Università degli Studi Roma Tre
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea Magistrale in Matematica

Tesi di Laurea Magistrale in Matematica

Elliptic Curve Primality Proving

SINTESI

Candidata:
Alessandra Albanese

Relatore:
Prof. David Kohel
Referente Interno:
Prof. Francesco Pappalardi

Anno Accademico 2012-13
Sessione di Luglio 2013

Prime numbers are the building blocks of the integers. They are very important in mathematics and in public-key cryptography, where they are the basis of many algorithm such as the RSA cryptosystem algorithm. There are infinitely many prime numbers, as proved by Euclid in 300 BC, but given a large number, how might one say whether it is prime or not?

The most simple method to check whether a number n is prime or not, is trial division, which consists of dividing n by each integer m that is greater than 1 and less than equal to the square root of n. If the result of any of such division is an integer then n is composite, otherwise it is a prime. This method is of little practical use since it is very slow, but if n is composite it provides a factor of n. Modern primality tests can be divided into two main classes, probabilistic (or Monte Carlo) and deterministic algorithms. Probabilistic tests have the following form: "*If n is prime, then S is true about n*" where S is some easily verifiable arithmetic statement. If one wishes to check whether n is prime or composite, such tests verify the arithmetic statement S to see whether it holds for n. If the statement fails, n is composite. If the statement holds, however, it may be that n is prime, or that n is composite. Composite numbers that are recognized as prime by such tests are referred to as pseudoprimes.

Deterministic algorithms on the other hand do not erroneously report composite numbers as prime while probabilistic methods are typically faster. So typically former first check whether a number is composite by applying the latter. It is interesting to note that methods to determine primality, other than attempting to factorize, do not give any indication of the factors of the number when it turns out to be composite.

The fastest deterministic algorithm is known as "elliptic curve primality proving" (ECPP).

1 Elliptic functions

Let $\{e_1, \ldots, e_m\}$ be a linearly independent set of vectors in $\mathbb{R}^n$ (so that $m \leq n$). The additive subgroup of $(\mathbb{R}^n, +)$ generated by $e_1, \ldots, e_m$ is called a *lattice of dimension m, generated by* $e_1, \ldots, e_m$. As regard the group-teoretic structure, a lattice of dimension m is a free abelian group of rank m. Lattices are additives subgroup of $\mathbb{R}^n$.

Let ω_1 and ω_2 be two complex numbers (considered as two vectors in $\mathbb{R}^2$) linearly independent over $\mathbb{R}$. Over the complex numbers a lattice Λ associated with ω_1 and ω_2 is defined to be

$$\Lambda = \{m\omega_1 + n\omega_2 \, : \, n, m \in \mathbb{Z}\}. \tag{1.1}$$

We will write $\Lambda = [\omega_1, \omega_2]$.

Two lattices in $\mathbb{C}$ are said *homothetic* if and only if there exists an $\alpha \in \mathbb{C}^*$ such that $\Lambda_1 = \alpha\Lambda_2$. Homothety is a equivalence relation.

Let Λ be a lattice in $\mathbb{C}$, we are interested in meromorphic functions on $\mathbb{C}/\Lambda$, which can be thought of as a functions on $\mathbb{C}$ which are doubly periodic with respect to the lattice Λ. We define an *elliptic function* to be a meromorphic function on the 2-dimensional torus. The simplest construction of non-constant elliptic functions is due to Weierstrass.

Definition 1. *Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function (relative to Λ) is defined by the series*

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right),$$

an define the Eisenstein series of weight $2k$ (for Λ) as the series

$$G_{2k}(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \omega^{-2k}.$$

The Weierstrass $\wp$-function satisfies the differential equation

$$\wp'(z) = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6$$

for all $z \in \mathbb{C}$ with $z \notin \Lambda$.
It is standard notation to set

$$g_2 = g_2(\Lambda) = 60G_4 \quad \text{and} \quad g_3 = g_3(\Lambda) = 140G_6.$$

We set

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2.$$

The number $\Delta(\Lambda)$ is closely related to the discriminant of the polynomial $x^3 - 27g_2(\Lambda)x - g_3(\Lambda)$ that appears in the differential equation for $\wp(z)$.

Proposition 1.1. *If $\Lambda \subset \mathbb{C}$ is a lattice, then $\Delta(\Lambda) \neq 0$.*

The j-invariant of the lattice Λ is defined to be the complex number

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2} = 1728 \frac{g_2(\Lambda)^3}{\Delta(\Lambda)} \tag{1.2}$$

The number $j(\Lambda)$ is always defined since $\Delta(\Lambda) \neq 0$. The j-invariant $j(\Lambda)$ characterizes the lattice Λ up to homothety, indeed we have the following:

Theorem 1.2. *If Λ and Λ' are lattices in $\mathbb{C}$, then $j(\Lambda)$=$j(\Lambda')$ if and only if Λ and Λ' are homothetic.*

Given a lattice $\Lambda = [\omega_1, \omega_2]$, it is homothetic to the lattice $\Lambda = [1, \tau]$, where $\tau = \frac{\omega_1}{\omega_2}$. Since the j-function characterize the lattices up to homothety we will write $j(\tau)$ as for $j(\Lambda)$ where $\Lambda = [1, \tau]$ is the lattice homothetic to the lattice $\Lambda = [\omega_1, \omega_2]$ with $\tau = \frac{\omega_1}{\omega_2}$.
The j- function is a modular function, which is a meromorphic function on $\mathcal{H}^*$ invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$. In particular it is periodic of period 1, hence it has a Fourier series expansion:

Theorem 1.3. *There exist positive integers c_n, such that, if we set $q = e^{2i\pi\tau}$, we have for all complex τ with* $\operatorname{Im} \tau > 0$*:*

$$j(\tau) = \frac{1}{q} + 744 + \sum_{n \geq 1} c_n q^n.$$

We describe a way to compute the numerical value of the function $j(\tau)$ for $\tau \in \mathcal{H}$. It is useful to have τ with the largest possible imaginary part, hence to use $j(\tau) = j(A(\tau))$ for any $A \in SL_2(\mathbb{Z})$, for this we refer to [Coh93]. It is based on the following formulas.

Set $q = e^{2\pi i\tau}$, and

$$\Delta(\tau) = q\left(1 + \sum_{n\geq 1}(-1)^n \left(q^{n(3n-1)/2} + q^{n(3n+1)/2}\right)\right)^{24}.$$

This expression should be computed as written. The convergence is better than that of an ordinary power series since the exponents grow quadratically. We have also the following

$$g_2^3 - 27g_3^2 = \left(\frac{2\pi}{\omega_2}\right)^{12}\Delta.$$

Now the formula that we will use for computing $j(\tau)$ is

$$j(\tau) = \frac{(256f(\tau)+1)^3}{f(\tau)} \qquad \text{where} \qquad f(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)} \tag{1.3}$$

(note that changing τ into 2τ changes q into q^2).

2 Elliptic curves

Let K be a field. Elliptic curves with coefficient in K are curves of genus 1 having a specified base point. Every such curve can be written as the locus in $\mathbb{P}^2$ of a cubic equation with only one point (the base point) on the line at ∞, as an equation of the form (*Weierstrass equation*)

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3 \tag{2.1}$$

Here $O = [0, 1, 0]$ is the base point, and $a_1, \ldots, a_6 \in \overline{K}$.

(x, y, z) is a solution if and only if (tx, ty, tz) is also a solution, for $t \in K$, $t \neq 0$. Thus, in the projective case, it makes more sense to talk of $[x, y, z]$ being a solution, where the notation indicate that we consider as identical any two solution (x, y, z), (x', y', z') if and only if there is a nonzero $t \in K$ with $x' = tx$, $y' = ty$, $z' = tz$.

We will usually write the Weierstrass equation for the elliptic curve using non-homogeneous coordinates $x = x/z$ and $y = y/z$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.2}$$

always remembering that there is the extra point $O = [0, 1, 0]$ at the infinity. If $a_1, \ldots, a_6 \in K$, then E is said to be *over* K.

The projective solutions are almost exactly the same as the affine solutions of 2.2. In particular, a solution (x, y) of 2.2 may be identified with the solution $[x, y, 1]$ of 2.1, and any solution $[x, y, z]$ of 2.1 with $z \neq 0$ may be identified with the solution $(x/z, y/z)$ of 2.2. The solution $[x, y, z]$ with $z = 0$ do not correspond to any affine solutions, and are called the “points at infinity” for the equation.

If $char(\overline{K}) \neq 2$ then we can simplify the equation by completing the square. Thus replacing y by $\frac{1}{2}(y - a_1x - a_3)$ gives an equation of the form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6 \tag{2.3}$$

where

$$\begin{cases} b_2 &= \quad a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= \quad a_3^2 + 4a_6 \end{cases}$$

If further $char(\overline{K}) \neq 2, 3$, then replacing (x, y) by $(\frac{(x-3b_2)}{36}, \frac{y}{216})$ eliminates the x^2 term, yielding the simpler equation

$$E : y^2 = x^3 + ax + b \tag{2.4}$$

where

$$a = 27(b_2^2 - 24b_4) \quad \text{and} \quad b = 54(b_2^3 + 36b_2b_4 - 216b_6).$$

This equation has associated quantities

$$\Delta = -16(4a^3 + 27b^2), \qquad j = 1728\frac{(4a)^3}{\Delta}$$

The quantity Δ given above is called the *discriminant* of the Weierstrass equation, j is called the *j-invariant* of the elliptic curve E.

Proposition 2.1. *1. The curve given by a Weierstrass equation is nonsingular if and only if $\Delta \neq 0$.*

2. Two elliptic curves are isomorphic over $\overline{K}$ if and only if they both have the same j-invariant.

3. Let $j_0 \in \overline{K}$. There exists an elliptic curve defined over $K(j_0)$ whose j-invariant is equal to j_0.

We describe now a way to add two points on a given elliptic curve.
If P_1 and P_2 are two points on the curve, then we can uniquely describe a third point which is the intersection of the curve with the line through P_1 and P_2. If the line is tangent to the curve at a point, then that point is counted twice; and if the line is parallel to the y-axis, we define the third point as the point "at infinity". Exactly one of these conditions then holds for any pair of points on an elliptic curve.
It is then possible to introduce a group operation, $+$, on the curve: if one take two points P_1 and P_2, and draw a line through them, then this line intersects an elliptic curve in three points (including multiplicities) P_1, P_2, P_3. If P_3 is the third point on this line, then draw the vertical line through P_3. $P_1 + P_2$ is the unique other point on this vertical line. This description of the group law can be summed up as follows:

Theorem 2.2. *Let E be an elliptic curve. The group law on E is determined by a choice $O \in E$ of an identity point and declaring that if three points of $P_1, P_2, P_3 \in E$ lie on the same line (counted with multiplicity) then*

$$P_1 + P_2 + P_3 = O.$$

With the binary operation defined above, $E(K)$ is an abelian group (with O as identity).
For $m \in \mathbb{Z}$ and $P \in E$, we define

$$[m]P = P + \cdots + P \quad \text{with } m \text{ terms, if} \quad m > 0$$

and

$$[m]P = -P \cdots - P \quad \text{with } |m| \text{ terms, if} \quad m < 0$$

moreover

$$[0]P = 0.$$

Definition 2. *The order of P is the smallest positive integer k such that $kP = O$.*

Since $E(\overline{K})$ is a group, for all $m \in \mathbb{Z}$ we can consider the homomorphism $[m] : E(\overline{K}) \to E(\overline{K})$ which associate to a point P the point mP. This map is given by a polynomial expression and so is a morphism of curves.
The kernel of $[n]$, denoted by $E[n]$, satisfies

$$E[n] = \{P \in E(\overline{K}) \mid [n]P = O\}.$$

This is the set of the points P whose order divides n. An element $P \in E[n]$ is called a n-torsion point.
Over the complex numbers, Weierstrass elliptic function $\wp$ gives us from a torus the algebraic form of the elliptic curve, via the map

$$\begin{array}{rcl} \phi : \mathbb{C}/\Lambda & \to & E \subset \mathbb{P}(\mathbb{C}) \\ z & \to & [\wp(z), \wp'(z), 1] \end{array} \tag{2.5}$$

with $\phi(\Lambda) = [0, 1, 0]$.
There is another form of Weierstrass equation for elliptic curves.

Definition 3. *A Weierstrass equation is in Legendre form if it can be written as*

$$E_\lambda : \; y^2 = x(x-1)(x-\lambda). \tag{2.6}$$

The j-invariant of E_λ is $2^8 \frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$.
All the 2-torsion points of a Legendre curve are rational.
If E is a curve elliptic over a finite field $\mathbb{F}_q$ of odd characteristic, and it is Legendre isogenous (which means isogenous to a Legendre elliptic curve $E_\lambda(\mathbb{F}_q)$), then $|E(\mathbb{F}_q)| \equiv 0 \pmod 4$, since $E_\lambda(\mathbb{F}_q)$ contains the whole 2-torsion

subgroup.

Let K be a finite field of characteristic $p > 0$, with $q = p^r$ elements and let E/K be an elliptic curve. Since there are only finitely many pairs (x, y) with $x, y \in K$, the group of the points over the elliptic curve is finite.

We have the following theorem which defines the structure of the group of the elements of the curve:

Theorem 2.3. *Let E be an elliptic curve over the finite field $\mathbb{F}_q$. Then*

$$E(\mathbb{F}_q) \cong \mathbb{Z}_n \qquad \textit{or} \qquad E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers n_1, $n_2 \geq 1$ with n_1 dividing n_2.

The following theorem, due to Hasse, gives a bound of the elements of the curve.

Theorem 2.4. *Let E/K be an elliptic curve defined over the field with q elements. Then*

$$|\#E(K) - q - 1| \leq 2\sqrt{q} \tag{2.7}$$

Although it provides an estimate of the elements of the curve, it's not so easy to determine the cardinality of the group.

We wish to estimate how many points there are in $E(K)$, or equivalently, one more (the point at infinity) than the the number of solution to the equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (x, y) \in K$$

or, if $p \neq 2, 3$:

$$y^2 = x^3 + Ax + B, \qquad (A, B) \in \mathbb{K}$$

Since each value of x yield at most two values of y, a trivial upper bound is $2q + 1$.

To make a list of points on $y^2 = x^3 + Ax + B$ over a finite field, we try each possible value of x, then find the square roots y of $x^3 + Ax + B$, if they exist. This procedure is the basis for a simple point counting algorithm.

Let $P \in E(\mathbb{F}_q)$. A fundamental result from group theory (a corollary of

Lagrange's Theorem) is that the order of a point always divides the order of the group. Also, for an integer n, we have $nP = O$ if and only if the order of P divides n. By Hasse's Theorem, $\#E(\mathbb{F}_q)$ lies in an interval of length $4\sqrt{q}$. Therefore, if we can find a point of order greater than $4\sqrt{q}$, there can be only one multiple of this order in the correct interval, and it must be $\#E(\mathbb{F}_q)$. Even if the order of the point is smaller than $4\sqrt{q}$, we obtain a small list of possibilities for $\#E(\mathbb{F}_q)$. Using a few more points often shortens the list enough that there is a unique possibility for $\#E(\mathbb{F}_q)$. This is the base of the Baby Steps, Giant Step method to find the order of the group.
For an elliptic curve E over $\mathbb{F}_q$ the number $\#E(\mathbb{F}_q)$ can also be computed by means of the division point method, due to Schoof ([Sch85]). This method is based on the Hasse's Theorem which implies the there is only a finite range of possible values for $|E(\mathbb{F}_q)|$. It suffices to compute $|E(\mathbb{F}_q)|$ modulo primes $l_1, \dots, l_s$ whose product exceeds $4\sqrt{q}$, and then applying the Chinese remainder Theorem. In order to efficiently compute $|E(\mathbb{F}_q)|$ modulo l_i the algorithm uses the division polynomial ψ_l.
There is another method to compute the number of points of an elliptic curve over a finite field which make use of the theory of complex multiplication. We shall describe it later.

3 Quadratic fields

We recall now some notions about algebraic number theory.
An ideal may be described as an $\mathcal{O}_K$-submodule of $\mathcal{O}_K$, so we look at $\mathcal{O}_K$-submodules of the field K.

Definition 4. *An $\mathcal{O}_K$-submodule $\mathfrak{a}$ of K is called a fractional ideal of $\mathcal{O}_K$ if there exists some nonzero $c \in \mathcal{O}_K$ such that $c\mathfrak{a} \subseteq \mathcal{O}_K$.*

Definition 5. *A fractional ideal of $\mathcal{O}_K$ is principal if it is of the form $c^{-1}\mathfrak{a}$ where $\mathfrak{a}$ is a principal ideal of $\mathcal{O}_K$.*

Let $\mathcal{F}$ be the group of fractional ideals under multiplication. The set $\mathcal{P}$ of principal fractional ideals is a soubgroup of $\mathcal{F}$.

Definition 6. *We define the class group of $\mathcal{O}_K$ to be the quotient group*

$$\mathcal{H} = \mathcal{F}/\mathcal{P}.$$

The *class number* $h = h(\mathcal{O}_K)$ is defined to be the order of $\mathcal{H}$.

Theorem 3.1. *The class group of a number field is a finite abelian group. The class number h is finite*

A quadratic field is a number field K of degree 2 over $\mathbb{Q}$. Then $K = \mathbb{Q}(\theta)$ where θ is an algebraic integer, and θ is a zero of

$$t^2 + at + b \qquad (a, b \in \mathbb{Z}).$$

The quadratic fields are those of the form $\mathbb{Q}(\sqrt{d})$, for d a squarefree rational integer.
The discriminant of $\mathbb{Q}(\sqrt{d})$ is

1. $4d$ if $d \not\equiv 1 \pmod 4$

2. d if $d \equiv 1 \pmod 4$

Let d_K the discriminant of $K = \mathbb{Q}(\sqrt{d})$, we can describe the ring of integers $\mathcal{O}_K$ as follows:

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{d_K + \sqrt{d_K}}{2}\right]$$

Definition 7. *An order $\mathcal{O}$ in a quadratic field K is a subset $\mathcal{O} \subset K$ such that $\mathcal{O}$ is a subring of K containing* 1, *$\mathcal{O}$ is a finitely generated $\mathbb{Z}$-module, $\mathcal{O}$ contains a $\mathbb{Q}$-basis of K.*

Proposition 3.2. *If Λ is an order, there exists $\tau \in \mathbb{C}$ such that $\Lambda = [1, \tau]$, and the lattice with basis $1, \tau$ is an order if and only if τ is a complex quadratic algebraic integer.*

A quadratic form in two variables is an homogenous polynomial of degree two:

$$f(x, y) = ax^2 + bxy + cy^2 \qquad a, b, c \in \mathbb{Z} \tag{3.1}$$

which is denoted more briefly by (a, b, c).

These forms are considered under an equivalence relation. One can associate to each form its discriminant D and compute the number $h(D)$ of reduced forms of such discriminant. If $D < 0$ each equivalence class contains exactly one form called reduced. The set of reduced forms of discriminant D is a finite abelian group called the *form group*. There is an algorithm, due to Cornacchia which find the solutions of the equation $x^2 + |D|y^2 = 4p$ or says that such a solution does not exists, when one work in complex quadratic orders of discriminant $-D$ (with $D > 0$) congruent to 0 or 1 modulo 4, and p an odd prime:

1. If $p = 2$ do as follows. If $D + 8$ is the square of an integer, output $(\sqrt{D+8}, 1)$, otherwise say that the equation has no solution. Then terminate the algorithm.

2. Compute $k \leftarrow \left(\frac{D}{p}\right)$. If $k = -1$, say that the equation has no solution and terminate the algorithm.

3. Compute an integer x_0 such that $x_0^2 \equiv D \pmod{p}$ and $0 \leq x_0 < p$, and if $x_0 \not\equiv D \pmod{2}$, set $x_0 \leftarrow p - x_0$. Finally, set $a \leftarrow 2p$, $b \leftarrow x_0$ and $l \leftarrow \lfloor 2\sqrt{p} \rfloor$.

4. If $b > l$, set $r \leftarrow a \pmod{b}$, $a \leftarrow b$, $b \leftarrow r$ and go to step 4.

5. If D does not divide $4p - b^2$ or if $c = (4p - b^2)/|D|$ is not the square of an integer, say that the equation has no solution and terminate the algorithm. Otherwise output $(x, y) = (b, \sqrt{c})$ and terminate the algorithm.

There is a correspondence between ideals in an order and primitive quadratic forms of a given discriminant D, which implies a correspondence between the ideal class group and the form class group. The correspondence is given by the following theorem:

Theorem 3.3. *Let $\mathcal{O}$ be the order of discriminant D in an imaginary quadratic field K.*

1. *If $f(x,y) = ax^2 + bxy + cy^2$ is a primitive positive definite quadratic form of discriminant D, then $[a, (-b+\sqrt{D})/2]$ is a proper ideal of $\mathcal{O}$.*

2. *The map sending $f(x,y)$ to $[a, (-b+\sqrt{D})/2]$ induces an isomorphism between the form class group and the ideal class group $C(\mathcal{O})$. Hence the order of $C(\mathcal{O})$ is the class number $h(D)$.*

3. *A positive integer m is represented by a form $f(x,y)$ if and only if m is the norm $N(\mathfrak{a})$ of some ideal $\mathfrak{a}$ in the corresponding ideal class in $C(\mathcal{O})$ ($N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}|$).*

Given an order $\mathcal{O}$ in an imaginary quadratic field K of discriminant D, we have seen that it is a lattice in the complex numbers. The j-invariant $j(\mathcal{O})$ is an algebraic integer. We will denote $H_{\mathcal{O}}(X)$ its monic minimal polynomial over $\mathbb{Q}$.

$H_{\mathcal{O}}(X)$, it is called *Hilbert class polynomial*, it has integer coefficients since $j(\mathcal{O})$ is an algebraic integer. The equation $H_{\mathcal{O}}(X) = 0$ is called the *class equation.*

Since $\mathcal{O}$ is uniquely determined by its discriminant D, write $H_D(X)$ is equivalent to write $H_{\mathcal{O}}(X)$.

Hilbert class polynomial is a polynomial of degree $h(D)$ such that the splitting field for the polynomial over $\mathbb{Q}(\sqrt{D})$ has Galois group isomorphic to the class group $C(D)$. This splitting field is called the Hilbert class field for $\mathbb{Q}(\sqrt{D})$ and is the largest abelian unramified extension of $\mathbb{Q}(\sqrt{D})$.

The Hilbert class field has the property that a prime number p splits completely in this field if and only if it is principal. In particular, since the Hilbert class field has degree $2h(D)$ over the rational field $\mathbb{Q}$, the proportion, among all primes, of primes p with p principal is $\frac{1}{2h(D)}$. Algorithm to compute H_D are important for elliptic curve primality proving. Now we want to compute the equation of degree $h(D)$, which is the Hilbert class polynomial for the discriminant D. The following algorithm computes the monic polynomial of degree $h(D)$ in $\mathbb{Z}[X]$ of which $j((D+\sqrt{D})/2)$ is a root. We make use of a polynomial variable P.

1. Set $P \leftarrow 1$, $b \leftarrow D \pmod 2$ and $B \leftarrow \lfloor\sqrt{|D|/3}\rfloor$.

2. Set $t \leftarrow (b^2 - D)/4$ and $a \leftarrow \max(b, 1)$.

3. If $a \not| t$ go to step 4. Otherwise compute $j \leftarrow j((-b + \sqrt{D})/2a)$ using the formula 1.3. Now if $a = b$ or $a^2 = t$ or $b = 0$ set $P \leftarrow P \cdot (X - j)$, else set $P \leftarrow P \cdot (X^2 - 2\mathrm{Re}(j)X + |j|^2)$.

4. Set $a \leftarrow a + 1$. If $a^2 \leq t$, go to step 3.

5. Set $b \leftarrow b + 2$. If $b \leq B$, go to step 2, otherwise round the coefficients of P to the nearest integer, output P and terminate the algorithm.

This algorithm compute all the reduced forms (a, b, c) of discriminant D and the quadratic numbers associated.

A drawback of the Hilbert class polynomial is that it has huge coefficients even for quite small discriminant. For this reason Yui and Zagier ([YZ97]) suggest to use the class equation obtained by using the Weber function $\mathfrak{f}(\tau)$, when D is congruent to 1 modulo 8 and not divisible by 3. The values of $\mathfrak{f}$ at suitable points $\tau \in \mathcal{H}$ of discriminant D generate the same fields as before but are the roots of a polynomial $W_D(X)$ having far smaller coefficients than $H_D(X)$.

Enge and Schertz [ES04] suggest to use double η quotient as class invariants. Double η quotient are a generalization of the simple η quotients which are given by

$$\mathfrak{m}_l(z) = \frac{\eta(z/l)}{\eta(z)}$$

for some integer l, and $\eta(z)$ is the Dedekind η-function given by

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n)$$

where $q = e^{2\pi i z}$. This approach, unlike the one above, can be used for any imaginary quadratic order, regardless the discriminant.

Sutherland [Sut12] instead, does not make use of modular function different from j, and compute H_D and not other class invariant. His approach is remarkable since the algorithm to compute $H_D(X)$ make use of the Chinese Remainder Theorem and it runs in $\mathcal{O}(|D|(\log|D|)^{5+o(1)})$. He make use of the isogeny volcanoes. A volcano is a certain type of graph, which typically consists of a cycle with isomorphic balanced trees rooted at each vertex. Volcanos arise as components of graph of isogenies between elliptic curves. Sutherland shows how isogeny volcanoes can be used to solve the problem of finding the Hilbert class polynomial, yielding an asymptotic improvement over the previous results.

4 Endomorphisms of an elliptic curve

We can now see at the endomorphisms of an elliptic curve E.
Endomorphisms are group homomorphisms from the group E to itself that are given by rational functions. The set of such endomorphisms, denoted by $\text{End}(E)$, naturally forms a ring, where addition is derived from elliptic addition, and multiplication is composition.
If n is an integer, the map $[n]$ that sends a point P on E to $[n]P$ is an element of $\text{End}(E)$, since it is a group homomorphism and $[n]P$ has coordinates that are rational functions of the coordinates of P. The ring $\text{End}(E)$ contains thus an isomorphic copy of the ring of integers $\mathbb{Z}$.
We say that an elliptic curve has complex multiplication if $\text{End}(E)$ is larger than $\mathbb{Z}$.
If the elliptic curve E is defined over the complex numbers, the following theorem gives us the classification of the possible endomorphisms rings of the curve E.

Theorem 4.1. *Let $E/\mathbb{C}$ be an elliptic curve, and let ω_1 and ω_2 be generators for the lattice Λ associated to E by 2.5. Then either*

i $\text{End}(E) = \mathbb{Z}$*; or*

ii $\mathbb{Q}(\omega_1/\omega_2)$ *is a quadratic imaginary extension of* $\mathbb{Q}$*, and E is isomorphic to an order in* $\mathbb{Q}(\omega_1/\omega_2)$

Let E an elliptic curve definite over some finite field $\mathbb{F}_q$. The Frobenius endomorphism F_q satisfies the quadratic equation

$$F_q^2 - tF_q + q = 0 \tag{4.1}$$

in the endomorphism ring $\mathrm{End}(E)$, where $|t| \leq 2\sqrt{q}$. If $|t| < 2\sqrt{q}$, then this polynomial has only complex roots, so $F_q \notin \mathbb{Z}$. Therefore

$$\mathbb{Z} \neq \mathbb{Z}[F_q] \subseteq \mathrm{End}(E).$$

The subring $\mathbb{Z}[F_q]$ generated by Frobenius is isomorphic to the imaginary quadratic order $\mathcal{O}_D$ of discriminant $D = t^2 - 4q$, with $\mathbb{F}_q$ corresponding to the element $\frac{t+\sqrt{D}}{2} \in \mathcal{O}_D$ of trace t and norm q.

When $t = \pm 2\sqrt{q}$, the ring of endomorphism is still larger than $\mathbb{Z}$, in fact the endomorphism ring is an order in a quaternion algebra.

This means that an elliptic curve E over a finite field $\mathbb{F}_q$ always has complex multiplication.

Knowing the complex multiplication field K gives a fast way of computing the cardinality of the curve $E(\mathbb{F}_q)$. Suppose that K is known for some elliptic curve E, then the ring of integers $\mathcal{O}_K$ contains the zeros $\pi, \overline{\pi}$ of the polynomial $X^2 - tX + q$, and $|E(\mathbb{F}_q)| = (\pi - 1)(\overline{\pi} - 1)$. Although this polynomial is not known, a zero can be determined by looking for an element π in $\mathcal{O}_K$ for which $\rho\overline{\rho} = q$. This ρ can be shown to be unique up to complex conjugation and units in $\mathcal{O}_K$. For a suitable units u in $\mathcal{O}_K$ we then have that $\pi = u\rho$, so that $|E(\mathbb{F}_q)| = (u\rho - 1)(\overline{u\rho} - 1)$. In most cases $\mathcal{O}_K$ will have only two units: 1 and -1, only if $K = \mathbb{Q}(i)$ (or $K = \mathbb{Q}(\sqrt{-3})$) we have four (or six) units in $\mathcal{O}_K$. In the case that $\mathcal{O}_K$ has only the units 1 and -1, an immediate method to decide wether $|E(\mathbb{F}_q)|$ equals $(\rho - 1)(\overline{\rho} - 1) = m'$ or $(-\rho - 1)(-\overline{\rho} - 1) = m''$ does not yet exist. In practice one could select a random point $P \in E(\mathbb{F}_q)$ such that not both $m' \cdot P$ and $m'' \cdot P$ are equal to O, so that $|E(\mathbb{F}_q)| = m$ for the unique $m \in \{m', m''\}$ for which $m \cdot P = O$. If $\mathcal{O}_K$ contains four or six units there exists a more directed method.

5 Elliptic curve primality proving

We describe now the elliptic curve primality proving.
The basic theorem which will enable us to prove that n is prime is the following due to Goldwasser and Kilian:

Theorem 5.1. *Let n be an integer coprime to 6 and different from 1, and E an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$. Let m and s be positive integer with s dividing m.*
Supposte there is a point $P \in E(\mathbb{Z}/n\mathbb{Z})$ satisfying the following conditions

- $mP = O$
- *$(m/q)P$ is defined and different from O, for each prime q dividing s.*

Then $|E(\mathbb{Z}/p\mathbb{Z})| \equiv 0 \pmod{s}$ for every prime p dividing n, and if $s > (\sqrt[4]{n}+1)^2$ then n is prime.

We recall that by the symbol $E(a, b)$ we mean the elliptic curve E of equation $y^2 = x^3 + ax + b$.
This is the procedure to prove the primality of a number n making use of the above theorem.
First select an elliptic curve $E(a, b)$ over $\mathbb{Z}/n\mathbb{Z}$ and an integer m, such that $m = |E(\mathbb{Z}/n\mathbb{Z})|$ if n is prime, and such that m can be written as kq for a small integer $k > 1$ and probable prime $q > (\sqrt[4]{n} + 1)^2$. There is two method to select E and m, which leads to Goldwasser-Kilian's algorithm and Atkin-Morain's algorithm. Next find a point $P \in E(\mathbb{Z}/n\mathbb{Z})$ satisfying the requirements in the Theorem 5.1 with $s = q$, on the assumption that q is prime. This is done as follows. First, find a random point $P \in E(\mathbb{Z}/n\mathbb{Z})$. Next, compute $(m/q) \cdot P = k \cdot P$, if $k \cdot P$ is undefined, we find a nontrivial divisor of n. If $k \cdot P = 0$, select a new P and try again. Otherwise, verify that $q \cdot (k \cdot P) = m \cdot P = 0$, which must be the case if n is prime, because in that case $|E(\mathbb{Z}/n\mathbb{Z})| = m$. The existence of P now proves that n is prime if q is prime. Finally the primality of q is proved recursively, by applying the

above process to $n' = q$.

This idea forms the *downrun* process. One build a decreasing sequence of probable primes $n_0 > n_1 > \cdots > n_k$ such that the primality of n_{i+1} implies that of n_i, and the last number n_k is so small that it can be proved prime by trial division. Iterating the algorithm not only provides a rigorous primality test but also generates a certificate of primality.

Definition 8. *The certificate of primality is a chain*

$$(n = n_0, a_0, b_0, m_0, q_0, P_0),\ \ldots\ , (q_{k-1} = n_k, a_k, b_k, m_k, q_k, P_k) \tag{5.1}$$

consisting of consecutive $n_i, a_i, b_i, m_i, q_i, P_i$ *entities along the recursion.*

Theorem 5.2. *The certificate of primality obtained by the algorithm of Goldwasser-Kilian and Atkins-Morain can be checked in polynomial time.*

The primary feature of the certificate is that it can be published associated with the original n that is proven prime. This concise listing can then be used by anyone who wishes to verify that n is prime, using Theorem 5.1 at the various steps along the way. The certificate feature is nontrivial, since many primality proofs must be run again from scratch if they are to be checked.

5.1 Goldwasser and Kilian test

The idea of Goldwasser and Kilian [**?**] is to make use of the algorithm of Schoof [Sch85] which computes the number of points on an elliptic curve defined over a finite field. The algorithm selects a random elliptic curve E modulo n and try to compute its number of points with Schoof's algorithm. If this algorithm works, then it produces an integer m that is the cardinality of the elliptic curve if n is prime. If the algorithm does not work, then n is not prime, since it is guaranteed to work for prime n. This must be repeated until m satisfies the requirements.

This is the Goldwasser-Kilian procedure to prove the primality of n:

Let n be a positive integer different from 1 and coprime to 6,

1. set $i = 0$ and $n_i = n$
2. choose a non singular elliptic curve E over $\mathbb{Z}/n_i\mathbb{Z}$
3. compute with Schoof's algorithm the number of points $m = |E(\mathbb{Z}/n_i\mathbb{Z})|$
4. check if $m = 2q$, with q a probable prime; else go to 2
5. choose at random $P \in E(\mathbb{Z}/n_i\mathbb{Z})$
6. compute mP and $(m/q)P$, if during the computation some operation was impossible go to step 9
7. check if $mP = O$, if it is not O go to 9
8. set $i = i + 1$ and $n_i = q$ and go to step 2
9. if $i = 0$ then n is composite, otherwise set $i = i - 1$ and go to step 2

If l is not prime the algorithm may run indefinitely and so should perhaps not be called an "algorithm", however it will never give a false answer.
It can be shown that under hypothesis on the distribution of primes in short intervals, the expected running time of the algorithm is $\mathcal{O}(\log^{12} n)$.
The most expensive part of the test is the $\mathcal{O}(\log^8 n)$ spent counting the points on a given elliptic curve. A recent improvement of the Schoof's algorithm due to Elkies and Atkin decreases the complexity of the algorithm to $\mathcal{O}(\log^6 n)$.

5.2 Atkin and Morain test

In a 1993 paper, Atkin and Morain [AM93] described an algorithm over elliptic curves which avoided the point counting algorithm. The algorithm still relies on the theorem stated above, but one does not start by selecting E but by selecting the complex multiplication field K of E. The field K can be used to calculate m, and only if m is of the required form kq, one determines the pair a, b defining E. This is done as follows. Let D be a negative fundamental discriminant ≤ -7. Denote by K the imaginary quadratic field $\mathbb{Q}(\sqrt{D})$ and by $\mathcal{O}_K = \mathbb{Z}[(D+\sqrt{D})/2]$ its ring of integers. We try to find $\pi\overline{\pi} = n$ in $\mathcal{O}_K$. First one checks whether or not n splits in K. If n is prime, this happens if and only if the discriminant D is a square modulo n. If n splits, one sees whether it is a product of two prime principal ideals. To do this one computes b such that $b^2 \equiv D \pmod{4n}$. Then the ideal I generated by $< n, \frac{b-\sqrt{D}}{2} >$ is a prime divisor of n. To check whether it is principal, one applies a lattice reduction algorithm in the lattice generated by n and $\frac{b-\sqrt{D}}{2}$ in $\mathbb{C}$, to compute a shortest vector. If the shortest vector has norm n, then we take it as our integer π and we know that $I = (\pi)$ is principal. If the norm of the shortest vector is not equal to n, then the ideal I is not principal and there does not exist an algebraic integer $\pi \in \mathbb{Q}(\sqrt{D})$ with $N(\pi) = n$. Assuming that π and D have been computed, then the cardinality of the elliptic curve will be of the form $m = (\zeta\pi - 1)(\overline{\zeta\pi} - 1)$, where $< \zeta >= \mathcal{O}_K^*$. If m is not of the required form kq, we select another D and try again. Supposing that $m = kq$, we explain how to compute the elliptic curve E over $\mathbb{Z}/n\mathbb{Z}$ from the quadratic integer π. Over the complex numbers a curve with complex multiplication by $\mathcal{O}_K$ can be constructed as the curve of j- invariant $j = j\left(\frac{D+\sqrt{D}}{2}\right)$. The j invariant is defined as a complex number, and not as an element of $\mathbb{Z}/n\mathbb{Z}$. In order to compute such value, we consider the minimal monic polynomial H of j in $\mathbb{Z}[X]$, with the methods described above. The degree of this polynomial equals the class number of $K = \mathbb{Q}(\sqrt{D})$, and is therefore $\approx \sqrt{|D|}$ (as these polynomials depends only on D, the should be tabulated). If n is prime, it splits by construction completely in the Hilbert class field H. We compute a root of the minimal polynomial of j in $\mathbb{Z}/n\mathbb{Z}$, and compute the equation of the curve E over $\mathbb{Z}/n\mathbb{Z}$ with j-invariant j. This is made by taking a quadratic non-residue modulo n, putting $g = \frac{j}{1728-j}$, g is well defined and non zero since $D \leq -7$, and choosing E as the elliptic curve $E(3g, 2g)$ or $E(3gc^2, 2gc^3)$. In such a way that $|E(\mathbb{Z}/n\mathbb{Z})| = m$.

If we don't make the restriction $D \leq -7$, one should also consider $D = -3$ (respectively $D = -4$) as it give rise to six (four) pairs E, m; the equations for the curves are

$$E(c^i, 0): \quad y^2 = x^3 - c^i x \qquad \text{for} \qquad 0 \leq i \leq 3$$

(respectively

$$E(0, c^i): \quad y^2 = x^3 - c^i \qquad \text{for} \qquad 0 \leq i \leq 5),$$

with c as above.

Once the elliptic curve has been found, the rest of the algorithm proceeds as in the Goldwasser- Kilian.

We present a heuristic analysis of the algorithm described above.

The dominating complexity of the computation of π is the $\mathcal{O}(\log^3 n)$ to solve the equation $b^2 \equiv D \pmod{n}$, made with a probabilistic algorithm to find the roots of a polynomial over a finite field (See [Knu81]).

It is reasonable to expect that one has to try $\mathcal{O}(\log^{2+\epsilon} n)$ values of D before m has the required form, so that we may assume that the final D is $\mathcal{O}(\log^{2+\epsilon} n)$.

The original version is to realize the Hilbert class field K_H/K via the computation of the minimal polynomial $H_D(X)$ of the special values of the classical j-invariant at quadratic integers.

Let $h(D)$ be the number of classes of $D < 0$, we have that $h(D) = \mathcal{O}(\sqrt{D})$. Evaluating the roots of $H_D(X)$ and building this polynomial con be done in $\mathcal{O}(h^2(D))$ operation (see [Eng09]). As shown above, we can assume that the dimension of D is $\mathcal{O}(\log^{2+\epsilon} n)$, we have thus that the complexity is $\mathcal{O}(\log^{2+\epsilon} n)$.

This polynomial can be computed and tabulated since they depends only on the discriminants.

The computation of a zero of $H_D(X) \pmod{n}$ makes use again of the probabilistic algorithm to compute roots in finite fields. Assuming n prime, a zero of this polynomial can thus be compute in time $\mathcal{O}(\log^{5+\epsilon} n)$, or using fast multiplication techniques in $\mathcal{O}((\deg H(X)) \log^{2+\epsilon} n) = \mathcal{O}(\log^{3+\epsilon} n)$.

The algorithm generates a sequence of probable primes $n = q_0 > q_1 > \cdots > q_k$, for which the primality of q_i proves the one on q_{i+1}, and q_k is such that its primality can be proven with trial divisions. The algorithm searches for an $m = |E(\mathbb{Z}/n\mathbb{Z})|$ such that it can be written as kq for a small integer $k > 1$ and a probable prime $q > (\sqrt[4]{n} + 1)^2$. Hasse-Weil bound states that $|E(\mathbb{Z}/n\mathbb{Z})| = m \leq (\sqrt{n} + 1)^2$. We have thus $q_{i+1} \leq \frac{(\sqrt{q_i}+1)^2}{2} \leq \frac{(\sqrt{q_0}+1)^2}{2^{i+1}}$, and the recursion depth is $\mathcal{O}(\log q_0) = \mathcal{O}(\log n)$.

Heuristically, it follows that the whole primality proof takes time $\mathcal{O}(\log^{6+\epsilon} n)$, or $\mathcal{O}(\log^{5+\epsilon} n)$ using fast multiplication techniques; including the $\mathcal{O}(\log n)$ factor for the recursion. This method has proved to be quite practical.

5.3 Fast version of elliptic curve primality test

There is a fast version of the elliptic curve primality proving of Atkins and Morain, due to Shallit. He has observed that the complexity of the algorithm can be improved to $\mathcal{O}(\log^{4+\epsilon} n)$. If the algorithm of Atkin and Morain makes use of the fast multiplication techniques, the asymptotically most expensive part of the algorithm is the time spent to find a discriminant: this requires $\mathcal{O}(\log^3 n)$ time. The basic idea of the fast version of ECPP is to build a base of small squareroots, and built the discriminant from this basis. In the standard version of the algorithm we need $\mathcal{O}(\log^2 n)$ discriminant to find a good one. In the fast version instead, one can build those discriminant as $-D = (-p)(-q)$, where p and q are taken from a pool of size $\mathcal{O}(\log n)$ primes. If we use such D's that can be written as the product of small primes; to compute the square roots modulo n of the D's, it then suffices to compute the square roots of those small primes, and reuse them, at the cost of some multiplication. The computation of the square roots can be done at the beginning of the computation.

The cost of this new step is that of computing $r = \mathcal{O}(\log n)$ square roots modulo l, for a cost of $\mathcal{O}(\log n \cdot \log^{2+\epsilon} n)$. The new cost of this phase is so $\mathcal{O}(\log^{3+\epsilon} n)$, this decrease the whole cost to $\mathcal{O}(\log^{4+\epsilon} n)$.

5.4 Using $D \equiv 1 \pmod 8$

We present now an improvement due to a choice of a discriminant $D < 0$ such that $D \equiv 1 \pmod 8$.
Let D be a negative fundamental discriminant, $D \equiv 1 \pmod 8$, and let $\mathcal{O}_K = \mathbb{Z}[\omega]$, with ω such that $\omega^2 - \omega + \left(\frac{1-D}{4}\right) = 0$ (so $\omega = \frac{1+\sqrt{D}}{2}$).
If we consider the ideal $(2) \subseteq \mathcal{O}_K$, we have that

$$(2) = (2, \omega)(2, \overline{\omega}) = (2, \omega)(2, 1 - \omega)$$

is the factorization of the ideal $(2) \subseteq \mathcal{O}_K$ in two distinct prime ideals in $\mathcal{O}_K$, indeed $N(\omega) = N\left(\frac{1+\sqrt{D}}{2}\right) = \frac{1-D}{4}$, and since by assumption $D \equiv 1 \pmod 8$, then $2|N(\omega)$.
Let $\rho = (2, \omega)$ and $\overline{\rho} = (2, 1 - \omega)$, and let E be an elliptic curve over a finite field $\mathbb{F}_q$, with endomorphism ring isomorphic to $\mathcal{O}_K$. If we consider the subgroup $E[2]$, which is an element of the endomorphism ring of E, we have

$$E[2] = E[\rho] \oplus E[\overline{\rho}],$$

where $E[\rho] = \{P \in E[\overline{K}] \mid \phi(P) = 0 \;\forall\; \varphi \in \rho\}$.
This implies that $E(\mathbb{F}_q)$ contains the whole 2-torsion subgroup, and thus $|E(\mathbb{F}_q)| \equiv 0 \pmod 4$. During the algorithm of Atkins and Morain, one can thus decide to use only negative discriminants D such that $D \equiv 1 \pmod 8$, since this leads to elliptic curve with cardinality a multiply of 4. This means that since we search for a curve whose cardinality is of the form kq for some B-smooth number k, we know that k is at least 4. This choice of the discriminant make the recursion shorter but limit the set of the discriminant which can be chosen in the first step of the algorithm, and this could lead to Hilbert polynomials with huge coefficients, since they grow with the increasing of D. Remembering that each elliptic curve E over a finite field of odd characteristic, with $|E| \equiv 0 \pmod 4$ is Legendre isogenous, one can use the λ invariant to compute the Hilbert class polynomial. The class polynomial with invariant λ exists always and it's degree is six times smaller, indeed we

can write j in function of λ (as showed above):

$$j(E_\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

and compute the Hilbert class polynomial as a function of λ by homogenizing the polynomial.

The depth of the recursion, with this choice of D is now $\frac{\log n}{2 \log 2}$ which does not change the asymptotic complexity of the algorithm, but makes the primality certificate shorter. We can choose D as the product of 2 distinct primes p and q, such that $D = -pq$, $-pq \equiv 1 \pmod 8$. In order to apply the algorithm for proving the primality of n, we need

$$\binom{D}{n} = 1 = \binom{-1}{n}\binom{p}{n}\binom{q}{n}.$$

We could use now the fast version of ECPP remembering that $-pq \equiv 1 \pmod 8$.

References

[AM93] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203):29–68, 1993.

[AT02] Roland Auer and Jaap Top. Legendre elliptic curves over finite fields. *J. Number Theory*, 95(2):303–312, 2002.

[Coh87] F. R. Cohen. A course in some aspects of classical homotopy theory. In *Algebraic topology (Seattle, Wash., 1985)*, volume 1286 of *Lecture Notes in Math.*, pages 1–92. Springer, Berlin, 1987.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[CP05] Richard Crandall and Carl Pomerance. *Prime numbers*. Springer, New York, second edition, 2005. A computational perspective.

[Eng09] Andreas Enge. The complexity of class polynomial computation via floating point approximations. *Math. Comp.*, 78(266):1089–1107, 2009.

[ES04] Andreas Enge and Reinhard Schertz. Constructing elliptic curves over finite fields using double eta-quotients. *J. Théor. Nombres Bordeaux*, 16(3):555–568, 2004.

[GK99] Shafi Goldwasser and Joe Kilian. Primality testing using elliptic curves. *J. ACM*, 46(4):450–472, 1999.

[Knu81] Donald E. Knuth. *The art of computer programming. Vol. 2*. Addison-Wesley Publishing Co., Reading, Mass., second edition,

1981. Seminumerical algorithms, Addison-Wesley Series in Computer Science and Information Processing.

[Lan94] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[Len87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math. (2)*, 126(3):649–673, 1987.

[Rie85] Hans Riesel. *Prime numbers and computer methods for factorization*, volume 57 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1985.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[ST02] Ian Stewart and David Tall. *Algebraic number theory and Fermat's last theorem*. A K Peters Ltd., Natick, MA, third edition, 2002.

[Sut12] A. V. Sutherland. Isogeny volcanoes. *ArXiv e-prints*, August 2012.

[vL90] Jan van Leeuwen, editor. *Handbook of theoretical computer science. Vol. A*. Elsevier Science Publishers B.V., Amsterdam, 1990. Algorithms and complexity.

[Was08] Lawrence C. Washington. *Elliptic curves*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, second edition, 2008. Number theory and cryptography.

[YZ97] Noriko Yui and Don Zagier. On the singular values of Weber modular functions. *Math. Comp.*, 66(220):1645–1662, 1997.