ ($M(L)$ is integral over $\mathbb{Z}$), the ring of integers of $K$. □

## 3.5 Elliptic Curves Over Finite Fields

We now look at elliptic curves over the prime field $\mathbb{F}_p$, where $p > 3$ is a prime number. Over $\mathbb{F}_p$, we can consider the projective line as the set $\mathbb{Z}/p\mathbb{Z}$ plus an extra "point at infinity", containing $p + 1$ elements. Although we are only interested in prime fields for our purpose of constructing elliptic curves with a certain cardinality, some of the results we state in this section can apply to the more general case $\mathbb{F}_q$, where $q = p^a$ is a power of $p$.

If $E$ is an elliptic curve defined over some field of characteristic $p$ then we let $E^{(q)}$ denote the curve that we get by raising each coefficient of the Weierstrass equation for $E$ to the $q^{\text{th}}$ power. It can easily be shown that $E^{(q)}$ is indeed an elliptic curve. In fact, direct calculations reveal that $\Delta(E^{(q)}) = \Delta(E)^q$, which implies that $E^{(q)}$ is singular if and only if $E$ is singular. From this we define the $q^{\text{th}}$-power *Frobenius morphism* $F_q$:

$$\begin{aligned} F_q\colon \qquad E &\to E^{(q)} \\ (x, y) &\mapsto (x^q, y^q) \end{aligned} \tag{16}$$

When $E$ is defined over $\mathbb{F}_q$ then this map is clearly an endomorphism of $E$, sending every point $(x, y) = (x^q, y^q)$ to itself. It can be shown that $F_q \notin \mathbb{Z}$ (see for example Silverman [16, §V.1, Theorem 3.1]), which imples that $\mathbb{Z}$ is always strictly larger than $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$. This implies that all elliptic curves over finite fields have complex multiplication and can thus be classified into two groups based on the structure of their endomorphism ring:

**Definition 3.1.** Let $E/\mathbb{F}_q$ be an elliptic curve. Then $E$ is said to be *supersingular* if $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ is an order in a quaternion algebra and *ordinary* if $\mathrm{End}_{\bar{\mathbb{F}}_q}(E)$ is an order in an imaginary quadratic field.

If we write $f(x) = x^3 + ax + b$, with $a, b \in \mathbb{F}_q$, it is clear that for every $x$ in $\mathbb{F}_q$ there are at most two solutions $y$ in $\mathbb{F}_q$ to the Weierstrass equation $y^2 = f(x)$. Taking into consideration the point at infinity, the order of the group $E(\mathbb{F}_q)$ is therefore clearly bounded above by $2q + 1$. A classical theorem of Hasse gives a more precise bound on the number of rational points.

**Theorem 3.6.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_q$. Then the order of the group $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points is an integer in the* Hasse interval

$$\mathcal{H}_q = [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}].$$

*Proof.* We briefly sketch the proof of this theorem. We will use the fact that the map $(1 - F_q)$, where $F_q$ is the $q^{\mathrm{th}}$ power Frobenious map, is separable and hence that $\deg(1 - F_q) = |\ker(1 - F_q)|$. The Frobenius endomorphism sends every point $P$ in $E(\mathbb{F}_q)$ to itself which implies that $P$ is in $E(\mathbb{F}_q)$ if and only if $P$ is in the kernel of the map $1 - F_q$. Hence

$$|E(\mathbb{F}_q)| = |\ker(1 - F_q)| = deg(1 - F_q),$$

and the proof follows from a version of the Cauchy-Schwarz inequality for positive quadratic forms over abelian groups, using the fact that $\deg(F_q) = q$ (see Silverman [16, §V.1, Theorem 1.1]). □

Over the prime field $\mathbb{F}_p$ there is a simple criteria for $E$ to be supersingular.

**Theorem 3.7.** *Let $E$ be an elliptic curve defined over $\mathbb{F}_p$. Then $E$ is supersingular if and only if $|E(\mathbb{F}_p)| = p + 1$.*

*Proof.* The proof of this theorem relies on the fact, which we state without proof, that $E$ is supersingular over $\mathbb{F}_p$ if and only if the dual Frobenius $\hat{F}_p$ is purely inseparable (see Silverman [16, V, Theorem 3.1(a)]). Let $a$ be an integer such that $[a] = F_p + \hat{F}_p$, i.e. $a = 1 - \deg(1 - F_p) + \deg(F_p)$ (here we use the property that $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$). This implies that

$$|E(\mathbb{F}_p)| = \deg(1 - \mathbb{F}_p) = 1 + p - a.$$

But $\hat{F}_p = [a] - F_p$ implies that $\hat{F}_p$ is purely inseparable if and only if $a = 0$ modulo $p$. □

We note that any rational point $P$ in $E(\mathbb{F}_p)$ is annihilated by the group order $N = |E(\mathbb{F}_p)|$, i.e. $[N]P = O_E$ [5, §9.2]. This fact can be used to check if a certain curve has a given number of rational points, as we will see later.

## 3.6 The Deuring Lifting Theorem

Let $K$ be a number field and let

$$E : y^2 = x^3 + ax + b \qquad (a, b \in K),$$

be an elliptic curve over $K$. We are interested in the operation of *reducing* $E$ modulo a prime $\mathfrak{p}$ of $\mathcal{O}_K$ lying above $p$. We will denote the natural reduction map by a tilde. If we can write $a, b$ in the form $r/s$, where $s \notin \mathfrak{p}$, then we can define $\tilde{a}$ and $\tilde{b}$ as the images of $a$ and $b$, respectively, in the finite field $\mathbb{F}_\mathfrak{p} \triangleq \mathcal{O}_K/\mathfrak{p}$. If $\Delta = -16(4\tilde{a}^3 + 27\tilde{b}^2) \neq 0$ then the curve $\tilde{E}$ given by

$$\tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b},$$

defines an elliptic curve over $\mathbb{F}_\mathfrak{p}$ and $\mathfrak{p}$ is said to be a “prime of good reduction”. In the 1940s, Deuring developed a remarkable theory concerning the reduction of elliptic curves. While the full statement of Deuring's results is beyound the scope of this essay, we will state without proof the following proposition, which defines the behaviour of the endomorphism ring of an elliptic curve under reduction [10, §5, Theorem 14].

**Proposition 3.8** (Deuring Lifting Theorem). *Let $E$ be an elliptic curve defined over the prime field $\mathbb{F}_p$, with a non-trivial endomorphism $\psi$. Then there exists an elliptic curve $E'$ defined over a number field $K$, an endomorphism $\psi'$ of $E'$, and a good reduction $\tilde{E}$ of $E'$ at a place $\mathfrak{p}$ lying above $p$, such that $\tilde{E}'$ is isomorphic to $E$ and $\tilde{\psi}'$ corresponds to $\psi$ under the isomorphism.*

We get an immediate corollary:

**Corollary.** *With notation as above, reduction induces an isomorphism*

$$\mathrm{End}_{\bar{K}}(E) \cong \mathrm{End}_{\bar{\mathbb{F}}_p}(\tilde{E}),$$

*which preserves degrees.*

$$\begin{tikzcd}
K : & & E' \arrow[dr, "reduce"] & \\
\mathbb{F}_p : & E \arrow[ur, "lift"] & \cong & \tilde{E}'
\end{tikzcd}$$

Now consider an elliptic curve $E$ over $\mathbb{C}$, with complex multiplication by an order $\mathcal{O}_D$, of discriminant $D$, in a quadratic imaginary field $K$. According to Proposition 3.8 there is some endomorphism $\pi \in \mathrm{End}_{\mathbb{C}}(E)$ which corresponds to $F_p \in \mathrm{End}_{\bar{\mathbb{F}}_p}(\tilde{E})$ under reduction modulo $p$. Since the reduction preserves degrees, $\deg(\pi) = \deg(F_p) = p$. The degree of the complex number $\pi \in \mathcal{O}_D$ is simply its norm in $K$, so $N(\pi) = \pi\bar{\pi} = p$, i.e. $p$ splits as the product of two elements in $\mathcal{O}_D$.

Now look at the group of rational points $E(\mathbb{F}_p)$. We have seen that the Frobenius endomorpishm $F_p$ acts trivially on points in $\mathbb{F}_p$. In other words, $P$ is in $E(\mathbb{F}_p)$ if and only if $F_p(P) = P$. This implies that

$$\begin{aligned}
|E(\mathbb{F}_p)| &= |ker(1 - F_p)| \\
&= \deg(1 - F_p) && \triangleright \quad \text{By proof of Theorem 3.6} \\
&= \deg(1 - \pi) && \triangleright \quad \text{Reduction map preserves degrees} \\
&= (1 - \pi)(1 - \bar{\pi}) && \triangleright \quad N(\pi) \\
&= 1 + p - (\pi + \bar{\pi}) && \triangleright \quad p = \pi\bar{\pi} \\
&= 1 + p - Tr(\pi)
\end{aligned}$$

These results are summarised by the following theorem [5, §7.2.4].

**Theorem 3.9.** *Let $E$ be an elliptic curve with complex multiplication by an imaginary quadratic order $\mathcal{O}_D$ of discriminant $D$, and let $p$ be a prime number that splits into a product of two prime elements in $\mathcal{O}_D$, say $p = \pi\bar{\pi}$ where $\pi \in \mathcal{O}_D$. Then, for a suitable choice of $\pi$, $|\tilde{E}(\mathbb{F}_p)| = p + 1 - t$, where $t = (\pi + \bar{\pi})$.*

The question of a "suitable choice of $\pi$" is important in this context. If $u$ is a unit in $\mathcal{O}_D$, then $N(u\pi) = N(\pi) = p$, but $(u\pi + \overline{u\pi}) \neq (\pi + \bar{\pi})$ in general. In

§2.4 we counted the number of units in the unique imaginary quadratic order of discriminant $D$, which we denote by $\varpi(D)$. It can be shown that for each $D$ there exist $\varpi(D)$ isomorphism classes of elliptic curves having complex multiplication by $\mathcal{O}_D$. What remains is to find the explicit equation of the elliptic curves in each case.

In the general case $D < -4$ the two units in $\mathcal{O}_D$ are $\pm 1$. This implies that an "incorrect" choice of $\pi$ gives an opposite value of $t$ in Theorem 3.9. If $j_0 \neq 0, 1728 \pmod{p}$ is a $j$-invariant corresponding to the order of discriminant $D$, then we set $k = j_0/(1728 - j_0)$ and choose one of the two elliptic curves defined by

$$y^2 = x^3 + 3kx + 2k \tag{17}$$

$$y^2 = x^3 + 3kc^2x + 2kc^3 \qquad (c \in \mathbb{F}_p \text{ and not a square}). \tag{18}$$

One of these curves will have $p + 1 - t$ rational points and the other will have $p + 1 + t$ points.

The special cases $D = -3, -4$ are a bit more involved. Atkin and Morain [2, §8.6.2] give complete algorithms for finding the proper equations in each case. We follow Cohen [5, §9.2] and let $g$ denote a value of $\mathbb{F}_p$ such that $g^{(p-1)/l} \neq 1$ for each prime $l$ dividing $\varpi(D)$. Then the isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_D$ are given by the equations

$$y^2 = x^3 - g^k x \qquad (0 \leq k \leq 3) \qquad \text{when } D = -4 \tag{19}$$

$$y^2 = x^3 - g^k \qquad (0 \leq k \leq 5) \qquad \text{when } D = -3. \tag{20}$$

# 4 Constructing Elliptic Curves

Now that we have presented the relevant theory of elliptic curves, $j$-functions and quadratic fields, it is time that we look at the task of constructing elliptic curves with a certain number of points over a prime field. In this section we will present a general method for such construction, which is based on the theory of complex multiplication and the class field theory of imaginary quadratic fields. We will refer to this simply as the *complex multiplication method*, or ‘CM method’ for short.

We begin this section by briefly describing a trivial “brute force” procedure for finding an elliptic curve with a given cardinality. Next we present the CM method and discuss computational complexity and other practical aspects. The main step of the CM method, constructing the class polynomial for discriminant $D$, will be covered in detail in §5.

## 4.1 Naive Method

A naive method to produce an elliptic curve with $N$ rational points in $\mathbb{F}_p$ is to randomly pick an element $a \in \mathbb{F}_p \backslash \{\frac{-27}{4}\}$ and try whether the elliptic curve

$$E_a : y^2 = x^3 + ax - a$$

has $N$ rational points. We observe that the point point $P = (1, 1)$ is on $E_a$ for all $a$. By writing $N = p + 1 - t$, we check whether $P$ is annihilated by either $N = p+1-t$ or $N' = p+1+t$. If it is, then we know that $E_a$ has $p+1 \pm t$ rational points. If $P$ was annihilated by $N$ then we are finished but if it was annihilated by $N'$ then we take the quadratic “twist” of $E_a$ by equation (17). The procedure Naive-Method$(p, N)$ illustrates this method.

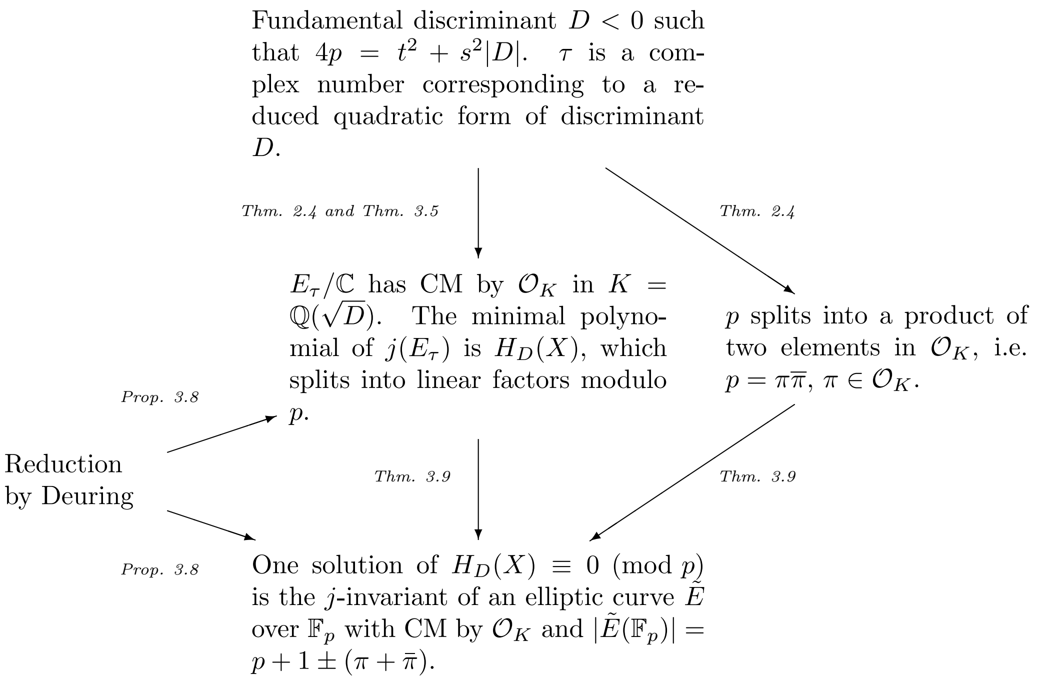
```
Naive-Method($p, N$)
$P \leftarrow (1,1)$
$t \leftarrow p+1-N$
$i \leftarrow 0$
$S \leftarrow \mathbb{F}_p \backslash \{\frac{-27}{4}\}$
repeat
    Pick a random $a \in S$
    $E_a \leftarrow y^2 = x^3 + ax - a$
    if $P$ is annihilated by $p+1-t$ then
        return $E_a$
    elseif $P$ is annihilated by $p+1+t$ then
        return quadratic twist of $E_a$
    end
    $S = S - \{a\}$
until $S = \varnothing$
```

Although the distribution of group orders $|E_a(\mathbb{F}_p)|$ is not even among the elements $a \in \mathbb{F}_p$, we can expect to check approximately $O(\sqrt{p})$ curves on average before finding a right one. According to Bröker and Stevenhagen [4] the expected running time of the naive algorithm is $O(\sqrt{p}) \times$ (constructing curve + multiplying $P$ + counting points) $= O(N^{1/2+\epsilon})$, for some small $\epsilon > 0$. When $N$ is small it may be feasible to use the naive method. All the other alternatives we will discuss in this essay are only assymptotically faster in $N$ and may very well be slower for small inputs. However for large $N$, say $N \gg 10^{10}$, the naive method becomes quite impractical.

## 4.2 Complex Multiplication Method

By the Deuring Lifting Theorem we can consider every elliptic curve over $\mathbb{F}_p$ as the reduction of some elliptic curve over a number field $K$ with the same endomorphism ring. Our task is to construct a curve having exactly $N$ rational points over $\mathbb{F}_p$.

Let $K$ be the imaginary quadratic field of discriminant $D$ where $p$ splits as the product of two elements. If we look at elliptic curves over $K$ with complex multiplication by the full ring of integers $\mathcal{O}_K$ in $K$ then we are able to apply Theorem 3.9 which immediately gives us the desired cardinality over $\mathbb{F}_p$. To find such a field $K$ we choose a fundamental discriminant $D < 0$ such that $4p = t^2 + s^2|D|$ has a solution for $t = p + 1 - N$ and $s$ any integer. Then, by Theorem 2.4, $(p)$ splits into two distinct ideals in $K$. In other words, $p$ is a norm in $K$ and $p = \pi\overline{\pi}$, where $\pi$ is an element of $\mathcal{O}_K$. If we next find the equation of an elliptic curve $E$ over $\mathbb{C}$ with $\mathrm{End}_{\mathbb{C}}(E) \simeq \mathcal{O}_K$ then by Theorem 3.9 the reduction of $E$ modulo $p$ will give us a curve with $p + 1 - t = N$ rational points over $\mathbb{F}_p$. We know that $j(E)$ is an algebraic integer of degree equal to $h(D)$, the class number of $K$. By Theorem 2.4 we know that our choice of $D$ implies that the minimal polynomial $H_D(X)$ of $j(E)$ splits completely into linear factors modulo $p$. This allows us to consider a root of $H_D(X) \equiv 0 \pmod p$ as the $j$-invariant of $\tilde{E}$, the reduction of $E$ modulo $p$. We finally construct $\tilde{E}$ by the formulas given in §3.6 and that solves our task. The interaction of theory which underlies the CM method is further illustrated in the following diagram.



Fundamental discriminant $D < 0$ such that $4p = t^2 + s^2|D|$. $\tau$ is a complex number corresponding to a reduced quadratic form of discriminant $D$.

$E_\tau/\mathbb{C}$ has CM by $\mathcal{O}_K$ in $K = \mathbb{Q}(\sqrt{D})$. The minimal polynomial of $j(E_\tau)$ is $H_D(X)$, which splits into linear factors modulo $p$.

$p$ splits into a product of two elements in $\mathcal{O}_K$, i.e. $p = \pi\overline{\pi}$, $\pi \in \mathcal{O}_K$.

Reduction by Deuring

One solution of $H_D(X) \equiv 0 \pmod p$ is the $j$-invariant of an elliptic curve $\tilde{E}$ over $\mathbb{F}_p$ with CM by $\mathcal{O}_K$ and $|\tilde{E}(\mathbb{F}_p)| = p + 1 \pm (\pi + \overline{\pi})$.

Figure 1: Basic theory behind the complex multiplication method

Let us assume that $D < -4$. Once we know the $j$-invariant in $\mathbb{F}_p$, the elliptic curve with $p+1-t$ points is constructed from one of the two equations (17). To see whether we have the right curve we can pick a random rational point and see whether it is annihilated by $N$. If that is not the case then we have selected a curve with $p+1+t$ points and the opposite equation gives the right choice. The complex multiplication method is summarised by the following procedure.

**Remark.** The two special cases $D = -3$ and $D = -4$ can be handled in a manner similar to the general case. To select between the different isomorphism classes in each case we can use certain algorithms instead of multiplying random points as in the general case. We refer the reader to [2] for full details.

```
CM-Method($p, N$)
$t \leftarrow p + 1 - N$
Find a fundamental discriminant $D$ which satisifies $4p = t^2 + s^2|D|$ for $s \in \mathbb{Z}$.
Construct the Hilbert class polynomial $H_D(X)$.
Compute a solution $j_0$ of $H_D(X) \equiv 0 \pmod{p}$.
Construct the equation of an elliptic curve $E$ over $\mathbb{F}_p$ of invariant $j_0$.
Find a random point $P$ on $E$.
if $[N]P \neq O_E$ then
    $E \leftarrow$ quadratic "twist" of $E$
end
return $E$
```

## 4.3 Computational Aspects

Apart from the construction of the Hilbert class polynomial $H_D(X)$, which we will look at in detail in §5, the other hard step in this algorithm is computing a root of $H_D(X) \equiv 0 \pmod{p}$. Many standard factorisation algorithms are known for that purpose. See for example Cohen [5, §1.6.1] or Knuth [8, §4.6.2].

Finding a "good" discriminant $D$ that is suitable for our prime $p$ is quite simple, as we are expecting a certain cardinality $N$ (the situation becomes more involved when we use this method for primality testing, as we will see in §6). We set $t = p + 1 - N$ and

$$D = \frac{t^2 - 4p}{s^2} = \frac{(p+1-N)^2 - 4p}{s^2},$$

and search for an $s$ such that $s^2$ divides $(t^2 - 4p)$ and $D < 0$ is fundamental and as small as possible. The condition that $D$ is small is important as we expect the algorithm to run in time asymptotic to a power of $|D|$, as we will soon see[2]. Of course, a necessary condition for this algorithm to produce a solution is that the integer $N$ is contained in the Hasse interval $\mathcal{H}_p$. In fact, since we restrict to the case of a prime field $\mathbb{F}_p$, all integers in $\mathcal{H}_p$ do occur as the group order $E(\mathbb{F}_p)$ of some elliptic curve $E$ over $\mathbb{F}_p$ [4].

We should note one special case for the algorithm, namely when $N = p + 1$. Then by Theorem 3.7 we know that we can pick any supersingular curve over $\mathbb{F}_p$. There are many criteria for supersingular curves, see for example [16, §V, Theorem 4.1]. As an example, the elliptic curve $E/\mathbb{F}_p$ defined by $y^2 = x^3 + 1$ is supersingular if and only if $p \equiv 2 \pmod 3$.

Finally we remark on the computational complexity of the method. The two time consuming steps in the algorithm are the construction of the Hilbert class polynomial $H_D(X)$ and the computation of a root of $H_D(X)$ modulo $p$. Crucial to the complexity analysis is the estimate $\log(h(D)) \sim \log(\sqrt{d})$ [11, §XVI.4], where we write $d = |D|$. It follows that the approximation $h(D) \sim \sqrt{|D|}$ should not be too bad. We will see in the next section that the basic complex analytic method to construct $H_D(X)$ takes time $O(d^2(\log d)^2)$. By one approximation [12, §5.10] it takes time $O(d(\log p)^3)$ to calculate a solution to $H_D(X) \equiv 0 \pmod p$. Which one of these two steps will dominate the running time of the algorithm depends of course on the relative size of $d$ and $p$. In general, we expect the $O(d^2(\log d)^2)$ term to prevail if we seek elliptic curves with a large number of rational points. The other steps in the algorithm count less towards the overall complexity. For example, there is an algorithm to compute $[m]P$, for an integer $m$ and a point $P$ on $E$, in time asymptotically $O(\log m)$ [14].

[2] In elliptic curve cryptography the discriminant has to be of certain minimal size to ensure security. According to [1] some cryptography standards recommend using elliptic curves with complex multiplication by an order of discriminant at least equal to 200.

# 5 Constructing the Class Polynomial

The main step in the complex multiplication method is the construction of the class polynomial of the imaginary quadratic order of discriminant $D$. In this section we present a few different ways of solving that task. In their original paper [2], Atkin and Morain suggested a complex analytic method based on numerical evaluation of the $j$-function, which we will look at in some detail. The complex analytic method has been estimated to run in time asymptotically $O(d^2(\log d)^2)$, which is not much better than the naive method when we consider small inputs. This method also requires extensive computing resources to work with the huge Hilbert polynomials in high precision. Over the past few years a number of authors have suggested alternative approaches to tackle these problems. Bröker and Stevenhagen [4] have proposed solving the class equation in a non-archimedean setting by working over the $p$-adic numbers. The main advantage of this method is that it requires substantially less precision than the complex analytic approach. To address the problem of working with huge Hilbert polynomials with integer coefficients, Agashe, Lauter, and Venkatesan [1] have come up with an algorithm based on the Chinese Remainder Theorem, which can be used to directly construct $H_D(X)$ modulo $p$ from a set of polynomials $H_D(X)$ modulo smaller primes. Apart from avoiding the computation of the full Hilbert class polynomial over the complex numbers, this method promises to be asymptotically faster than the complex analytic approach for certain inputs, as we will see. At the end of this section we will also look at how we can use higher class invariants, instead of the invariant $j$, to generate Hilbert class fields.

## 5.1 Numerical Evaluation of the $j$-Function

In §2.2 we gave a formula for $j(\tau)$ in terms of the Dirichlet $\eta$-function and the modular invariant $\Delta(\tau)$ (equations (4) and (6)). The convergence of the $q$-expansion for $\eta$ is quite good as the exponents for each term grow quadratically. It should therefore be practical to apply this formula directly to compute a numerical value of $j(\tau)$. To see how many terms have to be included for a desired precision, we look at the truncated series

$$\eta_M(\tau) = q_\tau^{1/24}\left(1 + \sum_{m=1}^{M}(-1)^m\big(q_\tau^{m(3m-1)/2} + q_\tau^{m(3m+1)/2}\big)\right), \tag{21}$$

where $M$ is a positive integer and $q_\tau = e^{2i\pi\tau}$ as before. For an upper bound on the error we get by truncating the series we use the following Lemma [13].

**Lemma 5.1.** *Let $q_\tau = e^{2\pi i\tau} = \rho_\tau e^{i\theta}$, where $\tau$ is a complex number in the upper half plane $\mathcal{H}$ such that $0 < |q_\tau| < \frac{1}{2}$. Then if $M$ is a positive integer,*

$$|\eta(\tau) - \eta_M(\tau)| \leq 6\rho_\tau^{3M^2/2}.$$

*Proof.* Write $q_\tau = \rho_\tau e^{i\theta} = \rho_\tau(\cos(\theta) + i\sin(\theta))$ and assume that $0 < |q_\tau| < 1$. Then define the functions

$$\begin{aligned} f(\tau) = f(q_\tau) &= \sum_{n=1}^{\infty}(-1)^n(q_\tau^{m(3m-1)/2} + q_\tau^{m(3m+1)/2}) \\ f_M(\tau) = f_M(q_\tau) &= \sum_{m=1}^{M}(-1)^m(q_\tau^{m(3m-1)/2} + q_\tau^{m(3m+1)/2}) \end{aligned}$$

Let $r(\tau) = r(q_\tau)$ and $r_N(\tau) = r_N(q_\tau)$ to be the real parts of $f(\tau)$ and $f_N(\tau)$, respectively, and

$$\begin{aligned} \delta(\tau) = \delta(q_\tau) &= r(\rho_\tau) - r(q_\tau) \\ \delta_M(\tau) = \delta_M(q_\tau) &= r_M(\rho_\tau) - r_M(q_\tau) \end{aligned}$$

We look at the difference $\delta(q_\tau) - \delta_N(q_\tau)$. This is an alternating series and since $|\rho_\tau| < 1$ we get (using shorthand notation $f_m = m(3m-1)/2$ and $g_m = m(3m+1)/2$)

$$\begin{aligned} &|\delta(q_\tau) - \delta_N(q_\tau)| = \\ &\qquad \sum_{m=M+1}^{\infty} (-1)^m(\rho_\tau^{f_m}(1 - \cos(\theta f_m)) + \rho_\tau^{g_m}(1 - \cos(\theta g_m))) \\ &\qquad \leq \rho_\tau^{f_m}(1 - \cos(\theta f_m)) + \rho_\tau^{g_m}(1 - \cos(\theta g_m))\big|_{m=M+1} \\ &\qquad \leq 2(\rho_\tau^{(M+1)(3M+2)/2} + \rho_\tau^{(M+1)(3M+4)/2}) \\ &\qquad = 2\epsilon_{M+1}. \end{aligned}$$

Simple manipulation yields

$$\begin{aligned}|r(q_\tau) - r_M(q_\tau)| &= |(r(q_\tau) - r(\rho_\tau)) + (r_M(\rho_\tau) - r_M(q_\tau)) + (r(\rho_\tau) - r_M(\rho_\tau))| \\ &= |(\delta_M(q_\tau) - \delta(q_\tau)) + (r(\rho_\tau) - r_M(\rho_\tau))| \\ &\leq 3\epsilon_{M+1}.\end{aligned}$$

Repeating the calculations for the imaginary parts, we obtain the bound $|f(\tau) - f_N(\tau)| \leq 6\epsilon_{N+1}$. We estimate the size of the term $\epsilon_m$ by

$$\begin{aligned}\epsilon_m &= \rho_\tau^{m(3m-1)/2} + \rho_\tau^{m(3m+1)/2} \\ &= \rho_\tau^{m(3m-1)/2}(1 + \rho_\tau^m) \\ &\leq 2\rho_\tau^{m(3m-1)/2} \\ &\leq \rho_\tau^{3(m-1)^2/2} \quad \text{if} \quad m \geq \tfrac{-2\log 2/\log\rho_\tau + 3}{5},\end{aligned}$$

which is true for all $m \geq 1$ if $\rho_\tau \leq \frac{1}{2}$. Combining this with the bound for $|f(\tau) - f_N(\tau)|$, and noting that $|q_\tau^{1/24}|$ is always less than 1, gives the desired result. □

## 5.2 Complex Analytic Approach

By Theorem 2.3, we know that

$$H_D(X) = \prod_{[a,b,c] \in Cl(D)} \left(X - j\left(\tfrac{-b+i\sqrt{d}}{2a}\right)\right),$$

where $Cl(D)$ is the set of all reduced quadratic forms of discriminant $D$ and $d = |D|$. We know that the degree of $H_D(X)$ equals the class number $h = h(D)$. By iterating through all reduced forms of discriminant $D$, and computing a numerical value of the corresponding $j$-value, we get a simple method for constructing the polynomial $H_D(X)$. The important part here is that if we ensure sufficient precision in our calculations then we can *exactly* determine $H_D(X)$ because it has integer coefficients (Theorem 2.3).

**Remark.** As we noted in §2.4, we can use the fact that $H_D(0)$ is a cube of a rational integer to check our computations.

To make sure that we get the correct outcome we make some observations on the polynomial $H_D(X)$. Because it has integer coefficients the absolute error in the final computation of each coefficient must be within 0.5. To achieve this accuracy we need some prior estimate of the size of the coefficients. From $\tau = (-b + i\sqrt{d})/(2a)$ we obtain $\rho_\tau = e^{-\pi\sqrt{d}/a}$ and $\theta = -\pi b/a$, where we write $q_\tau = \rho_\tau e^{i\theta}$. By the $q$-expansion of $j$ (eq. (2.2)) we get the estimate $|j(\tau)| = O(q_\tau^{-1}) = O(e^{\pi\sqrt{d}/a})$. We then get an upper bound $B$ on the size of the coefficients by forming a product of all the values of $e^{\pi\sqrt{d}/a}$ associated with reduced quadratic forms $[a, b, c]$ of discriminant $D$, times the largest (middle) binomial coefficient.

$$B = \binom{h}{\lfloor h/2 \rfloor} \exp\biggl(\pi\sqrt{d} \sum_{[a,b,c]} \frac{1}{a}\biggr). \tag{22}$$

The required decimal precision is obtained by taking the base-10 logarithm of this bound:

$$\mathrm{Prec}(D) = \left\lceil \frac{\log\binom{h}{\lfloor h/2 \rfloor} + \pi\sqrt{d}}{\log 10} \sum_{[a,b,c]} \frac{1}{a} \right\rceil + p_0. \tag{23}$$

Here $p_0$ is an empirical constant that takes care of rounding errors and errors due to our estimate of $|j(\tau)|$. According to Cohen [5, §7.6.2] and Atkin [2, §7.1], the value of $p_0$ is typically chosen to be 10. The figure $\mathrm{Prec}(D)$ should be calculated once, before computing $H_D(X)$.

Now we need to know what value of $M$ in eq. (21) approximates $\eta(\tau) = \eta((-b + i\sqrt{d})/(2a))$ with the desired floating point precision. We observe that if $[a, b, c]$ is a reduced form of negative discriminant $D$ then $d = 4ac - b^2 \geq 4a^2 - a^2$, which implies that $a \leq \sqrt{d/3}$. Hence

$$\rho_\tau = e^{-\pi\sqrt{d}/a} \leq e^{-\pi\sqrt{3}} < \tfrac{1}{2},$$

so we can apply Lemma 5.1. Equating the base-10 logarithm of the error bound given by the Lemma and the precision $\mathrm{Prec}(D)$ yields

$$M = \left\lceil \sqrt{a \frac{2}{3} \frac{\mathrm{Prec}(D) \log 10 + \log 6}{\pi\sqrt{d}}} \right\rceil \tag{24}$$

Then to calculate an accurate numerical value of $j(\tau)$ we compute $\eta_M(\tau)$ by eq. (21) and apply the result to eq. (7). For that we need to compute both $\Delta(\tau)$ and $\Delta(2\tau)$. In general, to compute $\Delta(k\tau)$ we compute $\eta_M(q_\tau^k)$ to the order $M$ obtained by replacing $a$ with $\frac{a}{k}$ in eq. (24).

We can make some further remarks to make the computation more efficient. If $[a, b, c]$ is ambiguous (see §2.3) we get $j([a, -b, c]) = \overline{j([a, b, c])}$, where $\bar{x}$ denotes the complex conjugate of $x$. If $r$ is a root of $H_D(X)$ then $\bar{r}$ is also a root, so we can halve the computation by checking for ambiguous forms. Then if $[a, b, c]$ is ambiguous we adjoin a factor

$$(X - j([a, b, c]))(X - \overline{j([a, b, c])}) = X^2 - 2\Re(j([a, b, c]))X + |j([a, b, c])|^2$$

to the polynomial. Otherwise we adjoin a factor $(X - j([a, b, c]))$. Finally we note that because $b$ is even if and only if $D$ is even (look at $D = b^2 - 4ac$, and the term $4ac$ is even), we can reduce the number of iterations by initially checking the parity of $D$.

With these remarks in mind, the procedure Hilbert-Basic runs through all positive $a, b$ such that $b \le a \le \sqrt{d/3}$ and $a$ divides $\frac{b^2-D}{4}$, and constructs a polynomial whose roots are the $j$-invariants associated with the reduced forms $[a, b, \frac{b^2-D}{4a}]$.

```
HILBERT-BASIC($D$)
Compute Prec($D$)                              ▷ Using formula (23)
$H_D \leftarrow 1$                             ▷ Polynomial variable $H_D$
$b \leftarrow |D| \bmod 2$                     ▷ Init. $b$ to 0 or 1 ($D$ odd/even)
$B \leftarrow \lfloor\sqrt{|D|/3}\rfloor$      ▷ Upper bound of range
while $b \leq B$ do
    $t \leftarrow \frac{b^2-D}{4}$             ▷ Possibly $t = ac$
    $a \leftarrow \max(b, 1)$                  ▷ If $b = 0$ then $a \neq b$
    repeat
        if $a \mid t$ then
            $j \leftarrow j((-b+\sqrt{D})/(2a))$        ▷ Using (21) and (7)
            if $a = b$ or $a^2 = t$ or $b = 0$ then
                $H_D \leftarrow P \cdot (X - j)$
            else
                $H_D \leftarrow P \cdot (X^2 - 2\Re(j)X + |j|^2)$
            end
        end
        $a \leftarrow a + 1$                   ▷ Loop on $a$
    until $a^2 > t$
    $b \leftarrow b + 2$                       ▷ Loop on $b$ (either odd or even)
end
Round coefficients of $H_D$ to nearest integer
return $H_D$ modulo $p$
```

We note that there are two serious drawbacks to this procedure. First of all, the Hilbert class polynomial has huge integer coefficients, which grow fast as the class number increases. Secondly, the algorithm requires immense precision for floating point calculations in order to ensure correct results. From a practical point of view, the high precision and memory handling required by this method hinders its implementation on simple processors with limited amount of memory, as encountered in many cryptography applications.

**Example 1.** Let us look at a simple example to illustrate the algorithm. We will construct $H_D(X)$ for a fundamental discriminant $D = -23$. The class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-23})$ is $h(-23) = 3$ and the three reduced quadratic forms of discriminant -23 are $f_1 = [1,1,6]$, $f_2 = [2,1,3]$ and $f_3 = [2,-1,3]$, with corresponding $\tau$-values $\tau_1$, $\tau_2$ and $\tau_3$, respectively. We calculate the required precision by formula (23)

$$\mathrm{Prec}(-23) = \lceil \tfrac{\log 3+\pi\sqrt{23}}{\log 10}(1+\tfrac{1}{2}+\tfrac{1}{2})+10\rceil = 25.$$

This means that our calculations have to be carried out with at least 25 decimal digits. To achieve this precision we need to compute $\eta_M(\tau)$ to order $M = 2$ and $M_2 = M_3 = 3$ for arguments $\tau_1$, $\tau_2$ and $\tau_3$, respectively. That we need only consider 2 or 3 terms to achieve such high precision illustrates the good convergence of the $q$-expansion. Now we compute the polynomial

$$P = (X - j(\tau_1))(X - j(\tau_2))(X - j(\tau_3)),$$

and after taking real parts and rounding the coefficients to the nearest integer, we get

$$H_{-23}(X) = X^3 + 3491750X^2 - 5151296875X + 12771880859375.$$

We observe that the constant factor is correctly a cube of an integer, $23375^3 = 12771880859375$. To verify our result we check if $H_{-23}(X)$ splits into linear factors modulo a prime $p$. We look at the prime $p = 59$, which is “good” for the discriminant $D = -23$, which means that there is a solution to $4 \cdot 59 = t^2 + 23s^2$ (just take $(t,s) = (12,2)$). Reduction modulo 59 gives

$$H_{-23}(X) \equiv (X-20)(X-42)(X-44) \pmod{59},$$

and all the roots lie in $\mathbb{F}_{59}$. Taking $j_0 = 20$, we construct the elliptic curve $E : y^2 = x^3 + 33x + 13$ from equation (17). Point counting reveals that the order is correctly $|E(\mathbb{F}_{59})| = 48 = 59 + 1 - 12$.

## 5.3 Directly Constructing $H_D(X)$ Modulo $p$

In the complex analytic method we compute the class polynomial over $\mathbb{C}$ using the fact that its coefficients are rational integers. Even though we are eventually looking for $H_D(X) \bmod p$, we first have to compute $H_D(X)$ with full precision and then perform reduction. The problem with this approach is that the coefficients of the class polynomial come to be very large. We have already seen an example for class number 3 where the constant term of $H_D(X)$ has 16 decimal digits. In the case when $D = -832603$, for example, the class number is 96 and the constant term has more than 1200 digits. These large coefficients make the complex analytic method rather unwieldy in practise.

In a recent paper, Agashe et al. [1] suggest a method to directly compute the reduced polynomial $H_D(X) \bmod p$ without ever constructing $H_D(X)$ over $\mathbb{C}$. This is achieved by generating a set of reduced polynomials $H_q(X) = H_D(X)$ mod $q$, where $q$ is a prime number relatively small compared to $p$. Then using an algorithm based on a modified version of the Chinese Remainder Theorem, the polynomial $H_D(X) \bmod p$ can be constructed one coefficient at a time, from knowledge of each of the reduced polynomials $H_q(X)$.

**Theorem 5.2** (Modified Chinese Remainder Theorem)**.** *Let $S_m = (m_i)_{i=1}^l$ and $S_a = (a_i)_{i=1}^l$ be sets of integers for some $l > 0$, such that all the $m_i$ are co-prime and $0 \leq a_i < m_i$ for $i = 1, 2, \cdots, l$. Assume that there exists an integer $x$ such that $|x| < (\frac{1}{2} - \epsilon)\prod_{i=1}^l m_i$ for some small positive real number $\epsilon < \frac{1}{2}$. Then, given an integer $n$ less than $|x|$, there exists an algorithm for directly computing $x \bmod n$ from $S_m$ and $S_a$.*

**Remark.** The point of the theorem is that we can compute $x \bmod n$ without ever knowing $x$ explicitly.

*Proof.* We will prove the existence of such an algorithm. Define

$$\begin{aligned} M &= \prod_{i=1}^{l} m_i \\ M_i &= M/m_i \\ b_i &\equiv 1/M_i \pmod{m_i} \qquad\qquad 0 \leq b_i < m_i \end{aligned}$$

The definition of $b_i$ implies that $b_i M_i \equiv 1 \pmod{m_i}$ for all $i = 1, 2, \cdots, l$. Then by the Chinese Remainder Theorem, the positive integer $s = \sum_{i=1}^l a_i b_i M_i$ is congruent to $x$ modulo $M$, i.e. $s = x + rM$, where $r$ is some non-negative integer. We write $x = s - rM$ and we want to compute $x \bmod n$. If we knew nothing of $x$ we would not be able to infer anything about the integer $r$, but because we are told that $x < (\frac{1}{2} - \epsilon)M$, we observe that $r = \lfloor \frac{s}{M} + \frac{1}{2} \rfloor$ (if $x$ were greater or equal than $M/2$ then $r$ would be $\lceil \frac{s}{M} + \frac{1}{2} \rceil$). If we can recover $r$, then $x \bmod n$ may be computed by

$$x \bmod n = (s \bmod n) - (r \bmod n) \cdot (M \bmod n),$$

as all the quantities on the right hand side are known. To solve for $r$, we observe that $|x| < (\frac{1}{2} - \epsilon)M$ implies that $\frac{s}{M} + \frac{1}{2}$ is not within $\epsilon$ of an integer. Thus we can recover $r$ by computing an approximation $r_0$ such that $|r_0 - \frac{s}{M}| < \epsilon$ and then round $r_0$ to the nearest integer. We achieve this by setting

$$r_0 = \sum_{i=1}^{l} \frac{a_i b_i}{m_i},$$

where each term in the series is computed with floating point precision $\epsilon/l$. □

From the ideas developed in the proof of Theorem 5.2 we present an algorithm for computing $x \mod n$, given $n$, $S_m$, $S_a$ and $\epsilon$ having the same signature and properties as in the theorem. Note that in the description of the algorithm we let $rem(a, b)$ denote a *variable* (and not a function call) holding the value of $a$ mod $b$, the remainder of the Euclidian division of $a$ by $b$.

```
Modified-CRT($n, S_m, S_a, \epsilon$)
 1  $M \leftarrow \prod_{i=1}^{l} m_i$
 2  $l \leftarrow |S_m|$
 3  for $i \leftarrow 1$ to $l$ do                          ▷ Calculate the $M_i$'s and $b_i$'s
 4      $M_i \leftarrow M/m_i$
 5      $b_i \leftarrow 1/M_i \bmod m_i$
 6  end
 7  $rem(M, n) \leftarrow M \bmod n$
 8  Compute $rem(M_i, n) \leftarrow rem(M, n)/(m_i \bmod n)$ for all $i$
 9  Compute $rem(a_i b_i, n) \leftarrow a_i b_i \bmod n$ for all $i$
10  $r \leftarrow$ round($\sum_{i=1}^{l} \frac{a_i b_i}{m_i}$          ▷ With precision $\epsilon/l$
11  $rem(r, n) \leftarrow r \bmod n$
12  $rem(s, n) \leftarrow (\sum_{i=1}^{l} rem(a_i b_i, n) \cdot rem(M_i, n)) \bmod n$
13  return $(rem(s, n) - rem(r, n) \cdot rem(M, n)) \bmod n$
```

**Remarks.**

1. The computation of $M_i$ mod $n$ in step 8 can be parallelised. This could be useful when working with very large class numbers.

2. In step 10 we need to compute each term to precision $\epsilon/l$. In practise, we would perform the calculations with $\lceil -\log \epsilon/l/\log 10\rceil + p_0$ significant

digits, where $p_0$ is some positive constant that takes into account rounding errors, as we described in §5.2.

Now we describe how this algorithm can be used to compute $H_D(X) \bmod p$ directly. Unless otherwise noted we assume that $D < -4$. To begin with, we calculate $B$, the upper bound of coefficients of $H_D(X)$, by formula (22), and the class number $h$. One way of computing the class number is to use an algorithm similar to the HILBERT-BASIC procedure, i.e. by traversing the reduced quadratic forms of discriminant $D$ and keeping a counter. We then fix a small positive number $\epsilon$ (for example $\epsilon = 0.001$ as suggested in [1]) and set $M = B/(\frac{1}{2} - \epsilon)$. Next we generate a set of distinct prime numbers $q$, that satisfy $4q = x^2 + |D|$ for some integer $x$, such that the product of all the primes will exceed $M$.

For each prime $q$ we search for the $h$ elliptic curves over $\mathbb{F}_q$ that have $q + 1 - t$ or $q + 1 + t$ rational points, where $t$ comes from $4q = t^2 + |D|$. We can do this either by counting points or by finding a random point on the curve and seeing if it is annihilated by either order (in the latter case we are doing something similar to the naive algorithm that we described on page 22). In the algorithm HILBERT-CRT below we apply the first method. After computing these $j$-invariants we construct the polynomial $H_D(X)$ mod $q$. Finally we use the MOD-CRT routine to compute $H_D(X)$ mod $p$, one coefficient at a time, from the coefficients of all the "smaller" polynomials.

**Remark.** By selecting a fundamental discriminant $D$ which satisifies $4p = t^2 + s^2|D|$, for some integers $t$ and $s$, we know that the roots of $H_D(X) \bmod p$ are the $j$-invariants of elliptic curves that have $p + 1 \pm t$ rational points over $\mathbb{F}_p$. The opposite, that a suitable $j$-invariant in $\mathbb{F}_p$ is a root of $H_D(X)$ mod $p$, is however not true in general. Checking all $j$-invariants in $\mathbb{F}_p$ for $p + 1 \pm t$ rational points would reveal curves having complex multiplication by an order in $K$ containing the order of index $s$ in $\mathcal{O}_K$. Hence we restrict the algorithm to discriminants that satisfy $D = t^2 - 4p$, which has solutions in $t$ for all odd primes $p$ unless $D \equiv 1 \pmod 8$. To date, the CRT method has not been extended to work with arbitrary orders in $K$, to our best knowledge.

```
HILBERT-CRT($D, p$)
Initialise $B$ and $h$
$S \leftarrow \varnothing$, $H \leftarrow \varnothing$
$M \leftarrow 1$
while $M \le B$ do                          ▷ Generate a set $S$ of small primes
                                            ▷ such that their product $M$ exceeds $B$
    Find a prime $q$ such that
    $4q = t^2 + d$ has a solution for $t$
    $S \leftarrow S \cup \{q\}$                     ▷ Add $q$ to the set $S$
    $M \leftarrow M \cdot q$
end
for each $q$ in $S$ do                      ▷ Compute $H_D(X)$ mod $q$ for all $q \in S$
    $S_q \leftarrow \varnothing$
    for each $j \in \mathbb{F}_q \backslash \{0, 1728\}$ do     ▷ We should also break when $|S_q| = h$
        $k \leftarrow \frac{j}{1728-j}$
        $E \leftarrow y^2 = x^3 + 3kx + 2k$       ▷ Elliptic curve $E$ with $j(E) = j$
        if $|E(\mathbb{F}_q)| = q + 1 \pm t$ then
            $S_q \leftarrow S_q \cup \{j\}$
        end
    end
    $H_q(X) = \prod_{j \in S_q}(X - j)$          ▷ $H_q(X)$ denotes $H_D(X)$ mod $q$
    $H \leftarrow H \cup H_q(X)$                  ▷ Add $H_q$ to the set $H$
end
for $i \leftarrow 1$ to $h$ do                 ▷ Lift to $H_D(X)$ mod $p$
    Form a set $S_a$ of the $i^{\text{th}}$ coefficients of every $H_q(X)$
    $c_i \leftarrow$ MOD-CRT($p, S, S_a, \epsilon$)     ▷ Compute the $i^{\text{th}}$ coefficient of $H_D(X)$ mod $p$
end
return $\sum_{i=1}^{h} c_i X^i$                ▷ $H_D(X)$ mod $p$
```

**Remark.** Note that in practise one would not implement this algorithm directly as it is written here. For example, a large part of the MOD-CRT procedure is common to all coefficients of $H_D(X)$ (mod $p$), so they should be executed only once. The two procedures are defined separately here simply for the sake of clarity.

According to [1] the overall complexity of this algorithm, when $d$ is large, is with high probability

$$O\big(d^{3/2}(\log d)^{10} + d(\log d)^2 \log p + d^{1/2}(\log p)^2\big).$$

This shows that we may expect this algorithm to run faster than the complex analytic method when $d$ is roughly larger than $(\log p)^2$ [1]. In practical terms, this might be the case in some cryptography applications, where one usually requires a large discriminant. On the other hand, in elliptic curve primality testing one typically looks for a small discriminant, which implies that the complex analytic approach might work better. We look better at primality testing in §6.

**Example 2.** The version of the Hilbert-CRT algorithm that we present here can only work for a discriminant $D \neq 1 \pmod 8$ as we have remarked. Let $D = -35$ be a fundamental discriminant and assume we want to compute $H_D(X)$ mod $p$ where $p = 3089 = 111^2 + 35$ is a prime number. The class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-35})$ is $h(-35) = 2$, corresponding to the reduced quadratic forms $[3, \pm1, 3]$. By formula (22) we obtain the bound $B \approx 2e^{13}$ and set $M = B/(\frac{1}{2} - \epsilon) \approx 10^6$, where we choose $\epsilon$ to be 0.001. Then we compute a set of small primes $q$ that satisfy $4q = t^2 + 35$, for some integer $t$, and whose product exceeds $M$. For each $q$ we also compute the two $j$-invariants of the elliptic curves over $\mathbb{F}_q$ that have $q + 1 \pm t$ rational points. The following table displays the results of these computations.

| $q$ | $t$ | $j$ | $H_D(X)$ mod $q$ |
|---|---|---|---|
| 11 | 3 | 4, 10 | $X^2 + 8X + 7$ |
| 29 | 9 | 13, 24 | $X^2 + 21X + 22$ |
| 191 | 27 | 12, 35 | $X^2 + 144X + 38$ |
| 281 | 33 | 198,207 | $X^2 + 157X + 241$ |
| 389 | 39 | 51, 177 | $X^2 + 161X + 80$ |
| 659 | 51 | 76, 78 | $X^2 + 505X + 656$ |

Setting $S = \{11, 29, 191, 281, 389, 659\}$, we calculate

$$\text{Modified-CRT}(p, S, \{8, 21, 144, 157, 161, 505\}, \epsilon) = 2068,$$
$$\text{Modified-CRT}(p, S, \{7, 22, 38, 241, 80, 656\}, \epsilon) = 1580.$$

Hence

$$H_{-35}(X) \equiv X^2 + 2068X + 1580 \equiv (X - 1874)(X - 2236) \pmod{59}.$$

Taking $j_0 = 1874$ gives the elliptic curve $E : y^2 = x^3 + 1104x + 736$ over $\mathbb{F}_{3089}$, which has exactly $N = 3089 + 1 - 111 = 2979$ rational points.

## 5.4 Non-Archimedean Approach

Bröker and Stevenhagen have recently come up with a new idea for constructing the Hilbert class polynomial in a non-archimedean ($p$-adic) setting. We will now briefly review this method, referring to to [4] for full details.

The first step in the non-archimedean method is to find a small prime $q < p$ such that $4q = t^2 + D$, for a positive $t$ as small as possible. Here $D$ is a fundamental discriminant for $p$, which is computed as before. For such a prime $q$, we know that there exists an ordinary elliptic curve over $\mathbb{F}_q$ with complex multiplication by the order $\mathcal{O}_K$ ($D$ is fundamental) and $N_q = q + 1 - t$ rational points. Since we are working with a small $N_q$ we can just as well search for such a curve using the naive method that we have seen before.

Now let $H$ denote the Hilbert class field of $K = \mathbb{Q}(\sqrt{D})$. According to the Deuring Lifting Theorem there exists an elliptic curve $E'$ over $H$, with complex multiplication by the unique quadratic order of discriminant $D$, and a prime $\mathfrak{q}|q$ in $H$, such that $E'$ reduces modulo $\mathfrak{q}$ to $E$. Now the important point is that since $q$ splits completely in $H$, the curve $E'$ is in fact defined over the $q$-adic field $\mathbb{Q}_q$. The Hilbert polynomial $H_D(X)$, whose roots are the $j$-invariants of isomorphic elliptic curves over $H$, generates the Hilbert class field. In the complex analytic approach we computed $H_D(X)$ by approximating the $j$-function using floating point arithmetic. If we instead consider elliptic curves over $\mathbb{Q}_q$, we can generate $H_D(X)$ using $q$-adic arithmetic, which has many advantages. Of course, the reduction of $H_D(X)$ modulo $p$ splits as before into linear factors, whose roots are $j$-invariants of the elliptic curves over $\mathbb{F}_p$ which we eventually want to generate.

The advantage of working in a $q$-adic setting is that the $q$-adic accuracy is preserved when adding or multiplying two integers. If $n$ and $m$ are known with $q$-adic accuracy up to $O(q^k)$ then $nm$ and $n + m$ are also known up to $O(q^k)$. This is of course not true over the real or complex numbers.

For this method to work, we of course need some method to numerically evaluate $j$ over $\mathbb{Q}_q$. This is provided by the recent work of Couveignes and Henocq, using a Newton process that doubles the precision with each iteration, as described in [4]. It would certainly carry us too far to describe this process in any detail. Complexity estimates of the non-archimedean algorithm have not yet been published, to our best knowledge, but the full details should be given in Bröker's forthcoming doctoral thesis (due in 2006).

## 5.5 Using Class Invariants

The coefficients of the Hilbert class polynomial become huge as the class number grows as we have mentioned. Even though our goal is to compute the reduction of this polynomial modulo $p$, the intermediary steps still need to be performed with high precision to ensure that we get the correct result.

From the work of Weber (see [7], for example) we know that we can construct generating polynomials for the Hilbert class fields using various higher level modular functions other than the $j$-function. If we let $\omega$ denote the generator of $\mathcal{O}_K$, the ring of integers of $K = \mathbb{Q}(\sqrt{D})$, we call $u(\omega)$ a *class invariant* if it is contained in $K(j(\omega)) = \mathbb{Q}(\omega, j(\omega))$. It follows that if $u(\omega)$ is a class invariant then so is any of its conjugates. Since we are working only with fundamental discriminants $D$, the field $K(j(\omega))$ is precisely $H$, the Hilbert class field of $K$ (Theorem 2.3). We will refer to the irreducible polynomial of the class invariant $u$ as a *Weber polynomial*, written as $W_D[u](X)$. If we can find a class invariant for $K$ and determine the Galois action of $Cl(D)$ on this invariant, we can compute its minimal polynomial over $K$. Of course, since our goal is to compute $j$-invariants of elliptic curves rather than just generate $H$, we also need some relation to recover $j$ from some value of $u$.

A concise treatment of the vast theory of class invariants is well beyond the scope of this essay. To give some idea of the subject we will look at one example, for a particular congruence class of $D$, in the complex analytic setting. Bröker and Stevenhagen [4] describe how the non-archimedean approach can be adapted to work with Weber polynomials as well as Hilbert polynomials, the full details of which will be published in Bröker's doctoral thesis. To our best knowledge, there are yet no published results concerning the extension of the CRT method to work with class invariants.

Assume that $\tau$ is a quadratic number defined by $a\tau^2 + b\tau + c = 0$. Then we define

$$f(\tau) = \zeta_{48}^{-1} \frac{\eta(\frac{\tau+1}{2})}{\eta(\tau)}, \tag{25}$$

$$\gamma_2(\tau) = \frac{f(\tau)^{24} - 16}{f(\tau)^8}, \tag{26}$$

where $\zeta_{48}$ is the 48th root of unity in $\mathbb{C}$. We can recover the elliptic modular invariant $j(\tau)$ by

$$j(\tau) = \gamma_2(\tau)^3 = \gamma_3(\tau)^2 + 1728. \tag{27}$$

We have the following theorem [2, Theorem 7.1].

**Theorem 5.3.** *Let $\tau$ be a quadratic number defined by $a\tau^2 + b\tau + c = 0$. If $3 \mid a$, $3 \mid c$ but $3 \nmid b$, then $\mathbb{Q}(\gamma_2(\tau)) = \mathbb{Q}(j(\tau))$.*

Now assume that $D$ is a fundamental discriminant and that $p$ is a rational prime that satisfies the relation $4p = t^2 + s^2|D|$. The roots of $W_D[\gamma_2](X)$ generate the Hilbert class field $H$ of $K = \mathbb{Q}(\sqrt{D})$ and the prime $p$ splits completely in $H$. To construct $W_D[\gamma_2](X)$ we also need to determine the Galois action of $Cl(D)$ on the invariant $\gamma_2(\tau)$. Using the functional equations for $\eta$, Atkin and Morain present a simple algorithm that computes an equivalent form $[a_1, b_1, c_1]$ and a CM-point $\tau_1$ from a given form $[a_0, b_0, c_0]$ and a point $\tau_0$, satisfying Theorem 5.3. We refer to [2, §7.2] for the details. Once we have constructed the Weber polynomial for $\gamma_2$, we recover the $j$-values from the roots of $W_D(X) \equiv 0 \pmod{p}$ in $\mathbb{F}_p$, using formula (27).

**Example 3.** We can use the $\gamma_2$ class invariant to compute the Weber polynomial for discriminant $D = -23$. Starting with $\tau_0$, a root of $3\tau^2 - 7\tau + 6$, we obtain

$$W_{-23}[\gamma_2](X) = X^3 + 155X^2 + 650X + 23375.$$

Clearly this is a more simple expression than the one we obtained by using $j$-invariants in Example 1. Reduction modulo $p = 59$ yields

$$W_{-23}[\gamma_2](X) \equiv (X - 40)(X - 47)(X - 53) \pmod{59}.$$

We verify that $(40)^3 \equiv 44 \pmod{59}$, $(47)^3 \equiv 42 \pmod{59}$ and $(53)^3 \equiv 20 \pmod{59}$, which is in accordance with our previous results.

From this example we see that we reduce the size of the constant term of the class polynomial from 14 decimal digits, when using $j$, to 5 decimal digits, when using $\gamma_2$. According to Cohen [5, §7.6.3] the use of higher class invariants reduces the size of coefficients only up to some constant factor. Although this may be useful in practise, it has of course, according to this, no effect on the *asymptotic* complexity estimate of an algorithm.

# 6 Primality Testing

In 1986 Goldwasser and Kilian presented the first general purpose primality test that was based on the theory of elliptic curves. A crucial step in their method was to search for an elliptic curve with a given number of rational points, by picking random curves and counting points. Although quite powerful in theory, this method proved hard to implement in practice. Soon after, Atkin came up with a better approach. Instead of searching for a curve, he applied the theory of complex multiplication to explicitly construct a curve with the properties needed for the test. We will now finish this essay by briefly describing this elliptic curve primality test, referring the reader to Atkin [2] and Cohen [5] for full details.

Let $N$ denote an integer whose primality is to be tested. The following proposition, which we state without proof, provides the basis for the primality test [5, Propositions 9.2.1 and 9.2.2].

**Proposition 6.1.** *Let $N > 3$ be an integer, $E$ an elliptic curve modulo $N$ and let $m = |E(\mathbb{F}_N)|$. Assume that we know a point $P \in E(\mathbb{F}_N)$ such that $m$ and $P$ satisfy the following conditions.*

*(i) There exists a prime divisor $q$ of $m$ such that $q > \left(N^{1/4} + 1\right)^2$.*
*(ii) $[m]P = O_E = (0 : 1 : 0)$.*
*(iii) $[\frac{m}{q}]P = (x : y : t)$ with $t \in (\mathbb{F}_N)^*$.*

*Then, assuming all computations are possible, $N$ is prime.*

The last statement of this proposition, concerning valid computations, is important. Since $N$ may be composite, we could very well be dealing with elliptic curves over *rings* instead of fields. However, instead of adapting our methods we simply act as if $N$ was prime. Then as soon as some basic arithmetic operation on $E$ fails, we know that $N$ must indeed be composite.

The first step of the primality test is to see whether $N$ is small enough to be easily factored using simple methods, such as trial division. We arbitrarily set a threshold $B$ that determines our action, e.g. $B = 10^{20}$. If $N$ is larger than $B$, then we progress to find a fundamental discriminant $D$ which satisfies the conditions of Theorem 2.4 for some $t$ and $s$, and for which $m = N + 1 - t$ has a large factor $q$ which is a probable prime. To solve for $t$ and $s$ we can use a well-known algorithm of Cornacchia (see [14] for a recent version that has been optimised for our purpose). Once such a discriminant has been found, we progress to compute the equation of an elliptic curve $E$ over $\mathbb{F}_N$ with $m$ rational points, using the CM method. Of course, if anything fails at this stage, we immediately abort the algorithm and output that $N$ is composite. After we have found the equation for $E$, we pick a random point $P$ and see if conditions (ii) and (iii) of Proposition 6.1 hold. If that is the case, then all there is left is to verify that $q$ is indeed a prime. We do that by making a *recursive* call to the primality testing procedure. This produces a tower of probable primes which acts as a certificate for the primality of $N$: If one term fails to be prime then the previous term is neither a prime, and the whole tower crumbles. The recursive process should terminate as $q < N$. In fact, since $q$ is always less than half of $N$, we expect the number of recursive calls to be $O(\log N)$. We summarise what has been said in the following algorithm.

```
AGK-Primality-Test(N)
if $N < B$ then
    Trial divide to see if $N$ is prime, return ‘prime’ or ‘composite’ accordingly.
end
repeat
    Find a fundamental discriminant $D$ such that $N$ splits as a product of two elements in the ring $\mathcal{O}_K$ of integers in $K = \mathbb{Q}(\sqrt{-D})$, i.e. $p = \pi\bar{\pi}, \pi \in \mathcal{O}_K$.
    $m \leftarrow N + 1 - (\pi + \bar{\pi})$
until $m = kq$ with $k > 2$ and $q > \left(N^{1/4} + 1\right)^2$ a probable prime
Compute $E$ with $m$ rational points by the CM method
Search for a rational point $P$ such that $[m]P = O_E$ but $[\frac{m}{q}]P \neq O_E$.
if there is such a point $P$ with $m > (N^{1/4} + 1)^2$ then
    if AGK-Primality-Test(q) =‘prime’ then
        return ‘prime’
    else
        return ‘composite’
    end
end
```

# References

[1] Amod Agashe, Kristin Lauter, and Ramarathnam Venkatesan. Constructing elliptic curves with a known number of points over a prime field, 2000.

[2] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–63, 1993.

[3] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. `pari/gp`, a computer algebra package, 2004. URL `http://www.parigp-home.de`.

[4] Reinier Bröker and Peter Stevenhagen. Elliptic curves with a given number of points. In Duncan A. Buell, editor, *Algorithmic Number Theory, 6th International Symposium, ANTS-VI*, volume 3076 of *Lecture Notes in Computer Science*, pages 117–131, Burlington, VT, USA, June 13-18, 2004, 2004. Springer.

[5] Henri Cohen. *A course in computational algebraic number theory.* Graduate texts in mathematics **138**. Springer, Berlin/London, 1993.

[6] David A. Cox. *Primes of the form $x^2+ny^2$ : Fermat, class field theory, and complex multiplication.* Wiley, New York, 1989.

[7] E. Kaltofen and N. Yui. Explicit construction of the hilbert class fields of imaginary quadratic fields by integer lattice reduction. In *Number Theory*, pages 149–202, New York/London, 1991. Springer.

[8] Donald Ervin Knuth. *The art of computer programming. 2nd ed. Vol.2.* Addison-Wesley, Reading, Mass., 1981.

[9] Neal Koblitz. *Introduction to elliptic curves and modular forms.* Graduate texts in mathematics **97**. Springer, New York/London, 1984.

[10] Serge Lang. *Elliptic functions.* Graduate texts in mathematics **112**. Springer, New York/London, 2nd edition, 1987.

[11] Serge Lang. *Algebraic number theory.* Graduate texts in mathematics **110**. Springer, New York/London, 1986.

[12] A. K. Lenstra and Jr. H. W. Lenstra. Algorithms in number theory. In *Handbook of theoretical computer science (vol. A): Algorithms and complexity*, pages 673–715. MIT Press, 1990.

[13] F. Morain. Construction of hilbert class fields of imaginary quadratic fields and dihedral equations modulo $p$. Technical Report RR-1087, INRIA, 1989 1989.

[14] Francois Morain. Implementing the asymptotically fast version of the elliptic curve primality proving algorithm, 2005.

[15] Francois Morain. Implementation of the atkin-goldwasser-kilian primality testing algorithm. Technical Report RR-0911, INRIA, 1988.

[16] Joseph H. Silverman. *The arithmetic of elliptic curves.* Graduate texts in mathematics **106**. Springer, New York/London, 1986.