IMPLEMENTATION OF THE ATKIN-GOLDWASSER-KILIAN PRIMALITY TESTING ALGORITHM

Francois MORAIN * †

morain@inria.inria.fr, morain@frcicg71.bitnet

Abstract. We describe a primality testing algorithm, due essentially to Atkin, that uses elliptic curves over finite fields and the theory of complex multiplication. In particular, we explain how the use of class fields and genus fields can speed up certain phases of the algorithm. We sketch the actual implementation of this test and its use on testing large primes, the records being two numbers of more than 550 decimal digits. Finally, we give a precise answer to the question of the reliability of our computations, providing a *certificate of primality* for a prime number.

IMPLEMENTATION DU TEST DE PRIMALITE D' ATKIN, GOLDWASSER, ET KILIAN

Résumé. Nous décrivons un algorithme de primalité, principalement dû à Atkin, qui utilise les propriétés des courbes elliptiques sur les corps finis et la théorie de la multiplication complexe. En particulier, nous expliquons comment l'utilisation du corps de classe et du corps de genre permet d'accélérer les calculs. Nous esquissons l'implémentation de l'algorithme et son utilisation pour tester la primalité d'entiers très grands, le record actuel étant la certification de deux nombres de plus de 550 chiffres décimaux. Nous donnons une réponse précise à la question de fiabilité des résultats, fournissant un *certificat de primalité* pour un nombre premier.

---

* Département de Mathématiques, Université de Limoges, 123, Avenue Albert Thomas, 87060 LIMOGES CEDEX & Projet ALGO, Institut National de Recherche en Informatique et en Automatique, Domaine de Voluceau, B. P. 105, 78153 LE CHESNAY CEDEX (France).

† On leave from the French Department of Defense, Délégation Générale pour l'Armement.

Introduction

During the eighties, a lot of progress has been made in the fields of integer factorization and primality testing.

Motivated by the introduction of public key cryptography ([43,85,109]) and accelerated by some advances in technology, new algorithms appeared that are fast, powerful and using deeper and deeper mathematical results. This is true for primality testing, in which were introduced Gauss sums and elliptic curves.

In this report, we want to present the algorithms used for testing integers for primality, the oldest as the most recent. After having recalled some elementary results (Fermat's theorem), we shall briefly present the work of Adleman, Pomerance, Rumely, Cohen and Lenstra, and we shall explain why it did not solve all the problems. Then, in the remaining of part I, we shall explain the use of elliptic curves in primality testing and this will lead us to the Goldwasser-Kilian-Atkin algorithm. The second part gives some details on the implementation of the test and on some results obtained with it. The most striking result is the certification of the largest factor of F_{11}.

Our main goal is to present the results needed to understand the theory of Atkin's test. We give all theoretical results with that in mind. There are few proofs, but we give many references. The practical implementation is not finished, so there are some incomplete chapters. All remarks are welcomed.

Acknowledgments. I am indebted to many people. I want to thank J. L. Nicolas who initiated me to elliptic curves and who has been supporting me ever since; H. Cohen for his advice; D. Bernardi who read the first (French) version for his numerous critical remarks which were very useful to me (he also helped me work out the computation of the j invariants of Euler numbers); B. Serpette and J. Vuillemin for their work on the powerful arithmetic of Le-Lisp, and the latter for his continuous support; P. Flajolet for his helping me with Maple, TEX and for some valuable comments on my work; J. McKay for introducing me to [83] and for some remarks on the draft version; F. Cossec for reading the first English version.

Gothic alphabet

a, A	$\mathfrak{a}$, $\mathfrak{A}$
b, B	$\mathfrak{b}$, $\mathfrak{B}$
c, C	$\mathfrak{c}$, $\mathfrak{C}$
d, D	$\mathfrak{d}$, $\mathfrak{D}$
e, E	$\mathfrak{e}$, $\mathfrak{E}$
f, F	$\mathfrak{f}$, $\mathfrak{F}$
g, G	$\mathfrak{g}$, $\mathfrak{G}$
h, H	$\mathfrak{h}$, $\mathfrak{H}$
i, I	$\mathfrak{i}$, $\mathfrak{I}$
j, J	$\mathfrak{j}$, $\mathfrak{J}$
k, K	$\mathfrak{k}$, $\mathfrak{K}$
l, L	$\mathfrak{l}$, $\mathfrak{L}$
m, M	$\mathfrak{m}$, $\mathfrak{M}$
n, N	$\mathfrak{n}$, $\mathfrak{N}$
o, O	$\mathfrak{o}$, $\mathfrak{O}$
p, P	$\mathfrak{p}$, $\mathfrak{P}$
q, Q	$\mathfrak{q}$, $\mathfrak{Q}$
r, R	$\mathfrak{r}$, $\mathfrak{R}$
s, S	$\mathfrak{s}$, $\mathfrak{S}$
t, T	$\mathfrak{t}$, $\mathfrak{T}$
u, U	$\mathfrak{u}$, $\mathfrak{U}$
v, V	$\mathfrak{v}$, $\mathfrak{V}$
w, W	$\mathfrak{w}$, $\mathfrak{W}$
x, X	$\mathfrak{x}$, $\mathfrak{X}$
y, Y	$\mathfrak{y}$, $\mathfrak{Y}$
z, Z	$\mathfrak{z}$, $\mathfrak{Z}$

Contents

Part I

Primality: past and present

Chapter 1

Elements of number theory

1.1 The ring Z/NZ

For N any integer greater than 1, let $\mathbf{Z}/\mathbf{NZ}$ denote the set of residue classes modulo N. The invertible residues modulo N form the group $(\mathbf{Z}/\mathbf{NZ})^*$.

Definition 1.1.1 *The* Euler-totient function φ *is defined by*

$$\varphi(N) = \mathrm{Card}(\mathbf{Z}/\mathbf{NZ})^*.$$

Proposition 1.1.1 *The function φ satisfies*

1. $\varphi(1) = 1$*;*
2. φ *is* multiplicative *that is*

$$\mathrm{pgcd}(N, M) = 1 \Rightarrow \varphi(NM) = \varphi(N)\varphi(M);$$

3. *if p is prime and k a non-zero integer then* $\varphi(p^k) = p^{k-1}(p-1)$.

Theorem 1.1.1 ([54]) *The group $(\mathbf{Z}/\mathbf{NZ})^*$ is cyclic whenever N equals 2, 4, p^k or $2p^k$, where p is an odd prime and k a non-zero integer.*

The following proposition gives a necessary and sufficient condition for N to be prime.

Proposition 1.1.2 *Let N be an integer. Then:*

$$N \text{ is prime} \Longleftrightarrow \varphi(N) = N - 1.$$

1.2 Characters

We follow the presentation of Ireland and Rosen. The proofs can be found in [64].

In the sequel p always denotes a prime number, $\mathbf{F}_p$ the field with p elements and g a generator of $\mathbf{F}_p{}^*$.

Definition 1.2.1 *A character on $\mathbf{F}_p$ is a homomorphism from $\mathbf{F}_p{}^*$ in $\mathbf{C}$. If χ is such a character, we have*

$$\forall\, a,\, b \in \mathbf{F}_p{}^*,\ \chi(a\,b) = \chi(a)\,\chi(b). \tag{1.1}$$

We extend χ to $\mathbf{F}_p$ by putting $\chi(0) = 0$ if $\chi \neq \epsilon$ and $\epsilon(0) = 1$.

The group ${\mathbf{F}_p}^*$ is cyclic. Let g be a generator. Let a an element of ${\mathbf{F}_p}^*$. There exists x such that $a \equiv g^x \mod p$. Then $\chi(a) = \chi(g)^x$. Moreover, $\chi(g^{p-1}) = \chi(1) = \chi(g)^{p-1}$. We deduce that $\chi(g)$ is a $(p-1)$-th root of unity. One can show the following result.

Proposition 1.2.1 *The set of all characters on $\mathbf{F}_p$ is a cyclic group of order $p-1$. The zero element is $\epsilon : \ a \ \longmapsto \ 1$.*

Proposition 1.2.2 *Let a in $\mathbf{F}_p$. Then*

$$\sum_{\chi} \chi(a) = 0. \tag{1.2}$$

Lemma 1.2.1 *Let n be a divisor of $p-1$. Then there are exactly n characters of order dividing n.*

Proof. If χ is of order n, we have $\chi(g)^n = 1$. Thus, there at most n characters of order dividing n. Moreover, if $\chi(g) = e^{\frac{2i\pi}{n}}$, then $\epsilon,\ \chi,\ \chi^2, \ldots, \chi^{n-1}$ are n different characters whose order divides n. ∎

Theorem 1.2.1 *If $n \mid p-1$, we denote by N the number of solutions of $x^n \equiv a \mod p$. Then*

$$N = \sum_{\chi^n = \epsilon} \chi(a). \tag{1.3}$$

Application: the Legendre-Jacobi symbol

Definition 1.2.2 *A character of order 2 is called a* quadratic character*.*

By lemma (1.2.1), there are two characters of order dividing 2. There is only one non trivial character χ defined by

$$\chi(g) = e^{\frac{2i\pi}{2}} = -1.$$

We deduce immediately that

$$\forall\ a \in\ {\mathbf{F}_p}^*,\ \chi(a) = \chi(g^x) = (-1)^x.$$

In other words

$$\chi(a) = +1 \Longleftrightarrow a \text{ is a square modulo } p.$$

Definition 1.2.3 *This character χ is called the* Legendre symbol *and it is written*

$$\chi(a) = \left(\frac{a}{p}\right).$$

Proposition 1.2.3 *This symbol enjoies the following properties (Cf. [54]).*

1. *$\forall\ a,\ 1 \leq a < p,\ \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$ (Euler's theorem);*
2. *$\forall\ a,\ b, \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;*

3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;
4. *quadratic reciprocity law: if q is prime, then we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

It is convenient to extend the Legendre symbol to the case where n is not a prime. To do so, we let $n = \prod p_i^{\alpha_i}$ and

$$\left(\frac{a}{n}\right) = 0 \text{ if } \mathrm{pgcd}(a, n) \neq 1,$$

$$\left(\frac{a}{n}\right) = \prod \left(\left(\frac{a}{p_i}\right)\right)^{\alpha_i} \text{ otherwise.}$$

Proposition 1.2.4 *This new object is called the* Jacobi symbol. *It satisfies the folowing properties:*

1. $\forall\, a,\, b, \left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$;
2. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$, $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$;
3. *quadratic reciprocity law: if m is an integer, we have*

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}};$$

4. $\left(\frac{n}{m}\right) = \left(\frac{n-m}{m}\right) = \left(\frac{n \bmod m}{m}\right)$, *if $n > m$.*

Properties 3 and 4 yield a fast algorithm for computing $\left(\frac{n}{m}\right)$ ([75]).

Chapter 2

From presumption to proof

Classically ([101]), one makes the distinction between *non primality* testing algorithms, which almost always recognize composite numbers, and *primality* tests which give a proof that a number is prime.

In all that follows, n will always designate an odd integer greater than 2 and different from a power of a prime. If n is prime, it will satisfy all the tests we are to describe. At each step, the number of composite numbers that survive will decrease.

2.1 Non primality tests

2.1.1 Trial division

The most natural way of proving that n is composite is to exhibit a number m ($m > 1$) that divides it. For this, we use the following theorem.

Theorem 2.1.1 *If n is composite, then there exists a prime $p \leq \sqrt{n}$, such that $p \mid n$.*

The algorithm proceeds in dividing n by all primes less than $\sqrt{n}$. If one of the remainders is 0, then we have a factor of n, else n is prime. This method is very expensive. If n is prime, the algorithm will stop after $O(\sqrt{n})$ or $O(\frac{\sqrt{n}}{\log n})$ operations, whether we have or not a table of primes less than $\sqrt{n}$.

From a practical point of view, we divide n by all primes less than a given B, e. g. 10000, 30030 ([134,133]), 10^6 ([34]), before we submit n to other tests in the case we do not get a factor.

We shall now suppose that n has no prime factors less than B.

2.1.2 Fermat's (little) theorem

Theorem 2.1.2 *If n is prime and a is an integer prime to n, then*

$$a^{n-1} \equiv 1 \bmod n. \tag{2.1}$$

If n does not satisfy (2.1), then n is composite. In practice, we choose a random a and check whether n satisfies (2.1). This computation is very efficient on a computer ([67]), and this enables us to quickly discard most composite numbers.

Unfortunately, the converse of this theorem is false. The smallest composite number satisfying (2.1) with $a = 2$ is $n = 341 = 11 \times 13$.

Definition 2.1.1 *Let a be an integer. A composite number n for which (2.1) holds is called* pseudoprime to base a, *or psp*(a).

Moreover, there are composite numbers n which are psp(a) for all a. They are called *Carmichäel numbers*. The smallest one is $n = 561 = 3 \times 11 \times 17$.

In [103], we find the following results.

Theorem 2.1.3 *Let $P_a(x) = \text{Card}\{n \leq x,\ n \text{ is } psp(a)\}$. Then there exists $x_0(a)$ such that for all $x \geq x_0$:*

$$\exp\left\{(\log x)^{\frac{5}{14}}\right\} \leq P_a(x) \leq x \exp\left(-\frac{\log x \log_3 x}{2 \log_2 x}\right),$$

where $\log_k n = \underbrace{\log \log \cdots \log}_{k \text{ times}} n$.

Corollary 2.1.1 *For all a, there are infinitely many psp*(a).

Theorem 2.1.4 *Let $C(x) = \text{Card}\{n \leq x,\ n \text{ is a Carmichäel number}\}$. Then:*

$$\forall\, \epsilon > 0,\ \exists\, x_0(\epsilon),$$

$$\forall x \geq x_0(\epsilon),\ C(x) \leq x \exp\left(-(1-\epsilon)\frac{\log x\ \log_3 x}{\log_2 x}\right). \tag{2.2}$$

It is not known whether there is an infinite number of Carmichäel numbers.

2.1.3 Solovay and Strassen ideas

Theorem 2.1.5 (Euler)
If n is prime and if a is prime to n then

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \bmod n, \tag{2.3}$$

where $\left(\frac{a}{n}\right)$ denotes the Legendre symbol.

The symbol $\left(\frac{a}{n}\right)$ is evaluated following the method described in [75]. If n does not pass this test for a given a, then n is composite. Once again, the converse is false. The smallest n satisfying (2.3) for $a = 2$ is $n = 561$.

Definition 2.1.2 *A composite n for which (2.3) holds for an integer a is called an* Euler pseudoprime to base a, *or* epsp(a).

Theorem 2.1.6 ([103]) *For all a, there are infinitely many epsp*(a).

Theorem 2.1.7 ([117]) *Let n be a composite number. Then:*

$$\text{Card}\{a, 1 < a < n,\ \gcd(a,n) = 1 \text{ and } n \text{ is } epsp(a)\} \leq \frac{n}{2}. \tag{2.4}$$

The test of Solovay and Stassen then consists in testing (2.3) with k values of a. If n is a epsp(a) for all these numbers, then the probability that n is composite is considered to be less than $\frac{1}{2^k}$.

We shall suppose that n is a epsp(a) for some a.

2.1.4 Miller's algorithm

This algorithm is described in [86]. We write $n = 1 + 2^t\, n_0$, with n_0 odd. We have then the following factorization :

$$a^{n-1} - 1 = (a^{n_0} - 1)(a^{n_0} + 1) \cdots (a^{2^{t-1} n_0} + 1). \tag{2.5}$$

If n is prime, then it divides the left hand side of (2.5). Thus n divides one of the factors in the right hand side:

$$a^{n_0} \equiv 1 \bmod n \text{ or } \exists\, j, 0 \leq j < t, a^{2^j n_0} \equiv -1 \bmod n. \tag{2.6}$$

If n does not satisfy (2.6), then it is composite. As for the preceding algorithms, the converse is false. The smallest number satisfying (2.6) for $a = 2$ is $2047 = 23 \times 89$.

Definition 2.1.3 *A composite n for which (2.6) holds for a given a is called a* strong pseudoprime to the base a*, or spsp(a).*

Theorem 2.1.8 ([103])
Let a be an integer greater than 1. We define $S_a(x) = \mathrm{Card}\{n \leq x,\, n\, is\, spsp(a)\}$. Then,

$$\forall x \geq a^{15\,a},\; S_a(x) > \frac{\log x}{4a \log a}. \tag{2.7}$$

Corollary 2.1.2 *For all a, there are infinitely many spsp(a).*

Theorem 2.1.9 ([88]) *Let n be a composite number. Then:*

$$\mathrm{Card}\{a,\, 1 < a < n, \gcd(a, n) = 1 \textit{ and } n \textit{ spsp}(a)\} \leq \frac{n}{4}.$$

The algorithm is then: test whether n satifies (2.6) for k bases. If n passes this test, then we might consider that n is composite with a probability bounded by 4^{-k}. For a more subtle treatment of this idea, see [9].

We have just described some very fast algorithms that can decide whether a number n is composite or has a probability to be prime which is close to 1. Numbers which have passed these tests are called *industrial* by Henri Cohen. In all applications to cryptography, this is enough.

In certain cases, it is worthwhile to give a proof of the primality of a number. We are about to describe algorithms which meet that requirement.

The number n we are interested in will now be supposed to be *pprime*, that is it is almost surely prime. For example, he is spsp for 50 bases (say).

2.2 Primality tests

2.2.1 Converses of Fermat's theorem

In order to prove that n is prime, it is enough, by proposition (1.1.2), to find an integer a, prime to n, whose order is exactly $n-1$. Precisely:

Theorem 2.2.1

$$\left.\begin{array}{l} a^{n-1} \equiv 1 \bmod n \\ \\ \forall\ p \mid n-1,\ a^{\frac{n-1}{p}} \not\equiv 1 \bmod n \end{array}\right\} \Longrightarrow n \textit{ is prime.}$$

We can improve this result in many ways. Let us give some definitions.

Definition 2.2.1 *Let $m = \prod_{i=1}^{k} p_i^{\alpha_i}$, p_i prime, $\alpha_i \geq 1$, an integer. For every integer $\mathcal{B}$, we put:*

$$F(m,\mathcal{B}) = \prod_{p_i \leq \mathcal{B}} p_i^{\alpha_i},\ R(m,\mathcal{B}) = \prod_{p_j > \mathcal{B}} p_j^{\alpha_j}.$$

Thus $m = F(m,\mathcal{B})R(m,\mathcal{B})$, for all $\mathcal{B}$.

If there is no possibility of confusion, we write F (resp. R) for $F(.,.)$ (resp. $R(.,.)$).

We recall three theorems proved in [20] (see also [127,133]).

Theorem 2.2.2 *Suppose we have found an integer $\mathcal{B}$ such that:*

$$R(n-1,\mathcal{B}) = 1 \textit{ or } \mathcal{B}F(n-1,\mathcal{B}) > \sqrt{n}. \tag{2.8}$$

Suppose also that:

1. *for all prime factor p of F, there exists a_p such that: $a_p^{\frac{n-1}{2}} \equiv -1 \bmod n$ and $\gcd(a_p^{\frac{n-1}{2p}} + 1, n) = 1$;*
2. *there exists a_0 such that: $a_0^{\frac{n-1}{2}} \equiv -1 \bmod n$ and $\gcd(a_0^{\frac{n-1}{2R}+1}, n) = 1$.*

Then n is prime.

Before going any further, we need some definitions. We are to work in the ring $(\mathbf{Z}/\mathbf{nZ})[T]/(T^2 - PT + Q)$, where P and Q are two integers. We put $D(P,Q) = P^2 - 4Q$. The *Lucas sequence* $\{V_n(P,Q)\}$ is defined by:

$$V_0(P,Q) = 2,\ V_1(P,Q) = P,\ V_k(P,Q) = PV_{k-1}(P,Q) - QV_{k-2}(P,Q), \text{ for } k \geq 2. \tag{2.9}$$

In the sequel, we suppose that D is fixed and that $\left(\frac{D}{n}\right) = -1$.

Theorem 2.2.3 *Suppose that:*

$$R(n+1,\mathcal{B}) = 1 \textit{ or } \mathcal{B}F(n+1,\mathcal{B}) > \sqrt{n}, \tag{2.10}$$

and:

1. *for all prime factor q of F, there exist two integers P_q and Q_q, satisfying $P_q^2 - 4Q_q = D$ and $\left(\frac{Q_q}{n}\right) = -1$, such that the sequence $\{V_k(P_q, Q_q)\}$ satisfies: $V_{\frac{n+1}{2}}(P_q, Q_q) \equiv 0 \bmod n$ and $\gcd(V_{\frac{n+1}{2q}} + 1, n) = 1$;*
2. *there exist P_0 and Q_0, for which $P_0^2 - 4Q_0 = D$ and $\left(\frac{Q_0}{n}\right) = -1$, such that $\{V_k(P_0, Q_0)\}$ satisfies: $V_{\frac{n+1}{2}}(P_0, Q_0) \equiv 0 \bmod n$ and $\gcd(V_{\frac{n+1}{2R}}, n) = 1$.*

Then n is prime.

Eventually, one can combine these two theorems.

Theorem 2.2.4 *Suppose that n satisfies (1.) and (2.) of the two preceding theorems and:*

$$F(n-1, \mathcal{B})F(n+1, \mathcal{B}) \;\; max(F(n-1, \mathcal{B}), F(n+1, \mathcal{B}))\, \mathcal{B}^3 > 2n. \tag{2.11}$$

Then n is prime.

One can also use the prime factors of $n^2 \pm n + 1$ or $n^2 \pm n + 1$ ([130,131,129,127]). Unfortunately, these tests are much more difficult to use in practice.

Obviously, there remains a problem. Very often, $n-1$ or $n+1$ have simultaneously large prime factors and it is very expensive to compute them. In some cases, though, we can carry on all the computations.

Let $\mathcal{F}$ be the set: $\mathcal{F} = \{f_{-1} : n \mapsto n-1,\ f_1 : n \mapsto n+1\}$. We define on $\mathcal{F}$ a map $\mathcal{T}$ which associates to a function f of $\mathcal{F}$ the primality testing algorithm using the factors of $f(n)$. More precisely, $\mathcal{T}f$ is a function which can take three possible values:

$$\mathcal{T}f(n) = \begin{cases} TRUE & \text{if n is prime,} \\ FALSE & \text{if n is composite,} \\ ? & \text{otherwise.} \end{cases}$$

Let us choose an integer B.

Definition 2.2.2 *The integer m is said to be B-*nicely factored *if $R(m, B) = 1$ or if $R(m, B)$ is pprime.*

We can now explain what is a favorable situation for our theorems.

Proposition 2.2.1 *Suppose we have found a sequence $(f^i)_{0 \leq i \leq l}$ of elements of $\mathcal{F}$, together with a sequence of integers (n_i) such that:*

1. *$n_0 = n$;*
2. *for all $i \geq 0$, $f^i(n_i)$ is B-nice factored and $\mathcal{T}f^i(n_i) = TRUE$, with $\mathcal{B} = B\, n_{i+1}$ and $n_{i+1} = R(f^i(n_i), B)$;*
3. *n_l is prime (e.g. $n_l < B^2$).*

Then n is prime.

Proof. For all i, we use the Tf^i test with n_i and $\mathcal{B} = Bn_{i+1}$, which proves that n_i is prime, whenever n_{i+1} is prime, which is ensured by the next step. ∎

Definition 2.2.3 *The sequence* (f^i) *is called a* primality chain *for* n*.*

It is possible to find such chains for pretty large numbers (see [128]), but it is difficult to find easily chains for *all* numbers of a given magnitude.

One of the interest of Atkin's test is to add more functions to $\mathcal{F}$, which allows to build these chains for all numbers.

Remark on the generation of prime numbers

One possible way to build prime numbers is as follows ([39,97]). One first select some small primes $p_1, \ldots, p_k$, and then search for exponents α_i such that:

$$n = 1 + \prod_{i=1}^{i=k} p_i^{\alpha_i} \tag{2.12}$$

is prime, using (2.2.2).

The merit of the new primality tests is that you can build ordinary primes n not having the property that $n-1$ has small prime factors.

2.2.2 Adleman, Pomerance, Rumely; Cohen, Lenstra

In [3,80,31], the authors describe a primality testing algorithm using some ideas which are implicit in [117]. They are able to prove that the running time of this algorithm is $O((\log n)^{c \log\log\log n})$, for some effectively computable constant $c > 0$. This test, improved by H. Cohen and H. W. Lenstra ([33]), has been implemented by the first author and A. K. Lenstra ([34]). The results are very impressive. We give below some typical times for their algorithm, on a CDC Cyber 170/750. The time used for elementary operations on *multiples*, 16 words of 47 bits, and *doubles*, 32 words of 47 bits, are also given. These operations are coded in Compass and used in a FORTRAN program.

operation	temps en ms
M+M	0.019
M× M	0.210
D mod M	0.470

The following data denote seconds of CPU.

number of digits	mininum time	maximum time	mean value
100	26	75	50
120	51	147	100
140	77	211	150
160	112	298	200
180	259	439	350
200	259	614	400

This algorithm has two (minor) drawbacks. It is very difficult to code and the verification of the results is impossible without rewriting all the program. In the sequel, we denote this algorithm by **CL**.

Chapter 3

Quadratic forms and quadratic fields

This chapter contains some elementary results on positive definite quadratic forms and some properties of quadratic fields. It is an introduction to the following two chapters.

3.1 Quadratic forms

Definition 3.1.1 *We call* binary quadratic form *any function Q from $\mathbf{Z} \times \mathbf{Z}$ in $\mathbf{Z}$ which associates to any pair $(x,\, y)$ the value $Q(x,y) = a\,x^2 + b\,x\,y + c\,y^2$, where a, b and c are in $\mathbf{Z}$. We note $Q = (a,b,c)$. The* discriminant *of $Q = (a,b,c)$ is $\delta(Q) = \delta(a,b,c) = b^2 - 4\,a\,c$.*

Definition 3.1.2 *The form $Q = (a,b,c)$* represents *the integer m if there exists two integers x and y such that: $Q(x,y) = m$.*

In what follows, we are interested in *positive definite* forms, i. e. the forms satisfying:

$$\forall\ (x,y) \neq (0,0),\ Q(x,y) > 0.$$

A necessary condition for $Q = (a,b,c)$ to be of this kind is $\delta(Q) < 0$. This implies that a and c are of the same sign. We may thus suppose that they are both positive.

We now fix a positive integer d, and we suppose that if p is any of its odd prime factors, then $p^2 \not| \; d$. We put $\mathcal{E}(-d) = \{(a,\, b,\, c) \mid \delta(a,b,c) = -d\}$. This set is not empty iff $-d$ is a quadratic residue modulo 4, that is $d \equiv 0 \bmod 4$ or $d \equiv 3 \bmod 4$. We remark that b and d are of the same parity.

3.1.1 Equivalence relation on $\mathcal{E}(-d)$

To the form $(a,\, b,\, c)$, we associate the following matrix A:

$$\begin{pmatrix} a & \dfrac{b}{2} \\ \dfrac{b}{2} & c \end{pmatrix} \tag{3.1}$$

If X is the vector $\begin{pmatrix} x \\ y \end{pmatrix}$ then $Q(x,\, y) = {}^t X\, A\, X$.

We define:

$$SL_2(\mathbf{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \mid \alpha,\, \beta,\, \gamma,\, \delta \textit{ in } \mathbf{Z} \textit{ and } \alpha\,\delta\, - \beta\,\gamma = 1 \right\}$$

Let Q and Q' be two elements of $\mathcal{E}$. We say that Q and Q' are equivalent, which we denote by $Q \sim Q'$, iff there is a matrix P of $SL_2(\mathbf{Z})$ such that $A' = {}^tP\,A\,P$.

Definition 3.1.3 *A form* (a, b, c) *is said to be* primitive *if* $\gcd(a,\, b,\, c) = 1$, *and* reduced *if* $|b| \leq a \leq c$ *and* $b \geq 0$ *whenever* $c = a$ *or* $|b| = a$.

Theorem 3.1.1 *This relation is an equivalence relation. Each equivalence class contains exactly one primitive reduced form.*

It is easy to see that a primitive reduced form $(a,\, b,\, c)$ satisfies:

$$|b| \leq a \leq c \Longrightarrow 4\,a^2 \leq 4\,a\,c = d + b^2 \leq d + a^2. \tag{3.2}$$

Hence:

$$|b| \leq a \leq \sqrt{\frac{d}{3}}. \tag{3.3}$$

As a consequence, there is a finite number of reduced primitive forms of discriminant $-d$. We note this number $h(-d)$. This the cardinal of $\mathcal{H}(-d)$, the set of all equivalence classes for $\sim$.

Definition 3.1.4 $-d$ *is said to be a* fundamental discriminant *if*

1. *d has no odd prime factor to a power greater than 1;*
2. *$d \equiv 3 \bmod 4$ or $d \equiv 4 \bmod 16$, or $d \equiv 8 \bmod 16$.*

Proposition 3.1.1 *If $-d$ is fundamental, then every reduced form is primitive.*

We end this enumeration by the following definition. If q is an odd prime, we put $q^* = (-1)^{\frac{q-1}{2}} q$. This implies that $q^* \equiv 1 \bmod 4$ for all q. We also put $4^* = -4$ and $8^* = \pm 8$, as is explained in the following lemma.

Lemma 3.1.1 *Let $-D$ be a fundamental discriminant. There are four cases:*

$$\begin{array}{llllll}
D \equiv & 3 \bmod & 4: & D = q_1 & q_2 \cdots q_t \textit{ and then } -D = & & \prod_{i=1}^t q_i^*; \\
D \equiv & 4 \bmod & 16: & D = 4 & q_2 \cdots q_t \textit{ and then } -D = & (-4) & \prod_{i=2}^t q_i^*; \\
D \equiv & 8 \bmod & 32: & D = 8 & q_2 \cdots q_t \textit{ and then } -D = & (-8) & \prod_{i=2}^t q_i^*; \\
D \equiv & 24 \bmod & 32: & D = 8 & q_2 \cdots q_t \textit{ and then } -D = & (+8) & \prod_{i=2}^t q_i^*.
\end{array}$$

Proof. Let us prove the case $D \equiv 3 \bmod 4$. Suppose that the first l factors of D are congruent to 3 modulo 4. Then $-D = (-1)^l \prod_{i=1}^t q_i^*$, where q_i^* is congruent to 1 modulo 4. But $-D$ is congruent to 1 modulo 4, and we deduce that l is even and then $-D = \prod_{i=1}^t q_i^*$.

We can do the same for the other cases. ■

3.1.2 Reduction of forms

It is possible to give an algorithm that computes the reduced form associated to a given form. This has been introduced by Gauss ([47]).

Let $Q = (a, b, c)$ be a quadratic form of discriminant $-d$. Each step of the algorithm associates to Q a form $Q' = (a', b', c')$ equivalent to Q that satisfies: $-a < b' \leq a$ and $a' \leq c'$. We may choose:

$$a' = a, \; b' = b + 2ak, \; c' = k^2 a + kb + c,$$

with $k = \left\lfloor \frac{a-b}{2a} \right\rfloor$. If $a' \leq c'$, then Q' is reduced, else we replace Q with $(c', -b', a')$ and we go on the reduction process. It is possible to show that the algorithm terminates and that the final form is indeed reduced.

Let us look at one step of the algorithm. Let A' be the matrix associated to Q'. This matrix is deduced from A by:

$$A' = {}^t(T^k)\; A\; T^k, \tag{3.4}$$

where:

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Then, we possibly have to modify the result as:

$$A' := {}^tS\; A'\; S, \tag{3.5}$$

with:

$$S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let use note that S and T are elements of $SL_2(\mathbf{Z})$, and thus $Q' \sim Q$.

We make the following change of variables:

$$X = \begin{pmatrix} x \\ y \end{pmatrix} = (T^k S) \begin{pmatrix} x' \\ y' \end{pmatrix} = (T^k S)\; X'. \tag{3.6}$$

Then:

$${}^tX\; A\; X = {}^tX'\; {}^t(T^k S)\; (T^k S)\; A'\; {}^t(T^k S)\; (T^k S)\; X' = {}^tX'\; A'\; X',$$

which means that: $Q(x, y) = Q'(x', y')$, if X and X' are related by (3.6).

The reduction process transforms a matrix A into a matrix A' that is equivalent to A, providing us with the matrix N such that:

$$A' = {}^tN\; A\; N \text{ and } N \in SL_2(\mathbf{Z}).$$

We summarize the algorithm and insist on the matricial point of view, that we shall need in chapter 3.

procedure GAUSSRED;

1. $N := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;

2. **if** $c < a$ **then** $Q := (c, -b, a)$, $N := N\; S$;

3. 1. $k := \left\lfloor \dfrac{a-b}{2a} \right\rfloor$;
   2. $b := b + 2ak$;
   3. $c := \dfrac{b^2+d}{4a}$;
   4. $N := N\,T^k$;
4. **if** $c < a$ **then** go to 2;
5. **if** $b < 0$ and $((c = a)$ or $(-b = a))$ **then** $b := -b$; $N := N\,S$;
6. (a, b, c) is reduced **end.**

3.1.3 An algorithm which determines all reduced forms

This algorithm is described in [15]. Let $-D$ be a fundamental discriminant.

procedure QFLIST;

1. $r := \left\lfloor \sqrt{\dfrac{D}{3}} \right\rfloor$;
2. $b := D \bmod 2$;
3. **while** $b \leq r$
   1. $m := \dfrac{b^2+D}{4}$;
   2. **for** $a \mid m$ and $a \leq \lfloor \sqrt{m} \rfloor$
      1. $c := \dfrac{m}{a}$;
      2. **if** $b \leq a$ **then**
         if $b = a$ or $c = a$ **then** store (a, b, c) **else** store $(a, \pm b, c)$;
   3. $b := b + 2$;
4. **end.**

3.1.4 Composition of forms

It is possible to endow $\mathcal{E}(-d)$ with a group law which is compatible with $\sim$. The zero element of this law is called the *principal form*. Its value is given by:

$$\begin{cases} (1, 0, \dfrac{d}{4}) & \text{if } d \equiv 0 \bmod 4, \\ (1, 1, \dfrac{d+1}{4}) & \text{otherwise.} \end{cases}$$

The algorithm used to compute $Q \times Q'$ is to be found in [115]. We need only the following result.

Definition 3.1.5 *A form is said to be* ambiguous *iff its order is 2.*

Proposition 3.1.2 *The ambiguous forms are of the types:* $(a, 0, c)$, (a, a, c) *or* (a, b, a).

3.2 Quadratic fields

A *quadratic field* K is a field extension of degree 2 over $\mathbf{Q}$. There exists an integer (positive or negative) δ without square factors such that $K = K_\delta$. We note this field K_δ. The *discriminant* of K_δ is:

$$d = \begin{cases} 4\delta & \text{if } \delta \equiv 2 \text{ or } 3 \bmod 4, \\ \delta & \text{if } \delta \equiv 1 \bmod 4. \end{cases}$$

In all that follows, we refer to case (i) (resp. (ii)) to designate the case $\delta \equiv 2$ or $3 \bmod 4$ (resp. $\delta \equiv 1 \bmod 4$).

The conjugate of an element $\xi = r + s\sqrt{\delta}$ of K_δ is $\xi' = r - s\sqrt{\delta}$. Its *norm* is defined by:

$$N_\delta(\xi) = \xi\xi' = r^2 - \delta s^2,$$

the *trace* of ξ is:

$$T_\delta(\xi) = \xi + \xi' = 2r.$$

The element θ of K_δ is said to be an *integer* iff $N_\delta(\theta)$ and $T_\delta(\theta)$ are integers of $\mathbf{Z}$. To distinguish between elements of $\mathbf{Z}$ and integers of K_δ, we call the first ones *rational integers.*

One shows that:

Proposition 3.2.1 *The set of all integers of K_δ, noted $\mathcal{O}_\delta$, is a subring of K_δ. More precisely, $\mathcal{O}_\delta$ is the set $\{a + b\omega$, a and b in $\mathbf{Z}\}$ with:*

$$\omega = \begin{cases} \sqrt{\delta} & \textit{in case } (i), \\ \dfrac{1+\sqrt{\delta}}{2} & \textit{in case } (ii). \end{cases}$$

Definition 3.2.1 *We say that an element ϵ of K_δ is a* unit *iff:*

$$\epsilon \in \mathcal{O}_\delta \textit{ and } \epsilon^{-1} \in \mathcal{O}_\delta.$$

Proposition 3.2.2 *The units of K_δ are precisely the elements ϵ such that:*

$$N_\delta(\epsilon) = \pm 1.$$

Theorem 3.2.1 *Let d be the discriminant of a quadratic field. Let $w(d)$ be the number of units in K_δ. Then:*

$$w(d) = \begin{cases} +\infty & if & d & > & 0, \\ 6 & if & d & = & -3, \\ 4 & if & d & = & -4, \\ 2 & if & d & < & -4. \end{cases}$$

Theorem 3.2.2 ([35, Ch. VI, §4]) *The group of unity of K_δ is a cyclic group. There exists a $\eta > 1$ that generates this group. Is is called the* fundamental unit *of K_δ.*

There is an algorithm that computes the fundamental unit of K_δ([35, Ch. VI, §5]). One can find tables of such elements in [15] and [63].

3.2.1 Modules, orders, ideals

The proofs we do not give are to be found in [15].

Definition 3.2.2 *Let $\alpha_1, \ldots, \alpha_r$ be elements of K_δ. We define a* module *of K_δ to be the set*

$$M = \{\alpha_1 l_1 + \ldots + \alpha_r l_r,\ l_i \in \mathbf{Z}\}.$$

We write:

$$M = [\alpha_1, \ldots, \alpha_r].$$

Definition 3.2.3 *An* order *of K_δ is a subring of $\mathcal{O}_\delta$, containing 1.*

Proposition 3.2.3 *The orders of K_δ are precisely the modules of K_δ that are of the form $\mathcal{O}(f) = [1, f\omega]$, with f a rational integer.*

Proposition 3.2.4 *Let $M = [\alpha, \beta]$ be a module of K_δ and let $\mathcal{S} = \{\gamma \in K_\delta,\ \gamma M \subset M\}$. Then $\mathcal{S}$ is an order of K_δ, called the* stabilizer *of M.*

Definition 3.2.4 *Let $M = [\alpha_1, \ldots, \alpha_r]$ be a module of K_δ. We say that M is an* ideal *of K_δ iff:*

$$\forall i,\ \alpha_i \in \mathcal{O}_\delta \text{ and } \omega\alpha_i \in M.$$

Proposition 3.2.5 *An ideal $[\alpha_1, \ldots, \alpha_r]$ can be written as $[a, b + c\omega]$, with a, b, c in $\mathbf{Z}$.*

Proof. Since α_i is in K_δ, it can be written as $b_i + c_i\omega$, with b_i and c_i in $\mathbf{Z}$. We put $c = \gcd(c_1, \ldots, c_r)$. By Bezout's theorem, we can find rational integers $k_1, \ldots, k_r$ such that:

$$k_1 c_1 + \cdots + k_r c_r = c. \tag{3.7}$$

We then build the following rational integer b:

$$k_1\alpha_1 + \cdots + k_r\alpha_r = b + c\omega = \xi. \tag{3.8}$$

We deduce:

$$\begin{aligned} a_i &= \alpha_i - \frac{c_i}{c}\xi = b_i + c_i\omega - \frac{c_i}{c}(b + c\omega) \\ &= b_i - \frac{c_i}{c} b, \end{aligned}$$

and a_i is a rational integer. We put $a = \gcd(a_1, \ldots, a_r)$. With the help of (3.8) and of the equation $\alpha_i = a_i + \frac{c_i}{c}\xi$, we see that:

$$[\alpha_1, \ldots, \alpha_r] = [a, b + c\omega]. \blacksquare$$

Proposition 3.2.6 *The module $M = [a, b + c\omega]$ is an ideal iff the following conditions are satisfied:*

$$a \equiv b \equiv 0 \bmod c, \tag{3.9}$$

$$b^2 - \delta c^2 \equiv 0 \bmod ac, \text{ in case } (i), \tag{3.10}$$

$$b(b + c) - \frac{\delta - 1}{4} c^2 \equiv 0 \bmod ac, \text{ in case } (ii). \tag{3.11}$$

Proof. Let us write that $a\omega$ and $(b+c\omega)\omega$ are in M:

$$a\omega = Aa + B(b+c\omega),$$

$$\omega(b+c\omega) = Ca + D(b+c\omega),$$

with A, B, C and D in $\mathbf{Z}$. From the first equation, we get $a = Bc$ and $Aa + Bb = 0$, what we summarize by: $a \equiv b \equiv 0 \bmod c$.

In case (i), we have $\omega^2 = \delta$, and we get

$$b = Dc,$$

$$c\delta = Ca + Db,$$

that is to say: $b^2 - c^2\delta \equiv 0 \bmod ac$.

In case (ii), $\omega^2 = \frac{\delta-1}{4} + \omega$, hence:

$$b(b+c) - \frac{\delta-1}{4}c^2 \equiv 0 \bmod ac. \blacksquare$$

From now on, we write an ideal as $(a, b+c\omega)$, and we note (p) the principal ideal $p\mathcal{O}_\delta$. We define the product of two ideals $\mathfrak{i}$ and $\mathfrak{j}$ as the ideal generated by all the products of an element of $\mathfrak{i}$ by an element of $\mathfrak{j}$. We say that an ideal $\mathfrak{i}$ *divides* an ideal $\mathfrak{j}$ if there exists an ideal $\mathfrak{i}$' such that $\mathfrak{j} = \mathfrak{i}\,\mathfrak{i}'$.

Corollary 3.2.1 *If $(a, b+c\omega)$ is an ideal, then: $a = ca'$ and $b = cb'$, by (3.9). We then get: $(a, b+c\omega) = (c, c+\omega)(a', b'+\omega)$.*

Definition 3.2.5 *If $\mathfrak{i} = (a, b+c\omega)$ is an ideal, with $a > 0$ and $c > 0$, its* norm *is $\mathcal{N}(\mathfrak{i}) = ac$.*

Definition 3.2.6 *An ideal $\mathfrak{p}$ ($\mathfrak{p} \neq \mathcal{O}_\delta$) is said to be* prime *if for all pair of ideals $(\mathfrak{i}, \mathfrak{i}')$, we have:*

$$\mathfrak{p} \mid \mathfrak{i}\,\mathfrak{i}' \Longrightarrow \mathfrak{p} \mid \mathfrak{i} \text{ or } \mathfrak{p} \mid \mathfrak{i}'.$$

Theorem 3.2.3 ([35, Ch. VII, §10]) *A prime ideal $\mathfrak{p}$ in K_δ may be written as $\mathfrak{p} = (p, \pi)$ where p is a prime rational integer satisfying $\mathfrak{p} \mid (p)$ and $N_\delta(\pi) \equiv 0 \bmod p$.*

3.2.2 Decomposition of rational primes in K_δ

Theorem 3.2.4 ([35, Ch. VIII, §1]) *Let p be a rational prime number greater than 2.*

1. *If $\left(\frac{d}{p}\right) = 1$, then (p) may be written as $\mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$ and $\mathfrak{p}'$ are two different prime ideals in K_δ and $\mathcal{N}(\mathfrak{p}) = \mathcal{N}(\mathfrak{p}') = p$. We say that p* splits *in K_δ.*
2. *If $\left(\frac{d}{p}\right) = 0$, then $(p) = \mathfrak{p}^2$, with $\mathfrak{p}$ a prime ideal in K_δ and $\mathcal{N}(\mathfrak{p}) = p$. We say that p* ramifies *in K_δ.*
3. *If $\left(\frac{d}{p}\right) = -1$, then (p) is a prime ideal in K_δ. We say that p is* inert *in K_δ.*

This theorem is effective. The results are summarized below. We denote by r the solution of the system:

$$\begin{cases} r^2 & \equiv & d \bmod p, \\ r & \equiv & d \bmod 2. \end{cases}$$

Then:

$\left(\frac{d}{p}\right) = 1$: $\mathfrak{p} = (p, \frac{r-\sqrt{d}}{2})$;

$\left(\frac{d}{p}\right) = 0$: $\mathfrak{p} = (p, \sqrt{\delta})$ in case (i) and $\mathfrak{p} = (p, \frac{p+\sqrt{\delta}}{2})$ in case (ii);

$\left(\frac{d}{p}\right) = -1$: $\mathfrak{p} = (p)$.

3.2.3 Equivalence classes

Theorem 3.2.5 ([35, Ch. VII, §6]) *Let $\mathfrak{i}$ be a non zero ideal in K_δ. There exists an ideal $\mathfrak{i}^*$ and an integer α such that:*

$$\mathfrak{i}\,\mathfrak{i}^* = (\alpha).$$

Definition 3.2.7 *Two ideals $\mathfrak{i}$ and $\mathfrak{i}'$ are said to be* equivalents *iff there exist α and β in $\mathcal{O}_\delta$ such that:*

$$\mathfrak{i}\,(\alpha) = \mathfrak{i}'\,(\beta).$$

We note: $\mathfrak{i} \sim \mathfrak{i}$'.

Proposition 3.2.7 *The relation $\sim$ verifies the following properties:*

1. *it is an equivalence relation;*
2. *if $\alpha \in \mathcal{O}_\delta$, then: $(\alpha) \sim (1)$;*
3. *the inverse of the class of $\mathfrak{i}$ is the class of $\mathfrak{i}^*$, since $\mathfrak{i}\,\mathfrak{i}^* = (\alpha) \sim (1)$;*
4. *the product of the class of $\mathfrak{i}$ and the class of $\mathfrak{j}$ is the class of the product $\mathfrak{i}\,\mathfrak{j}$.*

Theorem 3.2.6 ([35, Ch. VIII, §2]) *In any ideal $\mathfrak{i}$ we can find an element α such that:*

$$0 < |N_\delta(\alpha)| \leq \mathcal{N}(\mathfrak{i})\sqrt{|d|}. \tag{3.12}$$

Corollary 3.2.2 *Any class of ideals contains an ideal $\mathfrak{i}$ such that: $\mathcal{N}(\mathfrak{i}) < \sqrt{|d|}$.*

Corollary 3.2.3 *The number of classes of ideals, denoted by $h(d)$, is finite.*

Theorem 3.2.7 *The set of ideal classes froms a group for the multiplication of the classes.*

3.2.4 Correspondance between ideals and quadratic forms

Let $\mathfrak{i} = (a, b + c\omega)$ an ideal of K_δ. We associate to $\mathfrak{i}$ the form $Q_\mathfrak{i}$ defined by:

$$Q_\mathfrak{i}(x, y) = \frac{N_\delta(ax + (b + c\omega)y)}{\mathcal{N}(\mathfrak{i})}. \tag{3.13}$$

Proposition 3.2.8 *The form Q has all its coefficients in $\mathbf{Z}$.*

Proof. Let us examine case (ii). We get:

$$\begin{aligned} Q_\mathfrak{i}(x, y) &= \frac{(ax + by + \frac{c}{2}y)^2 - d\frac{c^2y^2}{4}}{ac} \\ &= \frac{a}{c}x^2 + (2\frac{b}{c} + 1)xy + \frac{b(b + c) - \frac{d-1}{4}c^2}{ac}y^2. \end{aligned}$$

Using (3.9) and (3.11), we see that the coefficients of $Q_{\mathfrak{i}}$ are rational integers.

In case (i), we find:

$$Q_{\mathfrak{i}}(x,y) = \frac{a}{c}x^2 + 2\frac{b}{c}xy + \frac{b^2 - \delta c^2}{ac}y^2,$$

and we conclude with the help of (3.10). ■

Conversely, let $Q = (a, b, c)$ be a primitive quadratic form. We associate to it the ideal $\mathfrak{i} = (a, \frac{b-\sqrt{d}}{2})$.

Remark on the imaginary case

We have seen how to connect ideals and forms. When the field K_δ is imaginary, there is a one-to-one correspondance between classes of form and ideal classes by the virtue of (3.13). As an immediate consequence, the class numbers on each side are the same. The analogue of the multiplication of ideal classes is the composition of forms.

Chapter 4

Close encounter of class field theory

This chapter is divided in four parts. The first one presents the problem of the representability of numbers by quadratic forms. The second briefly explains the role of class field theory. The third studies the problem when seen from the quadratic form point of view. Finally, the last one collects the algorithms we use in practice.

4.1 Representation of primes by the principal form

4.1.1 Presentation of the problem

In all that follows, p denotes an odd prime number and $-D$ a fundamental discriminant. The field K_{-D}, identified to $K_{-D/4}$ when $4 \mid D$, is noted $\mathbf{K}$, the ring of integers of $\mathbf{K}$ is noted $\mathcal{O}$ and the norm of an element π is $N_D(\pi)$. We are looking for an element π of $\mathcal{O}$ such that $N_D(\pi) = p$ (this will be the heart of Atkin's test). Writing $\pi = a + b\omega$, with a and b in $\mathbf{Z}$, we get:

$$N_D(\pi) = p = \begin{cases} x^2 + \dfrac{D}{4}\, y^2, & \text{in case (i)}, \\[2ex] x^2 + xy + \dfrac{D+1}{4}\, y^2, & \text{in case (ii)}. \end{cases}$$

Thus, we want to represent p by the principal form. We remark that:

Proposition 4.1.1 *If p can be represented by the principal form, then the equation $N_D(\pi) = p$ has exactly $w(-D)$ solutions.*

Proof. Let π be a solution of $N_D(\pi) = p$. Then:

$$N_D(\xi) = p \Longleftrightarrow \exists\, \epsilon \textit{ unit of } \mathbf{K} \textit{ such that } \xi = \epsilon\, \pi. \blacksquare$$

We now give some general results on the representation of integers.

Proposition 4.1.2 *Let m be a number represented by a quadratic form. Then, for all prime divisor l of m, we have:*

$$\left(\frac{-D}{l}\right) = 0 \textit{ or } 1.$$

Proof. Suppose that $m = ax^2 + bxy + cy^2$. Then: $4am = (2ax + by)^2 + Dy^2$. Let l be a prime factor of m. We have:

$$(2ax + by)^2 \equiv -Dy^2 \bmod l.$$

Thus if $-D \not\equiv 0 \bmod l$, $-D$ must be a square modulo l. ■

Proposition 4.1.3 *A prime p can be represented by* a *quadratic form of $-D$ iff $\left(\frac{-D}{p}\right) \neq -1$.*

Proof. Necessity was proved above. If $\left(\frac{-D}{p}\right) = 0$ or 1, the ideal (p) has a divisor $\mathfrak{p} = (p, \pi)$, with $N_D(\pi) \equiv 0 \bmod p$, by theorem (3.2.3). Let us consider the associated quadratic form:

$$Q_{\mathfrak{p}}(x, y) = \frac{N_D(px + \pi y)}{\mathcal{N}(\mathfrak{p})}.$$

Since $\mathcal{N}(\mathfrak{p}) = p$, we deduce:

$$Q_{\mathfrak{p}}(1, 0) = \frac{p^2}{p} = p,$$

which completes the proof. ■

Corollary 4.1.1 *When $\left(\frac{-D}{p}\right) = 1$, p is represented by $(p, -r, \frac{r^2+D}{4p})$, with the notations of the preceding chapter.*

Proof. Apply proposition (3.2.8). ■

We give now some conditions for p to be represented by the principal form.

4.1.2 Formulation of the problem in terms of ideals

In this section, we insist on the role of principal ideals.

Proposition 4.1.4 *Let $\mathfrak{i}$ an ideal of $\mathbf{K}$, $\mathfrak{i} \neq \mathcal{O}$. Then:*

$$\mathfrak{i} \text{ is principal} \iff \exists\, \alpha \in \mathcal{O},\ N_D(\alpha) = \mathcal{N}(\mathfrak{i}).$$

Proof. Suppose that $\mathfrak{i}$ is principal. There exists α in $\mathcal{O}$ such that $\mathfrak{i} = (\alpha)$. Let us compute the norm of $\mathfrak{i}$. First, suppose that α is a rational integer. Then $\mathfrak{i} = (\alpha) = (\alpha, \alpha\omega)$ and the norm of $\mathfrak{i}$ is:

$$\mathcal{N}(\mathfrak{i}) = \alpha^2 = N_D(\alpha).$$

If α is no longer a rational integer, we see that $\mathcal{N}(\alpha) = \mathcal{N}(\alpha')$. Then:

$$\mathcal{N}((\alpha))^2 = \mathcal{N}((\alpha))\mathcal{N}((\alpha')) = \mathcal{N}((\alpha)(\alpha')) = \mathcal{N}((\alpha\alpha')) = \mathcal{N}((N_D(\alpha))) = N_D(\alpha)^2.$$

Since $\mathcal{N}(\mathfrak{i}) > 0$, we deduce: $\mathcal{N}(\mathfrak{i}) = N_D(\alpha)$.

Suppose now that $\mathfrak{i}$ is not principal. We show that:

$$\forall\, \theta \in \mathfrak{i},\ N_D(\theta) > \mathcal{N}(\mathfrak{i}).$$

Let θ be an element of $\mathfrak{i}$. We have $(\theta) \subset \mathfrak{i}$ but $(\theta) \neq \mathfrak{i}$, since $\mathfrak{i}$ is not principal. This relation implies the existence of an ideal $\mathfrak{j}$ such that $(\theta) = \mathfrak{i}\,\mathfrak{j}$ (*to contain is to divide*). Since $\mathfrak{i}$ is not principal, $\mathfrak{j}$ is different from $\mathcal{O}$ and so $\mathcal{N}(\mathfrak{j}) > 1$. Hence:

$$\mathcal{N}(\theta) = N_D(\theta) > \mathcal{N}(\mathfrak{i}). \blacksquare$$

Proposition 4.1.5 *Let $\mathfrak{i}$ be a principal ideal and ξ a solution of the problem*

$$\left| \begin{array}{l} Min\ N_D(\theta) \\ \theta \in \mathfrak{i} \end{array} \right. \tag{4.1}$$

Then: $\mathfrak{i} = (\xi)$.

Proof. We have just seen that $\mathfrak{i}$ can be written (π), with $N_D(\pi) = \mathcal{N}(\mathfrak{i})$. Since ξ is in $\mathfrak{i}$, we can find λ in $\mathcal{O}$ such that $\xi = \lambda\pi$. Computing the norms, we get:

$$N_D(\xi) = N_D(\pi)N_D(\lambda) \geq N_D(\xi)N_D(\lambda),$$

which implies that λ is a unit and thus: $\mathfrak{i} = (\pi) = (\xi)$. $\blacksquare$

Back to the original problem

Let p be a rational prime that splits in $\mathbf{K}$ as $p\mathcal{O} = \mathfrak{p}\,\mathfrak{p}'$ and $\mathcal{N}(\mathfrak{p}) = p$. If we summarize the preceding results, we obtain:

Theorem 4.1.1 *The equation $N_D(\pi) = p$ has a solution iff $\mathfrak{p}$ is principal.*

To test whether this property is satisfied, we compute an element ξ of $\mathfrak{p}$ which minimizes N_D on $\mathfrak{p}$. If $N_D(\xi) = p$, we win, else $\mathfrak{p}$ is not principal and the equation has no solution (Cf. section 4.4).

The problem now is to have conditions for an ideal of $\mathbf{K}$ to be principal. This is a very important theoretical problem, which we attempt to describe in the following section.

4.2 Class field theory

We follow the excellent book by H. Cohn ([37]). We begin by studying the general case, before going to the results concerning the quadratic fields.

4.2.1 A simple example

Consider the case where we want to represent a rational prime p by the principal form of discriminant -4. The corresponding field is $\mathbf{Q}(-4) = \mathbf{Q}(i)$. This field is known to be euclidean (Cf. [118]), and therefore $\mathcal{O}$ is a principal ideal domain. So all ideals are principal. Hence, if p splits in $\mathbf{Q}(i)$ as $\mathfrak{p}\mathfrak{p}'$, the ideal $\mathfrak{p}$ is principal and the equation we are interested in has a solution.

Unfortunately, there are few imaginary quadratic fields for which the ring of integers $\mathcal{O}$ is principal ([118]). The solution to our problem implies to search for other conditions satisfied by $\mathfrak{p}$. As a matter of fact, this solution will be to find a field $\mathcal{K}$ that has the following property:

$$p = N_D(\pi) \Longleftrightarrow \mathfrak{p} \text{ splits in } \mathcal{K}.$$

This field is called the *class field* and the search for it will not be completed before the next chapter with the introduction of the function j.

Before giving the essential results of class field theory, we introduce a particular isomorphism.

4.2.2 The Artin isomorphism

Let $L|K$ be an extension of Galois group $G = \mathrm{Gal}(L|K)$. Let $\mathcal{O}_L$ and $\mathcal{O}_K$ be their respective ring of integers. Let $\mathfrak{p}$ be a prime ideal of K, $\mathfrak{P}$ a prime ideal of L above $\mathfrak{p}$.

$$\begin{array}{cc} L & \mathfrak{P} \\ | & | \\ K & \mathfrak{p} \end{array}$$

Theorem 4.2.1 $\exists\, S \in G,\ \forall\, A \in \mathcal{O}_L,\ A^S \equiv A^{\mathcal{N}(\mathfrak{p})} \bmod \mathfrak{P}.$

Definition 4.2.1 *This element S is called the* Frobenius symbol. *We note:*

$$\left[\frac{L|K}{\mathfrak{P}}\right].$$

Proposition 4.2.1 *If $\mathfrak{P}$ is replaced by a conjugate $\mathfrak{P}^U$ $(U \in G)$, then:*

$$U^{-1}\left[\frac{L|K}{\mathfrak{P}}\right]U = \left[\frac{L|K}{\mathfrak{P}^U}\right].$$

Corollary 4.2.1 *If $L|K$ is abelian, the Frobenius symbol does not depend on $\mathfrak{P}$, but only on $\mathfrak{p}$. It is then called the* Artin symbol *and is denoted by:*

$$\left(\frac{L|K}{\mathfrak{p}}\right).$$

We deduce that:

$$\forall\, A \in \mathcal{O}_L,\ A^S \equiv A^{\mathcal{N}(\mathfrak{p})} \bmod \mathfrak{p}.$$

Examples

Quadratic fields

Let $K = \mathbf{Q}$, $L = \mathbf{Q}(\sqrt{d})$. It is easy to see that $L|K$ is an abelian extension of Galois group $G = \{1, U\}$, where U is defined by:

$$\sqrt{d}^U = -\sqrt{d}.$$

If $A = \frac{r+s\sqrt{d}}{2}$ is an integer of L and p a rational prime, we can compute $A^p \bmod p$ with the help of Fermat's theorem:

$$A^p \equiv \frac{r + s\sqrt{d}^p}{2} \bmod p.$$

On the other hand, we have:

$$\begin{array}{rcl} \sqrt{d}^p & = & d^{\frac{p-1}{2}}\sqrt{d} \\ & \equiv & \left(\frac{d}{p}\right)\sqrt{d} \bmod p, \end{array}$$

by Euler's theorem. We deduce that $A^p \equiv A$ or A^U whether $\left(\frac{d}{p}\right)$ equals $+1$ or -1. We thus identify the Artin symbol with the Jacobi symbol.

Genus field
If $-D = \prod_{i=1}^{t} q_i^*$ is a fundamental discriminant, we put $\mathbf{K} = \mathbf{Q}(\sqrt{-D})$ and we define the *genus field* of $\mathbf{K}$ to be $\mathbf{K}_{\mathrm{g}} = \mathbf{Q}(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*})$. One shows ([37, Ch. 18]) that:

$$\left(\frac{\mathbf{K}_{\mathrm{g}}|\mathbf{K}}{\mathfrak{p}}\right) \simeq \left(\left(\frac{q_1^*}{p}\right), \ldots, \left(\frac{q_t^*}{p}\right)\right).$$

4.2.3 Algebraic results

Let $L|K$ be a field extension of degree n, $\mathcal{O}_L$ and $\mathcal{O}_K$ their ring of integers. A prime ideal $\mathfrak{p}$ of K *splits* in L iff:

$$\mathfrak{p} = \mathfrak{P}_1 \ldots \mathfrak{P}_n \text{ in } L$$

where all the $\mathfrak{P}_i$ are disctinct prime ideals of L.

Definition 4.2.2 *The* Hilbert class field *of K is the maximal abelian unramified extension of K. It is noted K_H.*

Theorem 4.2.2 *For every field K, the class field K_H verifies*

$$\mathrm{Gal}(K_H|K) \simeq \mathrm{Cl}(K),$$

the class group of K.

Corollary 4.2.2 $[K_H : K] = h$.

Theorem 4.2.3 *The prime ideals of K that split in K_H are precisely the principal ideals of K.*

Consequence: this theorem gives a solution to our original problem. An ideal $\mathfrak{p}$ of $\mathbf{K}$ is principal iff it splits in $\mathbf{K}_{\mathrm{H}}$, the class field of $\mathbf{K}$. Hence p can be represented by the principal form iff p splits in $\mathbf{K}$, i. e. $p = \mathfrak{p}\mathfrak{p}'$ and $\mathfrak{p}$ splits in $\mathbf{K}_{\mathrm{H}}$.

It remains to find the class field of an imaginary quadratic field.

4.3 Partial solution: genus of forms and Euler numbers

4.3.1 Genus of forms

This theory is due to Gauss [47]. Alternatively, one can read [35, Ch. XIII, §3] and [15, Ch. III, §8, 3]. We limit ourself to the treatment of the case of forms of negative discriminant.

Generic characters

Let us write the factorization of a fundamental discriminant D:

$$\begin{array}{rrcccccl} & D & = & q_1 & q_2 & \cdots & q_t & \equiv 3 \bmod 4, \\ \text{or} & D & = & 4 & q_2 & \cdots & q_t & \equiv 4 \bmod 16, \\ \text{or} & D & = & 8 & q_2 & \cdots & q_t & \equiv 8 \bmod 16, \end{array}$$

where the q_i are disctinct prime numbers.

Let m be a positive integer, prime to $2D$. For all odd q_i we define the following character:

$$\chi_i(m) = \left(\frac{m}{q_i}\right).$$

In the case where D is odd, we can write:

$$\prod_{i=1}^{t} \chi_i(m) = \prod \left(\frac{m}{q_i}\right) = \prod (-1)^{\frac{m-1}{2}\frac{q_i-1}{2}} \left(\frac{q_i}{m}\right),$$

using the quadratic reciprocity law. With the help of lemma (3.1.1), we then have:

$$\prod_{i=1}^{t} \chi_i(m) = \prod \left(\frac{q_i^*}{m}\right) = \left(\frac{-D}{m}\right).$$

When D is even, we define χ_1 by:

$$\chi_1(m) \prod_{i=2}^{t} \chi_i(m) = \left(\frac{-D}{m}\right).$$

Let us prove:

Proposition 4.3.1 *Let m be an integer prime to $2D$, represented by the form $Q = (a, b, c)$ of discriminant $-D$. Then:*

1. $\left(\frac{-D}{m}\right) = \left(\frac{-D}{a}\right) = \left(\frac{-D}{c}\right) = 1,$
2. $\forall i,\ \chi_i(m) = \chi_i(a) = \chi_i(c).$

Proof. We write: $m = Q(x,\, y) = ax^2 + bxy + cy^2$. Therefore:

$$4am = (2ax + by)^2 + Dy^2,$$

which shows 1. Moreover, if q_i divides D, am must be a quadratic residue modulo q_i, which gives:

$$\chi_i(am) = 1 \Longleftrightarrow \chi_i(m) = \chi_i(a).$$

In the case where D is even, we have:

$$\chi_1(m) \prod_{i=2}^{t} \chi_i(m) = \left(\frac{-D}{m}\right) = 1 = \left(\frac{-D}{a}\right) = \chi_1(a) \prod_{i=2}^{t} \chi_i(a),$$

so $\chi_1(m) = \chi_1(a)$.

The same can be done with c. ∎

To a form $Q = (a, b, c)$, of discriminant $-D$, we can associate the *generic characters* $\chi_1(Q), \ldots, \chi_t(Q)$, defined by $\chi_i(Q) = \chi_i(a)$.

Genera

Let $e_1, \ldots, e_t$ be rational integers such that:

$$e_i = \pm 1,\ \prod_{i=1}^{t} e_i = 1.$$

We consider the set $G(e_1, \ldots, e_t) = \{C \in \mathcal{H}(-D),\ \chi_i(C) = e_i\}$. We recall that each class contains exactly one reduced form. So we idenfity a class with its reduced form.

To each of the 2^{t-1} possible values of t-uples $(e_1, \ldots, e_t)$, we associate the *genus* $G(e_1, \ldots, e_t)$. The *principal genus* is $G_1 = G(1, \ldots, 1)$.

Theorem 4.3.1 *Each genus contains at least one class of forms.*

Proof. Let $G = G(e_1, \ldots, e_t)$ be a genus. We prove that there exists at least one rational prime that is represented by a class of G. The rational prime p is represented by a form of G iff: $\forall\ i,\ \chi_i(p) = e_i$. This determines for each q_i at least one residue class modulo q_i. Using the Chinese remainder theorem, we build a residu class modulo D which must contain p. We then use the theorem of Dirichlet ([45]), which says that there exists an infinity of primes in this class. Eventually, we have $\left(\frac{-D}{p}\right) = 1$, because of the formula $\prod \chi_i(p) = \prod e_i = 1$. ■

Let C and C' be two (classes of) forms contained respectively in the genera G and G'. The *product* of these two genera is the genus $G'' = GG' = G(\chi_1(C''), \ldots, \chi_t(C''))$, where $C'' = CC'$. Of course, this definition is independent of the choice of C and C'.

Proposition 4.3.2 *The principal genus is a subgroup of $\mathcal{H}(-D)$.*

Proof. It is enough to show that the product of two forms of G_1 is in G_1. And this is clear, since $\chi_i(CC') = \chi_i(C)\chi_i(C') = 1$. ■

Corollary 4.3.1 *Let C be a class of forms. Put $CG_1 = \{CC_1,\ C_1 \in G_1\}$. Then the genera are exactly the sets CG_1 where C runs through $\mathcal{H}(-D)$.*

Proof. Actually, we have:

$$C' \in CG_1 \Longleftrightarrow \chi_i(C') = \chi_i(C). \blacksquare$$

Since the genera are mutually distinct, we deduce:

$$\mathcal{H}(-D) = \bigcup_{\prod e_i = 1} G_i,$$

and thus $h(-D) = 2^{t-1}\ Card(G_1)$. We proved:

Theorem 4.3.2 *The class number of $-D$ is a multiple of 2^{t-1} and the classes of forms fill 2^{t-1} genera containing $\frac{h(-D)}{2^{t-1}}$ forms each.*

We finish this section with the following theorem:

Theorem 4.3.3 (Gauss) *The principal genus G_1 is exactly the set of all squares of forms of $\mathcal{H}(-D)$.*

4.3.2 Comeback to $N_D(\pi) = p$: Euler numbers

The principal form ($(1, 0, \frac{D}{4})$ or $(1, 1, \frac{D+1}{4})$) is obviously in the principal genus. By the preceding section, the rational prime p is represented by *a* form of this genus iff $\chi_i(p) = 1$ for all i.

But there are $\nu = \frac{h(-D)}{2^{t-1}}$ forms in this genus. If $\nu = 1$, then the form that represents p is the principal one and we win. Else, we are not sure.

One knows 65 discriminants, called *Euler numbers*, for which $\nu = 1$. They are listed in the table below ([15]).

D	h(-D)	D	h(-D)	D	h(-D)	D	h(-D)	D	h(-D)
3	1	52	2	195	4	435	4	1012	4
4	1	67	1	228	4	483	4	1092	8
7	1	84	4	232	2	520	4	1155	8
8	1	88	2	235	2	532	4	1320	8
11	1	91	2	267	2	555	4	1380	8
15	2	115	2	280	4	595	4	1428	8
19	1	120	4	312	4	627	4	1435	4
20	2	123	2	340	4	660	8	1540	8
24	2	132	4	372	4	708	4	1848	8
35	2	148	2	403	2	715	4	1995	8
40	2	163	1	408	4	760	4	3003	8
43	1	168	4	420	8	795	4	3315	8
51	2	187	2	427	2	840	8	5460	16

Let $-D = \prod_{i=1}^{t} q_i^*$ be a fundamental discriminant. The genus field of $\mathbf{K}$, which is $\mathbf{K}_{\mathrm{g}} = \mathbf{Q}\left(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*}\right)$, was introduced in 4.2.2. One can show the following result:

Theorem 4.3.4 *Let p be a rational prime. Then:*

$$p \text{ splits in } \mathbf{K}_{\mathrm{g}} \iff \forall\, i,\ p \text{ splits in } \mathbf{Q}\left(\sqrt{q_i^*}\right) \iff \forall\, i,\ \chi_i(p) = +1.$$

For Euler numbers, the quest for the class field is finished. For such a number, we have seen that:

$$p = N_D(\pi) \iff \forall\, i,\ \chi_i(p) = +1.$$

Comparing to the preceding theorem, we get:

Theorem 4.3.5 *if D is an Euler number, then* $\mathbf{K}_{\mathrm{H}} = \mathbf{K}_{\mathrm{g}}$.

It remains to find the class field of an ordinary imaginary quadratic field. This will be done with the modular invariant described in the following chapter.

We conclude this chapter by describing some algorithms used to solve numericaly the problem of the representation problem.

4.4 Algorithms of resolution

4.4.1 Ideals and lattices

Let p be a rational prime that splits as $\mathfrak{p}\mathfrak{p}'$ in $\mathbf{K}$. We want a solution of $N_D(\pi) = p$. We saw that this problem is equivalent to search for an element of $\mathfrak{p}$ that minimizes N_D on $\mathfrak{p}$.

We may view $\mathfrak{p}$ as a lattice of $\mathbf{C}$. Looking for an ξ of minimal norm is the same thing as to find a shortest vector of this lattice for the euclidean metric. It is convenient to associate with an integer α of $\mathcal{O}$ ($\alpha = x + y\omega$) a vector of $\mathbf{C}$, of coordinates $X(\alpha)$ and $Y(\alpha)$ in the basis:

$$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{\sqrt{-D}}{2} \end{pmatrix}.$$

More precisely, we put:

$$X(\alpha) = \begin{cases} 2x & \text{in case (i)}, \\ 2x + y & \text{in case (ii)}, \end{cases} \tag{4.2}$$

$$Y(\alpha) = \begin{cases} 2y & \text{in case (i)}, \\ y & \text{in case (ii)}. \end{cases} \tag{4.3}$$

If $\vec{u} = \begin{pmatrix} X \\ Y \end{pmatrix}$, we then have:

$$||\vec{u}||^2 = N_D(\alpha) = \frac{X(\alpha)^2 + DY(\alpha)^2}{4},$$

in all cases. An ideal $\mathfrak{i} = (a, b + c\omega)$ is generated by: $\begin{pmatrix} 2a \\ 0 \end{pmatrix}$ and $\begin{pmatrix} X(b+c\omega) \\ Y(b+c\omega) \end{pmatrix}$. We have to find a shortest vector of $\mathfrak{i}$ for the norm associated to the scalar product:

$$\vec{u} = \begin{pmatrix} X \\ Y \end{pmatrix} \quad \vec{v} = \begin{pmatrix} X' \\ Y' \end{pmatrix} \Longrightarrow \vec{u}.\vec{v} = XX' + DYY',$$

forgetting the 4 of the denominator. The final algorithm is:

procedure RED(p, D);

(* looks for $\pi = x + y\omega$ such that $N_D(\pi) = p$ *)

1. 1. let r be the solution of:
   $$\begin{cases} r^2 & \equiv & -D \bmod p, \\ r & \equiv & D \bmod 2; \end{cases}$$
   2. we build $\vec{u} = \begin{pmatrix} 2p \\ 0 \end{pmatrix}$ and $\vec{v} = \begin{pmatrix} r \\ -1 \end{pmatrix}$, which generate $\mathfrak{p} = \left(p, \frac{r - \sqrt{-D}}{2}\right)$;
2. *reduction of* $\mathfrak{p}$ *([121])*:
   1. $\rho := \frac{(\vec{v}, \vec{u})}{(\vec{u}, \vec{u})}$, $m := \lceil \rho \rfloor$ (this is the nearest integer of ρ), $\epsilon := sgn(\rho - m)$;
   2. $\vec{v} := \epsilon(\vec{v} - m\vec{u})$;
   3. **if** $||\vec{v}|| \geq ||\vec{u}||$ **then** goto **3 else** exchange $\vec{u}$ and $\vec{v}$, goto **2.1**;
3. $\vec{u}$ is a shortest vector; we come back to $\mathcal{O}$ with the formula (4.2) and (4.3).
4. **end**.

4.4.2 Shanks' algorithm

We recall an algorithm by Shanks [114], whose goal was to find the solution of the equation:

$$mp = x^2 + Dy^2, \tag{4.4}$$

with p a rational prime and m minimal for a given D.

Here, we consider a rational prime p for which we know that it is representable by a form of a given genus. This algorithm allows us to find it.

We start with a form that trivially represents p (Cf. Corollary (4.1.1)). Let this form be $Q = (p, b, c)$. We reduce Q, obtaining a form $Q' = (a', b', c')$ and a matrix N such that: $N = \begin{pmatrix} \alpha & \beta \\ \gamma & \epsilon \end{pmatrix}$. We write:

$$\forall\ (x, y),\ px^2 + bxy + cy^2 = a'x'^2 + b'x'y' + c'y'^2, \tag{4.5}$$

where

$$\begin{pmatrix} x \\ y \end{pmatrix} = N \begin{pmatrix} x' \\ y' \end{pmatrix}.$$

We plug it in (4.5) and find:

$$p = a'\epsilon^2 - b'\epsilon\gamma + c'\gamma^2. \tag{4.6}$$

Finally, we are sure that a' is minimal in this equation, because of the reduction process. When p can be represented by the principal form, we are sure to find it.

4.4.3 To finish with the numerical methods

Suppose we are in case (i). Finding a π in $\mathcal{O}$ such that $N_D(\pi) = p$ is equivalent to solve: $x^2 + \frac{D}{4}y^2 = p$.

There is an algorithm, due to Cornacchia ([38]), which solves this problem. It can be interesting to compare this article with those of [19] and [132].

procedure CORNACCHIA(q, m);

(* solution of $u^2 + qv^2 = m$ *)

1. let x_0 be a solution of $x^2 \equiv -q \bmod m$ that satisfies $m > x_0 > \frac{m}{2}$.

2. we develop $\frac{m}{x_0}$ as a continued fraction:

$$\begin{array}{ll} m & = q_0 x_0 + x_1 \\ x_0 & = q_1 x_1 + x_2 \\ \ldots & \\ x_r & = q_{r+1} x_{r+1} + x_{r+2} \end{array}$$

   and we stop when $x_r^2 < m \leq x_{r-1}^2$;

3. if the equation has a solution, it is:

$$u = x_r \text{ and } v = \sqrt{\frac{m - x_r^2}{q}}.$$

Chapter 5

Primality testing using elliptic curves

5.1 Introduction to elliptic curves

5.1.1 Definition and first properties

In all that follows, $\mathbf{k}$ is a field of characteristic different from 2 and 3. An *elliptic curve* defined over $\mathbf{k}$ is a non singular projective algebraic curve of genus 1. One shows ([119]) that E is isomorphic to a curve with an homogeneous equation of the form:

$$y^2\, z = 4\, x^3 - g_2\, x\, z^2 - g_3 z^3, \tag{5.1}$$

with g_2 and g_3 in $\mathbf{k}$. This type of equation is called a *Weierstrass model.* We identify E to this curve. In the sequel, every elliptic curve is supposed to be defined by such an equation.

The affine part of E is the set of points of $\mathbf{k}$ that satisfie (5.1) and for which a system of homogeneous coordinates is $(x : y : 1)$. The *point at infinity*, of coordinates $(0 : 1 : 0)$ is noted O_E. The affine equation of E is:

$$y^2 = 4\, x^3 - g_2\, x - g_3. \tag{5.2}$$

We note $E(\mathbf{k})$ the set of points $(x,\, y)$ of $\mathbf{k}$ satisfying (5.1), together with O_E.

Definition 5.1.1 *Classically ([119]), we define the following quantities:*

$$\Delta = g_2^3 - 27\, g_3^2 : \textit{this is the } \text{discriminant} \textit{ of the curve}; \tag{5.3}$$

$$j = 1728\, \frac{g_2^3}{\Delta} : \textit{this is the } \text{modular invariant} \textit{ of } E. \tag{5.4}$$

Proposition 5.1.1 *E is singular iff $\Delta = 0$.*

Proposition 5.1.2 *Every element of* $\mathbf{k}$ *appears as the modular invariant of an elliptic curve E over* $\mathbf{k}$*.*

Proof. We give an effective proof.

- if $j = 0$, we may take the curve of equation

$$y^2 = 4x^3 - g_3,\ g_3 \neq 0; \tag{5.5}$$

- if $j = 1728$, we take:

$$y^2 = 4x^3 - g_2 x,\ g_2 \neq 0; \tag{5.6}$$

- if $j \neq 0$ et $j \neq 1728$, we put $h = \frac{27j}{j-1728}$ and the curve of equation:

$$y^2 = 4x^3 - h(x+1), \tag{5.7}$$

has j for invariant. ■

Theorem 5.1.1 ([55, Th. IV.4.1]) *Suppose that* **k** *is algebraically closed. Then E and E' are isomorphic iff $j(E) = j(E')$.*

Corollary 5.1.1 ([119]) *If* **k** *is algebraically closed, E and E' are isomorphic iff there exists u in* **k** *such that:*

$$g_2 = u^4\, g_2'. \tag{5.8}$$

$$g_3 = u^6\, g_3'. \tag{5.9}$$

As a consequence, if c is an element of **k** that is not q square, the curves corresponding to $(g_2,\, g_3)$ and $(c^2 g_2,\, c^3 g_3)$ are not isomorphic.

5.1.2 Group law on an elliptic curve

We define on a curve E over **k** an abelian law that we note additively. In the sequel, we use the same notation for the group and for the curve. To simplify things a little, we place ourself in the case where $\mathbf{k} = \mathbf{R}$.

In **R**, we consider the curve of equation:

$$y^2 = 4\,x^3 - g_2\,x - g_3. \tag{5.10}$$

If it is not singular, its discriminant is non zero. The shape of this curve is shown in figure 1. Let M_1 and M_2 be two points on the curve. We want to compute the point M_3 which is the sum of M_1 and M_2. We call $\mathcal{D}$ the line $M_1 M_2$ (if $M_1 = M_2$, $\mathcal{D}$ is the tangent line to E in M_1). We see that $\mathcal{D}$ meets E in a third point P. We then take for M_3 the point which is the reflexion of P about the the x-axes. We add also the following rules:

. $O_E + O_E = O_E$.

. $M + O_E = M$.

. the opposite of M of coordinates $(x,\, y,\, 1)$ is $(x,\, -y,\, 1)$.

We now work out explicit formulas giving the coordinates of M_3.

Figure 5.1: An elliptic curve over **R**.

Effective computation of the law

Let M_1 and M_2 be two points on the curve of respective coordinates $(x_1 : y_1 : 1)$ and $(x_2 : y_2 : 1)$. The point M_3, which is the sum of M_1 and M_2 has coordinates $(x_3 : y_3 : z_3)$. The equation of $\mathcal{D}$ is $y = \lambda\, x + \mu$, with

$$\lambda = (y_2 - y_1)(x_2 - x_1)^{-1} \text{ if } x_1 \neq x_2,$$

$$\lambda = (12\, x_1^2 - g_2)(2y_1)^{-1} \text{ otherwise.}$$

We intersect the line $\mathcal{D}$ with E and we find:

$$4\, x^3 - \lambda^2 x^2 - (2\, \lambda\, \mu + g_2)x - g_3 - \mu^2 = 0.$$

Since x_1, x_2 and x_3 are the three roots of this equation, we find: $x_1 + x_2 + x_3 = \frac{\lambda^2}{4}$. We deduce:

$$x_3 = \frac{\lambda^2}{4} - x_1 - x_2, \tag{5.11}$$

$$y_3 = \lambda(x_1 - x_3) - y_1. \tag{5.12}$$

These formulas are valid in the case where $\mathbf{k}$ is any field (with characteristic different from 2 and 3).

5.2 Lattices and elliptic curves

The aim of this section is to describe the relationship between elliptic curves over $\mathbf{C}$ and lattices. This will enable us to find an expression of the invariant j well suited for computation.

In the two following sections, we take $\mathbf{k} = \mathbf{C}$.

5.2.1 Weierstrass's function

We first follow [23], in which the proofs of the following results can be found.

Definition 5.2.1 *A* lattice *L in $\mathbf{C}$ is a discrete subgroup of $\mathbf{C}$ generated by two vectors ω_1 and ω_2, that we can take to satisfy $\mathrm{Im}(\frac{\omega_1}{\omega_2}) > 0$. We let: $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$.*

Figure 5.2: A lattice.

Proposition 5.2.1 *The series defined by:*

$$\frac{1}{z^2} + \sum_{l \in L, l \neq 0} \left(\frac{1}{(z-l)^2} - \frac{1}{l^2} \right) \tag{5.13}$$

is normally convergent on every compact included in $\mathbf{C} - L$.

Definition 5.2.2 *The sum of this series is called the* Weierstrass function *associated with the lattice L. It is denoted by $\wp_L(z)$.*

The proof of this proposition requires the following lemma, that we shall need later on.

Lemma 5.2.1 *Let k be an integer. Then, the series*

$$\sum_{l\in L,\, l\neq 0} \frac{1}{l^k}$$

is absolutely convergent for $k > 2$. Its sum is denoted by $G_k(L)$.

Proposition 5.2.2 *The function $\wp_L$ satisfies the following properties:*
1. $\wp_L$ is meromorphic and its poles are exactly the points of L. All the poles are double and the residus at these points are zero;
2. $\wp_L$ is even on L.

Theorem 5.2.1 *The function $\wp_L$ is differentiable and:*

$$\wp_L'(z) = -2 \sum_{l\in L} \frac{1}{(z-l)^3}.$$

Proposition 5.2.3 *The function $\wp_L'$ is periodic on L.*

Corollary 5.2.1 *The function $\wp_L$ is periodic on L.*

5.2.2 Expansion of $\wp$ near the origin

We follow [69]. We write:

$$\frac{1}{(z-l)^2} = \frac{1}{l^2(1-\frac{z}{l})^2}$$

$$= \frac{1}{l^2} + \frac{2\,z}{l^3} + \cdots + \frac{k\,z^{k-1}}{l^{k+1}} + \cdots$$

Hence, we deduce:

$$\wp_L(z) = \frac{1}{z^2} + 2\,z\,G_3(L) + \cdots + k\,z^{k-1}\,G_{k+1}(L) + \cdots$$

This formula is valid by lemma (5.2.1). We see that $G_{2k+1} = 0$ because $\wp(-l) = -\wp(l)$ on L. We have proven:

Theorem 5.2.2

$$\wp_L(z) = \frac{1}{z^2} + 3\,z^2\,G_4(L) + 5\,z^4\,G_6(L) + \cdots \tag{5.14}$$

Corollary 5.2.2

$$\wp_L'(z) = -\frac{2}{z^3} + 6\,z\,G_4(L) + 20\,z^3\,G_6(L) + \cdots \tag{5.15}$$

Proposition 5.2.4 *We put $g_2(L) = 60\,G_4(L)$ and $g_3(L) = 140\,G_6(L)$. Then:*

$$\forall\, z \in \mathbf{C} - L,\ \wp'^2(z) = 4\,\wp(z)^3 - g_2\,\wp(z) - g_3. \tag{5.16}$$

Theorem 5.2.3 *Let us consider the curve defined by the equation:*

$$y^2 = 4\,x^3 - g_2(L)\,x - g_3(L). \tag{5.17}$$

Then:

1. the equation $4\,x^3 - g_2\,x - g_3 = 0$ has three distinct roots;

2. for every point $(x : y : 1)$ on the curve, there exists a z in $\mathbf{C}$ such that $x = \wp(z)$ and $y = \wp'(z)$.

Conversely, if we are given the curve E of equation $y^2 = 4\,x^3 - a_2\,x - a_3$ in $\mathbf{C}$, such that the right hand side has three distinct roots, then there is a lattice L for which $a_2 = g_2(L)$ and $a_3 = g_3(L)$. The function $\wp_L$ associated to that lattice yields a parametrization of the curve.

Let $L = \omega_1\mathbf{Z} + \omega_2\mathbf{Z}$ be the above lattice. Putting $\tau = \frac{\omega_1}{\omega_2}$, with $\mathrm{Im}(\tau) > 0$, we may write: $L(\omega_1, \omega_2) = \omega_2\,L(1, \tau)$. Then:

$$g_2(L(\omega_1, \omega_2)) = \omega_2^4\,g_2(L(1, \tau))\ et\ g_3(L(\omega_1, \omega_2)) = \omega_2^6\,g_3(L(1, \tau)). \tag{5.18}$$

Therefore, the curve E is isomorphic to the curve defined by the lattice $L(1, \tau)$. In the sequel, we identify the two curves.

Let ψ be the function:

$$\begin{array}{cccl} \psi: & \mathbf{C} & \longrightarrow & E \\ & z & \longmapsto & (\wp(z) : \wp'(z) : 1) \text{ si } z \notin \mathrm{L} \\ & z & \longmapsto & O_E \text{ si } z \in \mathrm{L}. \end{array}$$

This yields a group isomorphism $\Psi : \mathbf{C}/L \longrightarrow E$. We thuis identify an elliptic curve to $\mathbf{C}/$ Land this gives a parametrization for E.

5.2.3 Another expression for G_k

We restrict ourself to the study of the lattice $L = \mathbf{Z} + \tau\mathbf{Z}$, where τ is a complex number of imaginary positive part. We look for an expression of $G_{2k}(L)$ which is suitable for the computation of the invariant of a curve. We omit the subscript L without ambiguity.

We write:

$$G_{2k} = \sum_{(m,\,n)\neq(0,\,0)} \frac{1}{(m\,\tau + n)^{2k}}. \tag{5.19}$$

Then:

$$G_{2k} = \sum_{n\neq 0} \frac{1}{n^{2k}} + \sum_{m\neq 0} \sum_{n=-\infty}^{+\infty} \frac{1}{(m\,\tau + n)^{2k}}, \tag{5.20}$$

$$G_{2k} = 2\,\zeta(2k) + 2 \sum_{m=1}^{+\infty} \sum_{n=-\infty}^{+\infty} \frac{1}{(m\,\tau + n)^{2k}}, \tag{5.21}$$

where ζ is the Riemann function.

Starting from:

$$\pi\ \cot \pi\, a = \frac{1}{a} + \sum_{n=1}^{+\infty} \left(\frac{1}{a+n} + \frac{1}{a-n} \right),\ a \notin bfZ, \tag{5.22}$$

we get by differentiation:

$$\frac{\pi^2}{\sin^2 \pi\, a} = \sum_{n \in Z} \frac{1}{(a+n)^2}. \tag{5.23}$$

With:

$$\sin \pi\, a = -\frac{e^{-i\pi\, a}}{2\, i}\,(1 - e^{2\, i\, \pi\, a}), \tag{5.24}$$

we find:

$$\frac{\pi^2}{\sin^2 \pi\, a} = (2i\pi)^2 \sum_{d \geq 1} d\, e^{2i\pi a d}. \tag{5.25}$$

We finish the computation by differentiating (5.25). We have proved:

Lemma 5.2.2

$$\sum_{n \in Z} \frac{1}{(a+n)^{2k}} = \frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{d \geq 1} d^{2k-1}\, e^{2i\pi a d},\ k \geq 1. \tag{5.26}$$

If we come back to L and put $a = m\tau$ and $q = e^{2i\pi\tau}$:

$$G_{2k}(\tau) = 2\,\zeta(2k) + 2\,\frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{\substack{m \geq 1 \\ d \geq 1}} d^{2k-1}\, q^{m\, d}, \tag{5.27}$$

which may be rewritten as:

$$G_{2k}(\tau) = 2\,\zeta(2k) + 2\,\frac{(2i\pi)^{2k}}{(2k-1)!} \sum_{n \geq 1} \sigma_{2k-1}(n)\, q^n, \tag{5.28}$$

where:

$$\sigma_r(n) = \sum_{d | n} d^r. \tag{5.29}$$

We give another form to this expression introducing the Bernouilli numbers. Let us consider the following series ([113]):

$$\frac{x}{e^x - 1} = \sum_{k=0}^{+\infty} b_k\, \frac{x^k}{k!}. \tag{5.30}$$

Proposition 5.2.5 *For every $k \geq 1$, $b_{2k+1} = 0$.*

Definition 5.2.3 *The k-th Bernouilli number is: $B_k = (-1)^{k+1}\, b_{2k}$.*

Theorem 5.2.4

$$\forall\ k \geq 1,\ \zeta(2k) = \frac{2^{2k-1}}{(2k)!}\, B_k\, \pi^{2k}. \tag{5.31}$$

Plugging this relation in (5.28), we find:

$$G_{2k}(\tau) = 2\,\zeta(2k) \left(1 + \frac{(-1)^k\, 4k}{B_k} \sum_{n \geq 1} \sigma_{2k-1}(n)\, q^n \right). \tag{5.32}$$

We put:

$$E_{2k} = \frac{G_{2k}}{2\,\zeta(2k)}. \tag{5.33}$$

In particular:

$$k = 2 : \zeta(4) = \frac{\pi^4}{90},\ B_2 = \frac{1}{30},\ E_4(\tau) = 1 + 240 \sum_{n\geq 1} \sigma_3(n)\, q^n. \tag{5.34}$$

$$k = 3 : \zeta(6) = \frac{\pi^6}{945},\ B_3 = \frac{1}{42},\ E_6(\tau) = 1 - 504 \sum_{n\geq 1} \sigma_5(n)\, q^n. \tag{5.35}$$

5.2.4 Expansion of j

By definition:

$$j(\tau) = 1728\, \frac{g_2^3(L)}{g_2^3(L) - 27\, g_3^2(L)}. \tag{5.36}$$

If we use the preceding results, we find:

$$j(\tau) = 1728\, \frac{E_4^3(q)}{E_4^3(q) - E_6^2(q)},\ q = e^{2i\pi\tau}. \tag{5.37}$$

Definition 5.2.4 *A* modular function of weight $2k$ *is a holomorphic function on* $H = \{z \mid \mathrm{Im} z > 0\}$, *which is meromorphic at infinity and satisfying:*

$$\forall\, z \in H,\ \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}),\ f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right). \tag{5.38}$$

Proposition 5.2.6 *The function $j(\tau)$ is a modular function of weight 0.*

We then develop j as a function of q (Cf. [28], VI.3):

Theorem 5.2.5

$$j(q) = \frac{1}{q} \left(1 + \sum_{n\geq 1} a_n\, q^n\right)^3, \tag{5.39}$$

with a_n a positive integer.

We deduce:

Corollary 5.2.3

$$j(q) = \frac{1}{q} + 744 + \sum_{n\geq 1} c_n\, q^n, \tag{5.40}$$

with c_n positive.

We shall have to compute the values of $j(\tau)$ for some τ and thus we have to compute the c_n's. We list their properties.

We begin by the expression of c_n as a series. This development was found independantly by Petersson [96] and Rademacher [106], using two different methods.

Theorem 5.2.6

$$c_n = \frac{2\pi}{\sqrt{n}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_1\left(\frac{4\pi\sqrt{n}}{k}\right), \tag{5.41}$$

with:

$$A_k(n) = \sum_{\substack{0<h<k,\ (h,k)=1 \\ hh'\equiv -1 \bmod k}} e^{-\frac{2i\pi}{k}(nh+h')}, \tag{5.42}$$

$$I_1(X) = -iJ_1(iX), \tag{5.43}$$

where J_1 is the first Bessel function:

$$J_1(z) = \sum_{\nu=0}^{\infty} \frac{(-1)^{\nu} z^{2\nu+1}}{2^{2\nu+1}\nu!(\nu+1)!}. \tag{5.44}$$

We deduce:

Corollary 5.2.4

$$c_n \sim \frac{e^{4\pi\sqrt{n}}}{\sqrt{2}\, n^{\frac{3}{4}}}. \tag{5.45}$$

On the other hand, the c_n's enjoy the following striking arithmetical properties, that will be useful to check our computations.

Theorem 5.2.7

If	$n \equiv 0 \bmod 2^a$	*then*	$c_n \equiv 0 \bmod 2^{3a+8}$	*([79])*
	$n \equiv 0 \bmod 3^b$		$c_n \equiv 0 \bmod 3^{2b+3}$	*([79])*
	$n \equiv 0 \bmod 5^c$		$c_n \equiv 0 \bmod 5^{c+1}$	*([78])*
	$n \equiv 0 \bmod 7^d$		$c_n \equiv 0 \bmod 7^d$	*([78])*
	$n \equiv 0 \bmod 11^e$		$c_n \equiv 0 \bmod 11^e$	*([5,78])*

(See also [6,4,77,94,123]).

We give in the appendix the values of c_n and a_n for $n \leq 160$, computed with MAPLE on a SUN 3/60. We give below the first ten coefficients, together with their factorization.

n		c_n
1	1	$2^2.3^3.1823$
2	2	$2^{11}.5.2099$
3	3	$2.3^5.5.355679$
4	2^2	$2^{14}.3^3.45767$
5	5	$2^3.5^2.2143.777421$
6	2.3	$2^{13}.3^6.11.13^2.383$
7	7	$3^3.5.7.271.174376673$
8	2^3	$2^{17}.3.5^3.199.41047$
9	3^2	$2^2.3^7.5.4723.15376021$
10	2.5	$2^{12}.3^5.5^2.13^2.5366467$

Some functions linked to j

We define ([125, III-§25]):

$$f(q) = q^{-\frac{1}{48}} \prod_{m\geq 1} \left(1 + q^{m-\frac{1}{2}}\right), \tag{5.46}$$

$$f_1(q) = q^{-\frac{1}{48}} \prod_{m\geq 1} \left(1 - q^{m-\frac{1}{2}}\right), \tag{5.47}$$

$$f_2(q) = \sqrt{2}\, q^{\frac{1}{24}} \prod_{m\geq 1} (1 + q^m), \tag{5.48}$$

where as usual $q = e^{2i\pi\tau}$. These three functions satisfy numerous identities. We only need:

$$j(q) = \frac{\left(f(q)^{24} - 16\right)^3}{f(q)^{24}} = \frac{\left(f_1(q)^{24} + 16\right)^3}{f_1(q)^{24}} = \frac{\left(f_2(q)^{24} + 16\right)^3}{f_2(q)^{24}}, \tag{5.49}$$

$$f(q)f_1(q)f_2(q) = \sqrt{2}. \tag{5.50}$$

(Cf. [125, III-§54]). We also set:

$$\gamma_2(q) = \sqrt[3]{j(q)},\ \gamma_3(q) = \sqrt[3]{j(q) - 12^3}, \tag{5.51}$$

where the cube root of the complex number z is taken as:

$$z = \rho\, e^{i\theta} \Rightarrow \sqrt[3]{z} = \sqrt[3]{\rho}\, e^{\frac{i\theta}{3}}.$$

5.2.5 Back to the isomorphism between lattices and curves

It is convenient to associate an elliptic curve E with a unique complex number τ such that $E \cong \mathbf{C}/L(1,\tau)$.

Theorem 5.2.8 ([61, 1, II, 4, 3]) *Let τ and τ' be two complex numbers. Let E and E' the curves respectively defined by $j(\tau)$ and $j(\tau')$. Then: $j(\tau) = j(\tau')$ iff there exist a, b, c, e in $\mathbf{Z}$ such that $ae - bc = \pm 1$ and:*

$$\tau' = \frac{a\tau + b}{c\tau + e}.$$

Moreover, if τ' is given, there is a unique τ such that $j(\tau) = j(\tau')$ and

$$\left\{\begin{array}{c} -\frac{1}{2} \leq \Re(\tau) < \frac{1}{2}, \\ \mid \tau \mid \geq 1 \text{ if } \Re(\tau) \leq 0, \\ \mid \tau \mid > 1 \text{ if } \Re(\tau) > 0. \end{array}\right. \tag{5.52}$$

In other words, E and E' are isomorphic iff $L(1,\tau)$ and $L(1,\tau')$ are homothetic. We have thus settled an equivalence relation between elliptic curves via lattices. The classes of equivalence are definde by the above conditions.

5.3 Complex multiplication

We have seen that it is possible to associate a curve E with a lattice L, generated by $(1, \tau)$, with $\mathrm{Im}\,\tau > 0$. We suppose that τ satisfies (5.52).

We introduce the set $End_k E$ of the endomorphisms of $E(\mathbf{k})$, seen as a group. It is a ring for operations $+$ and $\circ$ and is contains the identity for $\circ$. One shows ([55, th.IV.4.18]) that we can identify an element f of $End_k E$ with an homomorphism of $\mathbf{C}$ that keeps L unchanged by means of the function Ψ defined above. Such an homomorphism is in fact the multiplication by a complex number α. Let $\mathcal{A} = \{\alpha \in C \mid \alpha\ L \subset L\}$. We recognize the stabilizer of L. It is obvious that $\mathbf{Z} \subset \mathcal{A}$, and a fortiori $\mathcal{A}$ has a neutral element.

Definition 5.3.1 *The curve E has* complex multiplication by $\mathcal{A}$ *if $\mathcal{A} \neq \mathbf{Z}$.*

Theorem 5.3.1 ([55, th.IV.4.19]) *If E has complex multiplication, then there exists a $\delta > 0$ such that $\tau \in K_{-\delta}$. Moreover, $\mathcal{A}$ is a subset of the ring of integers of $K_{-\delta}$.*

Conversely, if $\tau = r + s\sqrt{-\delta}$, with r and s in $\mathbf{Q}$, E has complex multiplication. The ring of endomorphisms of E is isomorphic to

$$\{a + b\tau \mid a,\ b \textit{ in } \mathbf{Z} \textit{ and } 2br,\ b(r^2 + \delta s^2) \textit{ in } \mathbf{Z}\ \}.$$

Proof. Let us prove the first assertion. Let α be an element of $\mathcal{A}$, but not of $\mathbf{Z}$. Then, there exist rational integers a, b, c, and e such that:

$$\begin{cases} \alpha & = & a & + & b\tau \\ \alpha\tau & = & c & + & e\tau. \end{cases} \tag{5.53}$$

Since E has complex multiplication, $b \neq 0$. We find:

$$b\tau^2 + (a - e)\tau - c = 0, \tag{5.54}$$

which we write: $A\tau^2 + B\tau + C = 0$, with A, B, C mutually prime and $A > 0$. Since $\tau \notin \mathbf{R}$, the discriminant of this equation is negative. Hence, there is a $\delta > 0$ such that τ belongs to $K_\delta = \mathbf{Q}(\sqrt{-\delta})$. We write: $\tau = \frac{-B+\sqrt{-\delta}}{2A}$.

By (5.53), α is an element of K_δ and in fact an integer:

$$\alpha^2 - (a - e)\alpha + (ae - bc) = 0. \tag{5.55}$$

We have proved that $\mathcal{A}$ is an order of K_δ. We say that $\mathcal{A}$ is the *order* of $\mathrm{L}(1, \tau)$.

Conversely, let $\tau = r + s\sqrt{-\delta}$, with r and s in $\mathbf{Q}$. We are looking for $\alpha = a + b\tau$, with a and b in $\mathbf{Z}$, such that $\alpha\,\tau \in$ L. This implies that $\alpha\tau = a\tau + b\tau^2$ and thus $b\tau^2 \in$ L. But $\tau^2 = -(r^2+\delta s^2)+2r\tau$. We must have $2br \in \mathbf{Z}$ and $b(r^2 + \delta s^2) \in \mathbf{Z}$. The conditions are clearly sufficient and $\mathcal{A}$ is the desired set. It is clear that $\mathcal{A}$ is not equal to $\mathbf{Z}$. Therefore, E has complex multiplication. ■

Let E be a curve with multiplication and τ a quadratic number such that: $E \cong \mathbf{C}/\mathbf{L}(1, \tau)$. To τ is associated the quadratic form (A, B, C) where $A\tau^2 + B\tau + C = 0$. This is equivalent to say $\tau = \frac{-B+\sqrt{-\delta}}{2A}$. We rewrite conditions (5.52):

$$\mid \tau \mid = \frac{C}{A},$$

$$-A \leq B < A,$$
$$B \geq 0 \Longrightarrow C \geq A,$$
$$B < 0 \Longrightarrow C > A.$$

It follows that (A, B, C) is reduced. We can rephrase the conclusion of the above theorem. The isomorphism classes of elliptic curves with complex multiplication are in a one-to-one correspondance with the reduced forms of $\mathcal{H}(-d)$.

5.3.1 Class field of $\mathbf{Q}(\sqrt{-D})$

Let $-D$ be a fundamental discriminant and $\mathbf{K}$ the field $\mathbf{Q}(\sqrt{-D})$. We can now describe the class field $\mathbf{K}_{\mathrm{H}}$. Let $C_1, \ldots, C_h$ be the (representants of the) classes of quadratic forms od discriminant $-D$. To each class $C_r = (a_r, b_r, c_r)$, we associate the complex numbers $\tau_r = \frac{-b_r+\sqrt{-D}}{2a_r}$ and $j(\tau_r)$. This defines an elliptic curve $E_r \cong \mathbf{C}/\mathrm{L}(1, \tau_r)$, which has complex multiplication by the order of $\mathrm{L}(1, \tau_r)$. Then:

Theorem 5.3.2 ([125, III, §-115], [14], [116, C.coro.11.1.1])

1. *the $j(\tau_r)$ are algebraic of degree $h(-D)$;*
2. *$\mathbf{K}(j(\tau_r))$ is independant of r and it is exactly the class field $\mathbf{K}_{\mathrm{H}}$.*

From the general theory, we deduce that the Galois group $G = \mathrm{Gal}(\mathbf{K}_{\mathrm{H}}|\mathbf{K})$ is isomorphic to $\mathcal{H}(-D)$. More precisely, if C is in $\mathcal{H}(-D)$ and σ_C in G is its image through the Artin isomorphism, we have:

$$\forall\ r,\ \sigma_C(j(C_r)) = j(C^{-1}C_r). \tag{5.56}$$

The quest for the class field of $\mathbf{K}$ is finished. The final conclusion is:

Theorem 5.3.3 *The equation $N_D(\pi) = p$ has a solution iff p splits in $\mathbf{K}$ as $(p) = \mathfrak{p}\mathfrak{p}'$ and $\mathfrak{p}$ (resp. $\mathfrak{p}$') splits in the field $\mathbf{K}_{\mathrm{H}} = \mathbf{Q}(\sqrt{-D}, j(\omega))$, where ω generates $\mathcal{O}$.*

5.4 Elliptic curves over finite fields

In order to simplify the formulas, we suppose that an elliptic curve is given by:

$$y^2 = x^3 + ax + b. \tag{5.57}$$

We deduce:

$$\Delta = -16\,(4\,a^3 + 27\,b^2). \tag{5.58}$$

5.4.1 $n = p^\alpha$, p prime

The notion of elliptic curve over the field $\mathbf{F}_{p^\alpha}$ is well defined. We restrict ourself to the case where $\alpha = 1$. The results that follow can be generalized easily. We put $\mathbf{k} = \mathbf{Z/pZ}$.

The property of complex multiplication is defined essentially in the same way as the case of $\mathbf{C}$. One can show the following result:

Theorem 5.4.1 ([41]) *Let E be an elliptic curve over $\mathbf{k}$. Then $End_k E$ is isomorphic to the ring of integers of a quadratic field $\mathbf{K} = \mathbf{Q}(\sqrt{-D})$.*

It is convenient to introduce the particular endomorphism, called the *Frobenius*:

$$\begin{array}{cccc} \pi_p : & E & \longrightarrow & E \\ & (x:y:1) & \longmapsto & (x^p : y^p : 1). \end{array} \tag{5.59}$$

The curve E can be seen as the kernel of the endomorphism $\pi_p - Id$.

Theorem 5.4.2 *The endomorphism π_p is associated with an integer π of $\mathcal{O}_{-D}$ satisfying $N_D(\pi) = p$ (i.e. $p = \pi\pi'$). Moreover, the number of points on E is:*

$$m = (\pi - 1)(\pi' - 1) = p + 1 - (\pi + \pi'). \tag{5.60}$$

Corollary 5.4.1 (Hasse)

$$|\, p + 1 - m \,| \leq 2\sqrt{p} \tag{5.61}$$

Corollary 5.4.2 *Conversely, put $t = p+1-m$ and $D = 4p-t^2$. Then E has complex multiplication by $\mathcal{O}_{-D}$.*

Suppose now that p is a rational prime, $-D$ is a fundamental discriminant such that $\left(\frac{-D}{p}\right) = 1$. Suppose also that we have found $\pi \in \mathcal{O}_{-D}$ ($K = \mathbf{Q}(\sqrt{-D})$), such that $N_K(\pi) = p$. To this π we associate the Frobenius of a curve E defined over $\mathbf{k}$ such that the number of points on this curve is precisely $m = p + 1 - (\pi + \pi')$. This curve is completely characterized by a root j of $P_D(X) \bmod p$. It remains to say that $P_D(X)$ has all its roots in $\mathbf{k}$ and that all corresponding curves have the same number of points. By proposition (4.1.1), there are eaxctely $w(-D)$ elliptic curves with complex multiplication by $\mathcal{O}_{-D}$, characterized by their numer of points m.

Complementary results

The equations (5.11) and (5.12) define on E an abelian law. The structure of $E(\mathbf{Z/pZ})$ is described in the following theorem.

Theorem 5.4.3 ([24]) *The group $E(\mathbf{Z/pZ})$ is either a cyclic group or the product of two cyclic groups $E = E_{m_1} \times E_{m_2}$, with:*

$$m_1 \mid m_2 \textit{ and } m_1 \mid \gcd(p-1,\, m). \tag{5.62}$$

5.4.2 Elliptic curve over Z/nZ, $n \neq p^\alpha$

In this case, $\mathbf{Z/nZ}$ is not a field. Nevertheless, it is possible to define the notion of elliptic curve over a ring (Cf. [16,81]). We just need a more flexible definition.

Following [32,81], we let:

$$V_n = \{(x, y) \in \mathbf{Z/nZ},\ y^2 \equiv x^3 + ax + b \bmod n\} \cup \{O_n\},$$

with $(\Delta, n) = 1$. If P and Q are two elements of V_n, and p a prime divisor of n, we note P_p and Q_p their image by the projection of V_n on V_p (reduction modulo p). We remark that V_p is a non singular elliptic curve, since $(\Delta, p) = 1$.

On V_n, we define an operation, again noted $+$, which has the following properties. If P and Q are in V_n, the application of $+$ to the pair (P, Q) yields either a divisor of n or an element R of V_n which satisfies $R_p = P_p + Q_p$ for all prime divisor p of n. This operation has been named *pseudo addition* by Henri Cohen. We give below the algorithm used to encode this opreation.

procedure PSEUDOADD(P, Q, R, n, d);

(* $R := P + Q$, d is a factor of n *)

(* P = (x_1, y_1, z_1), Q = (x_2, y_2, z_2), R = (x_3, y_3, z_3) *)

1. **if** $P = O_n$ **then** $R := Q$; go to 5.
2. **if** $Q = O_n$ **then** $R := P$; go to 5.
3.
   1. $d := \gcd(x_2 - x_1, n)$;
   2. **if** $1 < d < n$ **then** go to 5.
   3. **if** $d = 1$ **then**
      1. $m := (y_2 - y_1)(x_2 - x_1)^{-1}$;
      2. $x_3 := m^2 - x_1 - x_2$;
      3. $y_3 := m(x_1 - x_3) - y_1$;
      4. go to 5.
4.
   1. $d := \gcd(y_1 + y_2, n)$;
   2. **if** $1 < d < n$ **then** go to 5.
   3. **if** $d = n$ **then** $R := O_n$; go to 5.
   4.
      1. $m := (3x_1^2 + a)(y_2 + y_1)^{-1}$;
      2. $x_3 := m^2 - x_1 - x_2$;
      3. $y_3 := m(x_1 - x_3) - y_1$;
5. **end.**

In the sequel, the operations we have to do on such a curve will be done with this algorithm. If we find a factor n in any step, we suppose that we stop all our computations to declare that n is composite.

We can now explain the Goldwasser-Kilian-Atkin test.

5.5 The GK algorithm

In order to test an integer for primality using elliptic curves, we need a theorem which is the analogue of theorem (2.2.2). We must be careful in stating such a theorem, because $E(\mathbf{Z}/\mathbf{pZ})$ is not always a cyclic group.

Theorem 5.5.1 *Let n be an integer greater than 1 and prime to 6. Let E be an elliptic curve over $\mathbf{Z}/\mathbf{nZ}$, m and s two integers such that $s \mid m$. Suppose we have found a point P on E that satisfies $m\,P = O_E$. We suppose also that for each prime factor q of s, we were able to compute verify that $\frac{m}{q}P \neq O_E$ using the preceding procedure without finding a factor of n. Then if p is a prime divisor of n, $\#E(Z/pZ) \equiv 0 \bmod s$.*

Corollary 5.5.1 *If $s > (\sqrt[4]{n}+1)^2$, then n is prime.*

Remark: if n is prime, m is the number of points on the curve and its role is that of $n-1$ in theorem (2.2.2).

Proof of the theorem. Let p be a prime divisor of n. We note E_p the curve E($\mathbf{Z}/\mathbf{pZ}$). Let Q be the point of E defined by $Q = (\frac{m}{s})P$. We call Q_p the corresponding point on E_p.

Since $mP = O_E$, we deduce that $s\,Q = O_E$ and $s\,Q_p = O_{E_p}$. If ω is the order of Q_p, we see that $\omega \mid s$.

If $q \mid s$, $(\frac{s}{q})Q_p = (x_q : y_q : z_q)$ on E_p. By assumption, $(\frac{s}{q})Q_p = \frac{s}{q}\,\frac{m}{s}\,P = (\frac{m}{q})P$ and $z_q \not\equiv 0 \bmod p$. Hence $\omega \not| \frac{s}{q}$. Therefore, $\omega = s$.

Since the order of a point of E_p divides the number of points on the curve, we have

$$\#E_p \equiv 0 \bmod s. \blacksquare \tag{5.63}$$

Proof of the corollary. If n is composite, there is a prime $p \leq \sqrt{n}$ that divides n. We know by the preceding theorem that $\#E_p = \alpha\,s$, with $\alpha \geq 1$. By Hasse's theorem: $\alpha\,s \leq (\sqrt{p}+1)^2$. We deduce that $(\sqrt{p}+1)^2 > \alpha\,(\sqrt[4]{n}+1)^2$, and thus $\sqrt{p}+1 > \sqrt{\alpha}(\sqrt{p}+1)$, which is impossible. Thus n is prime. $\blacksquare$

In order to use this theorem, it is imperative to find E and its number of points $m = \#E_n$. Schoof ([112]) has given an algorithm that computes the number of points on an elliptic curve defined over a finite field and that has a running time $O(\log^8 n)$ (Cf. [81]). We can now describe the **GK** algorithm.

procedure GK(n);

1. choose a non singular elliptic curve E over $\mathbf{Z}/\mathbf{nZ}$, for which the number of points m (computed with Schoof' algorithm) satisfies $m = 2\,q$, with q a probable prime;
2. if (E, m) satisfy the conditions of the theorem with $s = m$, then n is prime, else it is composite;
3. the primality of q is proved in the same way;
4. **end.**

The running time of the algorithm depends on the following theorems.

Theorem 5.5.2 ([49,81]) *Suppose that there exist two positive constants c_1 and c_2 such that the number of primes p in the interval $[x;\ x+\sqrt{2\,x}]$ $(x \geq 2)$ is greater than $c_1\sqrt{x}\,(\log x)^{-c_2}$. Then* **GK** *proves the primality of n in expected time $O(\log^{10+c_2} n)$.*

Theorem 5.5.3 ([49,81]) *There exist two positive constants c_3 and c_4 such that for all $k \geq 2$, the set of prime numbers n of k bits for which the expected time of* **GK** *is bounded by $c_3 \log^{11} n$ is at least $1 - c_8\, 2^{-k^{\frac{1}{\log\log k}}}$.*

The problem with that algorithm is that Schoof's algorithm seems difficult to implement. The idea is then to use the properties of the elliptic curves over finite fields which have complex multiplication.

5.6 The ATK algorithm

In algorithm **GK**, we begin by searching for a curve and then its number of points. Here, we do exactly the contrary. We use the properties of the curves modulo a prime. We then modify step 1 of **GK** by:

procedure ATK(n);

1.
   1. choose a fundamental discriminant $-D$ (in practice D runs through 3, 4, 7, 8,...) such that n splits as $\pi\,\pi'$;
   2. for this π, compute the number of points $m = n+1-(\pi+\pi')$. If $m = k\,q$, with k greater than 2 and q a probable prime, go to 1.3, else go back to 1.1.
   3. compute an invariant j (root of $P_D(X)$ in $\mathbf{Z/nZ}$), then the associated curve E (Cf. the following chapter).

The other steps of the algorithm is unchanged.

We note that there are exactely $w(-D)$ elliptic curves with complex multipplication by $\mathcal{O}_K$, characterized by their number of points $f_D^{\pi}(n) = n+1-(\pi+\pi')$. To this function we associate the function $\mathcal{T}f_D^{\pi}$ described in chapter 2, section 2. The function $\mathcal{T}f_D$ is then the test that returns '?' if the $w(-D)$ functions $\mathcal{T}f_D^{\pi}$ return '?' and the answer of one of the $\mathcal{T}f_D^{\pi}$ else.

Part II

Implementation of Atkin's test

Chapter 6

Precomputations

6.1 Computation of the polynomials $P_D(X)$

We have seen that the j-invariants of the elliptic curve which have complex multiplication by $\mathcal{O}_D$, $-D$ a fundamental discriminant, are algebraic integers of degree $h(-D)$. The polynomial

$$P_D(X) = \prod_{r=1}^{h(-D)} (X - j_r), \tag{6.1}$$

is thus in $\mathbf{Z}[X]$. This polynomial, once reduced in $\mathbf{Z/pZ}$, yields the j-invariants of curves with complex multiplication over $\mathbf{Z/pZ}$. We have thus to compute those polynomials. As a matter of fact, they are precomputed and then stored in the program. The first thing to do is to compute j.

Several authors ([12,50,124]) have listed the values of j for all known values of D of class number 2 or 3, and for some other values. This could be used to compute the corresponding $P_D(X)$. This method cannot be applied to polynomials of higher degree and so we must look for a method that always works. It seems that the simplest way to do this is the following *Rambo* method: evaluate j with sufficiently many digits and then form $P_D(X)$.

6.1.1 The method

Let $-D$ be a fundamental discriminant. We begin by listing all primitive reduced quadratic forms of discriminant $-D$ using the procedure QFLIST (Cf. section 3.1.3). To each form $(a_r,\ b_r,\ c_r)$, we associate the complex numbers $\tau_r = \frac{-b_r + i\sqrt{D}}{2\,a_r}$ and $j_r = j(\tau_r)$.

Then, we make two classes of forms. In the first one, we put all forms (a, b, c) for which $(a, -b, c)$ is also reduced. The second is formed by the remaining forms. This is motivated by the fact that the values of j corresponding to the forms (a, b, c) and $(a, -b, c)$ are conjugate (in $\mathbf{C}$). This saves some time. After we have computed the $h(-D)$ values of j, we build $P_D(X)$.

We need a way to check our computations. This is done as follows. We first notice that $\mathcal{N} := P_D(0)$ is the norm of j_r in $\mathbf{Q}(j)$. It is possible to compute this quantity independently of $P_D(X)$. Let τ be a quadratic number satisfying $A\tau^2 + B\tau + C = 0$. We define $disc(\tau) = B^2 - 4AC$. Then:

Theorem 6.1.1 ([51,44]) *Let $-D_1$ and $-D_2$ be two different fundamental discriminants. We* *put:*

$$J(D_1,D_2)=\left(\prod_{\substack{[\tau_1],\,[\tau_2]\\ disc(\tau_i)=D_i}}(j(\tau_1)-j(\tau_2))\right)^{\frac{4}{w_1w_2}} \tag{6.2}$$

where the product is extended to all reduce forms of discriminants $-D_1$ and $-D_2$, and w_i is the number of units in $\mathbf{Q}(\sqrt{-D_i})$. If l is a prime number satisfying $\left(\frac{D_1D_2}{l}\right)\neq -1$, we introduce:

$$\epsilon(l)=\begin{cases}\left(\frac{D_1}{l}\right) & if\ (l,D_1)=1\\ \\ \left(\frac{D_2}{l}\right) & if\ (l,D_2)=1.\end{cases} \tag{6.3}$$

If $n=\prod l_i^{\alpha_i}$ with $\left(\frac{D_1D_2}{l_i}\right)\neq -1$ for all i, we extend ϵ by $\epsilon(n)=\prod\epsilon(l_i)^{\alpha_i}$. Then:

$$J(D_1,D_2)^2=\pm\prod_{\substack{x^2\ <\ D_1D_2\\ x^2\ \equiv D_1D_2\ \mathrm{mod}4}} F\left(\frac{D_1D_2-x^2}{4}\right) \tag{6.4}$$

where

$$F(m)=\prod_{\substack{nn'=m\\ n,n'>0}} n^{\epsilon(n')}. \tag{6.5}$$

As a particular case

Corollary 6.1.1

$$J(D,-3)^2=(\mathcal{N})^{\frac{2}{3}}. \tag{6.6}$$

This formula shows that $\mathcal{N}^{\frac{2}{3}}$ and therefore $\mathcal{N}$ are always rational integers.

We now now some details of the actual computation.

6.1.2 Numerical evaluation of $j(\tau)$

Choice of a formula for j

We can use several formulas of j as q-expansion, where $q=e^{2i\pi\tau}$. The first task is to find one that is well suited for the computations.

The first idea was to compute separetely $E_4(q)$ and $E_6(q)$, then $j(q)=1728\frac{E_4(q)^3}{E_4(q)^3-E_6(q)^2}$. This was bad, since these two terms are very small (Cf. below) and this caused some error in evaluating $E_4(q)^3-E_6(q)^2$. The second solution tried to use:

$$E_4(q)^3-E_6(q)^2=q\prod_{n\geq 1}(1-q^n)^{24}=\sum_{n\geq 1}\tau(n)q^n, \tag{6.7}$$

given by Ramanujan. D. H. Lehmer computed $\tau(n)$ for $n\leq 300$ ([76]) and it would have been possible to use these tables. I did not use this idea, since there is a nice q-expansion of j. We saw that:

$$j(q)=\frac{1}{q}+744+\sum_{n\geq 1}c_n\,q^n, \tag{6.8}$$

where all the c_n are positive integers. The computation of these coefficients began with [138]. It had been extended to $n = 100$ in [122], using some relations of the c_n with the partition function (5.41). Herrmann has announced ([60]) that he had computed the 6002 first values of c_n. These values are unfortunately not given. Finally, Mahler has given explicit recurence formulas for these coefficients (see [83]).

It would have been tedious to type all these data. So I used MAPLE to compute the q-expansion of E_4 and E_6, and then deduce from them the q-expansion of j using the *Taylor* function of this package. The only thing to do was then to verify the properties (5.2.7) before storing them in a program. This is a very fast computation and the results coincide with that of [122].

Remark concerning the computation of $\sigma_r(n)$
All integers for which we have to compute $\sigma_r(n)$ are small ($n \leq 500$). I thus used a very straightforward algorithm that is very fast for this range.

function SIGMA(n, r);

1. $s := 0$;
2. **for** $d = 1..\lfloor\sqrt{n}\rfloor$:
    1. **if** $d \mid n$ **then**
        1. **if** $d^2 = n$ **then** $s := s + d^r$; **else** $s := s + d^r + (\frac{n}{d})^r$;
3. SIGMA:=s;
4. **end.**

Computation of $j(\tau)$

We have to evaluate j for values of τ of the form $\tau = \frac{-b+i\sqrt{D}}{2a}$, where $(a,\ b,\ \frac{b^2+D}{4a})$ is a primitive reduced form of discriminant $-D$. We put $q = \rho e^{-i\theta}$, with $\rho = e^{-\frac{\pi\sqrt{D}}{a}}$ and $\theta = \pi\,\frac{b}{a}$. Since this form is reduced: $a \leq \sqrt{\frac{D}{3}}$. We deduce: $\rho \leq e^{-\pi\sqrt{3}} < 4.34 \times 10^{-3}$. Hence, the series giving $j(\tau)$ converges very quickly. The evaluation of j is carried out separetely for the real part and the imaginary part.

We may remark that the leading term of j is $\frac{1}{q} + c_0$. Thus:

$$\log|j| \simeq \frac{\pi\sqrt{D}}{a}. \tag{6.9}$$

It is possible to estimate the error made in truncating the series for j. Let N be a positive integer. We want to get an upper bound for:

$$\Delta_N(q) = \sum_{n>N} c_n\, q^n.$$

By theorem (5.2.4), there exists a constant $C_1 > 1$ such that:

$$\forall\ n \geq 1,\ |c_n| \leq \frac{C_1}{\sqrt{2}}\,\frac{e^{4\pi\sqrt{n}}}{n^{\frac{3}{4}}}.$$

Then:

$$|\Delta_N(q)| \leq \sum_{n>N} \rho^n \frac{C_1}{\sqrt{2}} \frac{e^{4\pi\sqrt{n}}}{n^{\frac{3}{4}}}.$$

We write:

$$u_n = \rho^n \frac{e^{4\pi\sqrt{n}}}{n^{\frac{3}{4}}}$$

Hence:

$$\log u_n \leq \frac{n\pi\sqrt{D}}{a} \left(-1 + \frac{4a}{\sqrt{n\,D}}\right).$$

Since $a \leq \sqrt{\frac{D}{3}}$, we deduce:

$$\log u_n \leq -n \log R_N,$$

with:

$$\log R_N = \frac{\pi\sqrt{D}}{a} \left(1 - \frac{4}{\sqrt{3N}}\right).$$

We find:

$$|\Delta_N(q)| \leq \frac{C_1}{\sqrt{2}} \frac{1}{R_N^N} \frac{1}{R_N - 1}. \tag{6.10}$$

6.1.3 Computation of $P_D(X)$

We have just seen that $\log|j| \approx \frac{\pi\sqrt{D}}{a}$. The number of digits of $j(q)$ is asymptotically $\frac{\pi}{\log 10}\frac{\sqrt{D}}{a}$. We have to compute the coefficients of $P_D(X)$ to within 0.5 and in particular the product $\prod j_r$. The precision required is thus:

$$\frac{\pi\sqrt{D}}{\log 10} \sum \frac{1}{a} + \nu_0, \tag{6.11}$$

where the sum is taken over all primitive reduced forms of discriminant $-D$, and ν_0 a positive constant that takes care of the error made in our estimation of $\log|j|$. We then form all products of the form $X - j$, regrouping terms of the type $(X - j)$ and $(X - \bar{j})$ to get:

$$(X - j)(X - \bar{j}) = X^2 - (j + \bar{j})X + j\bar{j},$$

which reduces error computations.

We check the result with (6.6). If we find that $P_D(0)$ is the cube of an integer to within 0.5, we are confident that the computed polynomial is indeed the one we were looking for. I have computed all polynomials $P_D(X)$ corresponding to all known values of D for which $h(-D)$ is less than 10. This makes 454 polynomials ([22]). These computations were done using MAPLE ([29]) on a GOULD/NP1. It took roughly 10 hours of CPU time.

The coefficients of these polynomials are huge (sometimes more than 200 digits). It is sometimes possible to get smaller coefficients, as explained in the next paragraph.

Compacting data

We can reduce the amount of storage needed by our $P_D(X)$ using the following result.

Theorem 6.1.2 ([125,111]) *Let τ be a quadratic number defined by $A\tau^2 + B\tau + C = 0$ and satisfying (5.52). Then, if $3|B$, $3 \not| A$, $3 \not| B^2 - 4AC$, we have:*

$$\mathbf{Q}(\gamma_2(\tau)) = \mathbf{Q}(j(\tau)). \tag{6.12}$$

Conversely, let $-D$ be a fundamental discriminant not divisible by 3. It is always possible to find a form (A, B, C) that satisfies the preceding conditions. For instance, we may take:

$$\begin{cases} \left(1, 3, \dfrac{D+9}{4}\right) & \text{if } \mathrm{D} \equiv 3 \bmod 4, \\ \\ \left(1, 6, \dfrac{D+36}{4}\right) & \text{if } \mathrm{D} \equiv 0 \bmod 4. \end{cases} \tag{6.13}$$

The corresponding reduced form yields the same value of j (Cf. section 5.2.5).

The minimum polynomial of γ_2, noted $P_D^{\frac{1}{3}}(X)$, is of degree $h(-D)$ and its coefficients are smaller than those of the original $P_D(X)$. This saves some space. From a practical point of view, $P_D^{\frac{1}{3}}(X)$ is computed as follows:

procedure MINGAMMA;

1. $R(Y) := P_D(Y^3)$;
2. factor $R(Y)$ in $\mathbf{Q}$;
3. write: $R(Y) = R_1(Y)R_2(Y)$, where R_1 and R_2 are irreducible polynomials, of respective degree $h(-D)$ and $2h(-D)$;
4. $P_D^{\frac{1}{3}}(X)$ is precisely $R_1(X)$.
5. **end.**

For example, for $D = 23$, we find:

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

$$P_{23}^{\frac{1}{3}}(X) = X^3 + 155X^2 + 650X + 23375.$$

Factoring these polynomials P_D or $P_D^{\frac{1}{3}}$ over $\mathbf{Z/pZ}$ is very expensive. We shall see in next chapter how this computation can be avoided in the case where D is an Euler number.

6.2 Computation of the invariants of the Euler numbers

6.2.1 Summary of the results

If $-D = \prod_{i=1}^{t} q_i^*$ is an Euler number, all quadratic forms of discriminant $-D$ are ambiguous, since the square of a class C is in the genus G_1, which only contains the principal form.

Lemma 6.2.1 *Let $Q = (a, b, c)$ be an amibguous form and let $\tau = \frac{-b+i\sqrt{D}}{2a}$. Then:*

$$j(\tau) \in \mathbf{R}. \tag{6.14}$$

Proof. We know that an ambiguous form can be of three types. In the case where Q is of the shape $(a, 0, c)$ or (a, a, c), the number $q = e^{2i\pi\tau}$ is real and it follows that $j(\tau)$ is also real.

When $Q = (a, b, a)$, we see that $|\tau| = 1$. On the other hand, we know that $j(\tau) = j(\frac{1}{\tau})$ (j is a modular function). We deduce that:

$$j(\tau) = j(\overline{\tau})$$

and this is precisely $\overline{j(\tau)}$, which can be seen by looking at G_{2k}. Therefore: $j(\tau) \in \mathbf{R}$. ■

We know that the genus field $\mathbf{K}_{\mathrm{g}} = \mathbf{Q}(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*})$ coincides with the class field $\mathbf{K}_{\mathrm{H}}$. Let C be any class of $\mathcal{H}(-D)$ and σ_C its image by the Artin isomorphism. We have:

$$\forall C,\ \forall s,\ \sigma_C(j(C_s)) = j(C^{-1}C_s) = j(CC_s), \tag{6.15}$$

since all forms are ambiguous. On the other hand (Cf. section 4.2.2) the isomorphism σ_C is the Artin symbol of $\mathbf{K}_{\mathrm{H}}|\mathbf{K}$ and:

$$\sigma_C(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*}) = (\chi_1(C)\sqrt{q_1^*}, \ldots, \chi_t(C)\sqrt{q_t^*}). \tag{6.16}$$

Since all forms are ambiguous, all j are reals, by the lemma. Hence, the values of j are contained in the largest real subfield of $\mathbf{K}_{\mathrm{g}}$. If the first l prime factors of D are congruent to 1 modulo 4 and the others to 3, then the j's are in:

$$\mathbf{K}_{\mathrm{rg}} = \mathbf{Q}(\sqrt{q_1}, \ldots, \sqrt{q_l}, \sqrt{q_{l+1}q_{l+2}}, \ldots, \sqrt{q_{l+1}q_t}). \tag{6.17}$$

Since we have determined the field of definition of the j's, we can now describe some methods used to compute the exact expression for j. Do not forget that we have computed all the polynomials $P_D(X)$. As soon as we have computed a formula for j, we can check it by direct evaluation.

6.2.2 Weber's formula

Let $-D$ be an Euler number divisible by 4. Letting $m = \frac{D}{4}$, the principal form is $(1, 0, m)$ and the corresponding value of τ is $i\sqrt{m}$. Weber has proved the following formulas (Cf. [125, III-§143] and [126]):

Theorem 6.2.1 *There are two cases:*

1. *if m is odd then:*

$$\left(\frac{f(i\sqrt{m})}{2^{\frac{1}{4}}}\right)^{2h(-D)} = \prod \eta^{H(\delta)H(\delta')}, \tag{6.18}$$

where the product is taken over all the decompositions of D as $-D = \delta\delta'$ with $\delta \equiv 5 \bmod 8$ (δ positive or not). The function H is defined by:

$$H(\delta) = \begin{cases} \dfrac{2}{w(\delta)} & h(\delta) \quad \text{if } \delta < 0, \\ 2 & h(\delta) \quad \text{otherwise,} \end{cases} \tag{6.19}$$

For each factorization $-D = \delta\delta'$, one among δ and δ' is positive and then η is a fundamental unit of the corresponding real quadratic field.

2. *if m is even, then:*

$$\left(\frac{f_1(i\sqrt{m})}{2^{\frac{1}{4}}}\right)^{2h(-D)} = \prod \eta^{H(\delta)H(\delta')}, \tag{6.20}$$

with the same notations.

Example

Let $D = 840 = 8 \times 105$ that satisfies $h(-D) = 8$. With the help of the tables given in [15] and [63], we find:

δ	δ'	$H(\delta)$	$H(\delta')$	η
-3	280	$\frac{1}{3}$	4	$251 + 30\sqrt{70} = (5\sqrt{5} + 3\sqrt{14})^2$ †
5	-168	2	4	$\dfrac{1+\sqrt{5}}{2}$
21	-40	2	2	$\dfrac{5+\sqrt{21}}{2} = \dfrac{(\sqrt{3}+\sqrt{7})^2}{4}$
-35	24	2	2	$5 + 2\sqrt{6} = (\sqrt{2} + \sqrt{3})^2$

We deduce:

$$2^{18} f_1^{24} = (5\sqrt{5} + 3\sqrt{14})^4 (1 + \sqrt{5})^{12} (\sqrt{3} + \sqrt{7})^{12} (\sqrt{2} + \sqrt{3})^{12}.$$

We then plug that result in MAPLE to get:

$$\begin{array}{rrl} j = & 436810980663310134386664450093663086400 & \\ + & 195347809216301527540490053498198986240 & \sqrt{5} \\ + & 178327336111639887169359664860260102400 & \sqrt{6} \\ + & 79750409158415962769096479496235724800 & \sqrt{30} \\ + & 116742645173060259939233851836971520000 & \sqrt{14} \\ + & 52208898096020088304326516705167788800 & \sqrt{70} \\ + & 47659985316131200714081618743535430400 & \sqrt{84} \\ + & 21314193394702233808587585180348748800 & \sqrt{420}. \end{array}$$

Weber gives numerous examples of computation of j in [125, Tabelle VI].

† And not $(5\sqrt{5} + \sqrt{14})^2$ as indicated in [125, Tabelle VI].

6.2.3 A complementary method

This method was explained to me by D. Bernardi. We describe it on an example.

Let us consider the case $D = 1155$. We write: $-D = (5) \times (-3) \times (-7) \times (-11)$. The field containing j is then $\mathbf{K}_{\mathrm{rg}} = \mathbf{Q}(\sqrt{5}, \sqrt{21}, \sqrt{33})$.

To each form $C_r = (a_r, b_r, c_r)$ we associate $\tau_r = \frac{-b_r + i\sqrt{D}}{2a_r}$ and $j_r = j(\tau_r)$, and the Artin symbol $\sigma_r = \sigma_{C_r}$. We know that:

$$\sigma_r(\sqrt{q_1^*}, \ldots, \sqrt{q_t^*}) = (\chi_1(C_r)\sqrt{q_1^*}, \ldots, \chi_t(C_r)\sqrt{q_t^*}).$$

We evaluate $\chi_s(C_r)$ by the computation of $\left(\frac{q_s^*}{p}\right)$ where p is any prime number represented by C_r ($p \not| D$).

In the following table, we have listed all forms of discriminant -1155. For each of these, we have found a small prime p ($p \not| D$) represented by it and the values of the Jacobi symbol $\left(\frac{q^*}{p}\right)$, where q is a divisor of D. We have just indicated the signs of the symbols.

	a	b	$c = p$	$\left(\frac{-3}{p}\right)$	$\left(\frac{5}{p}\right)$	$\left(\frac{-7}{p}\right)$	$\left(\frac{-11}{p}\right)$
C_1	1	1	289	$+$	$+$	$+$	$+$
C_2	17	1	17	$-$	$-$	$-$	$-$
C_3	3	3	97	$+$	$-$	$-$	$+$
C_4	5	5	59	$-$	$+$	$-$	$+$
C_5	7	7	43	$+$	$-$	$+$	$-$
C_6	11	11	29	$-$	$+$	$+$	$-$
C_7	15	15	23	$-$	$-$	$+$	$+$
C_8	19	17	19	$+$	$+$	$-$	$-$

Let us decide that j_1 is written:

$$\begin{aligned} j_1 &= a + b\sqrt{5} + c\sqrt{-3 \times -7} + d\sqrt{-3 \times -11} + e\sqrt{-7 \times -11} \\ &\quad + f\sqrt{5 \times -3 \times -7} + g\sqrt{5 \times -3 \times -11} + h\sqrt{5 \times -7 \times -11}, \end{aligned}$$

with a, b, c, d, e, f, g, h in $\mathbf{Q}$.

Let us now consider the action of σ_2 on the j's. By theorem (6.15):

$$\forall s, \sigma_2(j(C_s)) = j(C_2^{-1}C_s) = j(C_2 C_s),$$

(C_2 is ambiguous). In particular: $\sigma_2(j_1) = j_2$. Therefore, j_2 may be written as:

$$\begin{aligned} j_2 = \sigma_2(j_1) = \; & a + b\,\sigma_2(\sqrt{5}) + c\,\sigma_2(\sqrt{-3})\,\sigma_2(\sqrt{-7}) \\ & + d\,\sigma_2(\sqrt{-3})\,\sigma_2(\sqrt{-11}) + e\,\sigma_2(\sqrt{-7})\,\sigma_2(\sqrt{-11}) \\ & + f\,\sigma_2(\sqrt{5})\,\sigma_2(\sqrt{-3})\,\sigma_2(\sqrt{-7}) + g\,\sigma_2(\sqrt{5})\,\sigma_2(\sqrt{-3})\,\sigma_2(\sqrt{-11}) \\ & + h\,\sigma_2(\sqrt{5})\,\sigma_2(\sqrt{-7})\,\sigma_2(\sqrt{-11}). \end{aligned}$$

Using the preceding table, we get:

$$j_2 = a - b\sqrt{5} - c\sqrt{21} + d\sqrt{33} - e\sqrt{77} + f\sqrt{105} - g\sqrt{165} + h\sqrt{385}.$$

We do the same with the six other forms and we obtain:

$$\begin{pmatrix} j_1 \\ j_2 \\ j_3 \\ j_4 \\ j_5 \\ j_6 \\ j_7 \\ j_8 \end{pmatrix} = \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & + & + & + & - & - & - \\ + & - & - & + & - & + & - & + \\ + & + & + & - & - & + & - & - \\ + & - & + & - & - & - & + & + \\ + & + & - & + & - & - & + & - \\ + & - & - & - & + & + & + & - \\ + & + & - & - & + & - & - & + \end{pmatrix} \begin{pmatrix} a \\ b\sqrt{5} \\ c\sqrt{21} \\ d\sqrt{33} \\ e\sqrt{77} \\ f\sqrt{105} \\ g\sqrt{165} \\ h\sqrt{385} \end{pmatrix}.$$

We have just written the signs of the coefficients of the matrix, since they are ± 1. In order to find the coefficients a, b, c, d, e, f, g et h, we have to invert that matrix. We do that with MAPLE and we get:

$$\begin{pmatrix} a \\ b\sqrt{5} \\ c\sqrt{21} \\ d\sqrt{33} \\ e\sqrt{77} \\ f\sqrt{105} \\ g\sqrt{165} \\ h\sqrt{385} \end{pmatrix} = \frac{1}{8} \begin{pmatrix} + & + & + & + & + & + & + & + \\ + & - & - & + & - & + & - & + \\ + & + & - & + & + & - & - & - \\ + & + & + & - & - & + & - & - \\ + & + & - & - & - & - & + & + \\ + & - & + & + & - & - & + & - \\ + & - & - & - & + & + & + & - \\ + & - & + & - & + & - & - & + \end{pmatrix} \begin{pmatrix} j_1 \\ j_2 \\ j_3 \\ j_4 \\ j_5 \\ j_6 \\ j_7 \\ j_8 \end{pmatrix}.$$

We then replace the j_s by their numerical value, as indicated in the above table:

s	j_s
1	$-23373692778731029019776599932265891844886003843.88$
2	1706.63
3	-2859186231495065.55
4	-1878214955.10
5	-4207529.03
6	-15686.61
7	-635.72
8	9.27

We deduce:

$$\begin{aligned} a &= -2921711597341378627472074991533593879124992000 \\ b &= -1306629148460963287630585767202654373354618880 \\ c &= -637569740649866931007417559855913439057920000 \\ d &= -508604706243764883294133415277319212624076800 \\ e &= -332959937881833102714456353625205560476467200 \\ f &= -285129856098002680171205468160808422359654400 \\ g &= -227454939367474000635400441674356512822886400 \\ h &= -148904210977577231461745263391546913552998400 \end{aligned}$$

6.2.4 How not to use the two preceding sections

Before using the machine guns described in the last two sections, it is worthwhile to make some remarks. We have to solve equations of degree 2^t by means of square roots.

When $t=0$, it is obvious. If $t=1$, we must solve equations of degree 2 and this is easy too. In the case $t=2$, we know that the equations are solvable by radicals, no matter where they come from. Using MAPLE and the function *solve* on the first example corresponding to $D=84$, I found the following results:

```
    |\^/|
._|\|   |/|_. INRIA - Rocquencourt
 \  MAPLE  /  Version 4.2 --- Dec 1987
 <____ ____>  For on-line help, type  help();
      |

> p84;
 4                  3                        2
x   - 3196800946944 x   - 5663679223085309952 x   + 88821246589810089394176 x

   - 5133201653210986057826304

# find first approximations of the roots with 30 digits
> Digits:=30:
> fsolve(p84);
-1787216.60124765701986744310183, 58.0070617294852765340555935901,

   15488.6808931242445922671434083, 3196802718613.91329280328999865

> solve(p84);
                            1/2
799200236736 + 302069634048 7

                1/2             1/2             1/2
               3    (142197407 7    + 376218976)
   + 54722304 --------------------------------------
                                1/4
                               7

# floating point approximation
> j:=":
> evalf(j);
                3196802718613.91329280328999865
```

We next simplify this expression by recognizing that:

$$142197407\sqrt{7}+376218976=\sqrt{7}(142197407+376218976\sqrt{7})=\sqrt{7}(8432+3187\sqrt{7})^2$$

and we find:

$$\begin{aligned} j &= 799200236736+302069634048\sqrt{7}+54722304\sqrt{3}(8432+3187\sqrt{7}) \\ &= 799200236736+302069634048\sqrt{7}+461418467328\sqrt{3}+174399982848\sqrt{21}. \end{aligned}$$

The floating point value is:

$$3196802718613.91329280328999865,$$

which is the correct value.

This case can thus be dealt with without complicated methods.

The case $t = 3$ and $4 \mid D$ is treated by Weber's formulas. Eventually, we are left with four odd values of D for which we must use the second method.

The last discriminant, $D = 5460$ and $t = 4$, is divisible by 4, and therefore we use Weber's formulas.

6.2.5 Utilisation in Atkin's test

We succeeded in calculating an expression of j in the field $\mathbf{K}_{\mathrm{rg}}$. This expression is a linear combination of square roots with coefficients in $\mathbf{Q}$ (as a matter of fact in $\mathbf{Z}$ except in the case $D = 15$, where we get some denominator $\frac{1}{2}$).

The computation of j in $\mathbf{Z}/\mathbf{pZ}$ is done by replacing the computation of square roots in $\mathbf{R}$ by the computation of square roots modulo p (these roots are of the form $\sqrt{q_s^*} \bmod p$ and we do know that $\left(\frac{q_s^*}{p}\right) = +1$, by the choice of a quadratic form of discriminant $-D$ to represent p).

The algorithm we use to find these roots is faster than Berlekamp's algorithm used to find a root of $P_D(X)$ modulo p.

Chapter 7

Practical considerations

7.1 Selecting D

Let n be the number tested for primality. The first part of the algorithm consists in choosing a fundamental discriminant $-D$ such that n splits in $\mathbf{K}= \mathbf{Q}(\sqrt{-D})$ as a product of two distincts principal ideals. We look for D in increasing order of $h(-D)$, first among Euler numbers, and then among the others.

We write $-D = q_1^* \dots q_t^*$ and the first thing to verify is:

$$\left(\frac{-D}{n}\right) = 1.$$

If this is the case, then we test if n can be represented by a form in the principal genus. That is to say, we verify that:

$$\forall\ i > 1, \left(\frac{q_i^*}{n}\right) = \left(\frac{n}{q_i}\right) = +1.$$

We do not compute $\left(\frac{q_1^*}{n}\right)$ since:

$$\left(\frac{q_1^*}{n}\right) = \left(\frac{-D}{n}\right) \prod_{i=2}^{t} \left(\frac{n}{q_i}\right).$$

This is done to avoid the case where $4 \mid q_1$.

If n satisfies all these conditions, we compute the form in the principal genus that represents n. We use procedure RED when D is odd and the procedure CORNACCHIA in the other case.

7.2 Looking for m

7.2.1 Possible values

We know that there are $w(-D)$ possible values for m. If n splits as $\varpi\ \varpi'$ in $\mathbf{K}$, the associated number of points is $m = n + 1 - (\varpi + \varpi')$. Starting with this decomposition of n, we find the others in the following table.

D	$w(-D)$	possible decompositions
3	6	$(\pm\varpi)(\pm\varpi')$, $(\pm\rho\varpi)(\pm\rho^2\varpi')$, $(\pm\rho^2\varpi)(\pm\rho\varpi')$
4	4	$(\pm\varpi)(\pm\varpi')$, $(\pm i\varpi)(\pm i\varpi')$
≥ 7	2	$(\pm\varpi)(\pm\varpi')$

with $\rho = e^{\frac{2i\pi}{3}}$ and $i^2 = 1$.

7.2.2 Factorization of $m = (\pi - 1)(\pi' - 1)$

We remark that $m = N_K(\pi - 1)$. Since this the norm of an integer of $\mathcal{O}_{-D}$, we have the following property. If l is a prime divisor of m, then, following (4.1.3): $l \mid D$ or $\left(\frac{-D}{l}\right) = +1$. This gives us some information on the potential divisors of m.

Trial division

We begin by looking for small prime factors of m. Let $p_1, \ldots, p_k$ be all the prime numbers less than a given B. We suppose they are stored in a file. We want to know which of them divide m. In order to optimize the computation, we make the following remark. We begin by factoring $n \pm 1$, then some numbers of the form $n + 1 \pm t$. We build the following vector:

$$RES[i] := (n + 1) \bmod p_i, \text{for } i = 1..k.$$

Divisibility of $n \pm 1$ is tested as follows:

for $i = 1..k$

1. **if** $RES[i] = 0$ **then** $p_i \mid n + 1$;
2. **if** $RES[i] = 2$ **then** $p_i \mid n - 1$.

This idea was already used in [20, Section 7, Rem. 1] and [34]. We can generalize it in the case where we want to factor $m_{\pm} = n + 1 \pm t$, with $|t| \leq 2\sqrt{n}$.

for $i = 1..k$

1. $r := t \bmod p_i$;
2. **if** $r = RES[i]$ **then** $p_i \mid m_-$;
3. **if** $r + RES[i] = 0$ or p_i **then** $p_i \mid m_+$.

We replaced $2k$ divisions of numbers of size L with k divisions of integers of size $\frac{L}{2}$.

Looking for larger factors

The larger the numbers we test, the larger the factors we must find. The preceding method has the disadvantage of requiring a lot of memory. For instance, storing all prime numbers below $B = 10^6$ requires 170 kbytes. In order to find factors less than 10^7 or 10^8, we must use another method. It seems that the best one is Pollard's ρ method ([98,17]) for the size of factor we want to discover (Cf. the empirical study in [18]).

Choice of the parameters

A current strategy for a number with less than 300 digits is to find all factors less than $B = 10^4$ by trial divisions and then use 4000 iterations of ρ. Thus, we are sure to discover all factors of m less than 10^6 (Cf. [53]).

7.3 Computation of j

Let D be a discriminant. The computation of the associated value of j modulo n depends on $h(-D)$, the class number of $-D$.

7.3.1 D is an Euler number

$h = 1$

This is a nice case, because we just have to do one division.

$h \geq 2$

We have computed in section 6 an expression of j as a linear combination of square roots with integer coefficients (except for $D = 15$). These expressions are stored in the following format:

h	j	*list*
2	$a + b\sqrt{d_1}$	$(d_1\ a\ b)$
4	$a + b\sqrt{d_1} + c\sqrt{d_2} + d\sqrt{d_1 d_2}$	$(d_1\ d_2\ a\ b\ c\ d)$
8	$a + b\sqrt{d_1} + c\sqrt{d_2} + d\sqrt{d_3} + e\sqrt{d_1 d_2} + f\sqrt{d_1 d_3} + g\sqrt{d_2 d_3} + h\sqrt{d_1 d_2 d_3}$	$(d_1\ d_2\ d_3\ a\ b\ c\ e\ d\ f\ g\ h)$

This is done in order to have an algorithm which is as compact as possible. More precisely, we use the following procedure:

procedure EULER(n, h, $\mathcal{L}$)
  (* $h = 2^g$ is the class number and $\mathcal{L}$ the list of coefficients giving j *)

1. **for** $i = 1..g$ $r_i = \sqrt{next(\mathcal{L})} \bmod n$;
2. $j := next(\mathcal{L}) \bmod n$;
3. **for** $i = 1..h$
    1. $z := next(\mathcal{L}) \bmod n$;
    2. $i = \epsilon_0 \ldots \epsilon_{g-1}$, with $\epsilon_i \in \{0, 1\}$;
    3. **for** $u = 0..(g-1)$
        1. **if** $\epsilon_u = 1$ **then** $z := z * r_u \bmod n$;
    4. $j := j + z \bmod n$;
4. return(j).
5. **end**.

7.3.2 D is common

The coefficients of $P_D(X)$ are stored in a file. Since P_D is monic, we do not store the leading 1. Moreover the constant term is a cube and so we only store the cube root of that coefficient.

We find a root of P_D over $\mathbf{Z/NZ}$ using Berlekamp's algorithm ([11,67]). We use the *folk's method*, that is to say:

procedure BERLEKAMP($P(X)$, n);

1. $F(X) := 1$, $x_0 := 0$;
2. **while** degree($F(X)$)$\neq 0$
   1. $x_0 := x_0 + 1$;
   2. $F := \gcd((X + x_0)^{\frac{n-1}{2}} - 1, P(X)) \bmod n$;
   3. **if** degree($F(X)$)> 1 **then** $P := F$;
3. $F = X - j$;
4. **end**.

We know that $P_D(X) \bmod n$ has exactly $h(-D)$ roots in $\mathbf{Z/nZ}$, which is the favorable case of this algorithm. One can show that the probability of success for each x_0 is $\frac{1}{2}$ (one even conjectures that this probability is $\geq 1 - \frac{1}{2^h}$ Cf. [105]). The cost of this algorithm is ([105]):

$$O(h^2(\log n)^2).$$

7.4 Looking for an equation of E

We are looking for a Weierstrass equation for E of the type $y^2 = x^3 + ax + b$. With these notations,

$$\Delta = -16\,(4\,a^3 + 27\,b^2),$$

$$j = 2^8\,3^3\,\frac{a^3}{4\,a^3 + 27\,b^2}.$$

7.4.1 The cases $D = 3, 4$

The theorems we use below are taken from the excellent book by Ireland and Rosen [64]. In all that follows, p is a prime number that splits in $\mathbf{Q}(i)$ (resp. $\mathbf{Q}(\rho)$ and we want an equation of a curve E, defined over $\mathbf{F}_p$, that has complex multiplication by $\mathcal{O}_{-4}$ (resp. $\mathcal{O}_{-3}$).

D = 3

We know that the j-invariant of our curve is 0. Hence, we can look for an equation of E of the form:

$$y^2 \equiv x^3 + b \bmod p, \tag{7.1}$$

where b is a non zero element of $\mathbf{F}_p$. One shows ([16])that such a curve has complex multiplication by $\mathcal{O}_{-3} = \mathbf{Z}[\rho]$, where $\rho = e^{\frac{2i\pi}{3}}$.

By the assumption that p splits in $\mathbf{Z}[\rho]$, we have:

$$p = \pi\pi'. \tag{7.2}$$

Lemma 7.4.1 *There is a unique solution of $\omega\omega' = p$ which satisfies:*

$$\omega \equiv 2 \bmod 3. \tag{7.3}$$

This solution is called primitive.

Proof. We know that equation (7.2) has six solutions. Starting from the solution π, the five others are $\zeta\pi$ where ζ is any sixth root of unity, that is an element of $\{-1, \pm\rho, \pm\rho^2\}$. We write: $\zeta = r + s\rho$, with r and s in $\{-1, 0, 1\}$. But π nay be written $\pi = A + B\rho$, with $N_3(\pi) = A(A-B) + B^2 = p$. We are looking for $\omega = \zeta\pi$ such that $\omega \equiv 2 \bmod 3$. This is equivalent to:

$$(A + B\rho)(r + s\rho) \equiv 2 \bmod 3,$$

or:

$$\left\{\begin{array}{cccccl} A & r & - & B & s & \equiv 2 \bmod 3. \\ B & r & + & (A-B) & s & \equiv 0 \bmod 3. \end{array}\right.$$

We remark that A and B cannot br both divisible by 3. If both are not, the system has the solution:

$$\left\{\begin{array}{ccr} r & \equiv & 2(A-B) \bmod 3. \\ s & \equiv & B \bmod 3. \end{array}\right.$$

We may verify that these formulas yield also a solution in the case where 3 divides A or B. Conversely, these formulas give a solution to the initial problem.

Then:

Theorem 7.4.1 *Suppose that $p \not| b$. Then the number of points on the curve of equation (7.1) is:*

$$N = p + 1 + \overline{\left(\frac{4\,b}{\pi}\right)_6}\,\pi + \left(\frac{4\,b}{\pi}\right)_6\,\pi', \tag{7.4}$$

where π is defined by (7.2) and (7.3), and $(\frac{\cdot}{\pi})_6$ is the sextic residue:

$$\left(\frac{\alpha}{\pi}\right)_6 \equiv \alpha^{\frac{p-1}{6}} \bmod \pi. \tag{7.5}$$

Application to Atkin's test. We are in the case where $n \equiv 1 \bmod 3$. We have determined π in $\mathbf{Z}[\rho]$ such that $n = \pi\,\pi'$ and $m = (\pi - 1)(\pi' - 1)$ is B-nicely factored. We are looking for *one* equation of the curve of number of points m. We know that π has a unique associate $\omega = \zeta\pi$ such that $\omega \equiv 2 \bmod 3$. We compute ω with the help of lemma (7.4.1).

Determination of b. Since $n = \omega\,\omega'$, with ω primitive, the number of points on the curve is:

$$N = n + 1 + \overline{\left(\frac{4b}{\omega}\right)_6}\,\omega + \left(\frac{4b}{\omega}\right)_6\,\omega'.$$

We note that if π and ω are associate, then: $(\frac{\cdot}{\pi})_6 = (\frac{\cdot}{\omega})_6$. With $\mathcal{B} = (\frac{4b}{\omega})_6 \bmod n$, N may be written:

$$N = n + 1 + \overline{\mathcal{B}}\,\pi\,\zeta + \mathcal{B}\,\overline{\pi\,\zeta}.$$

We see that: $\mathcal{B} \equiv -\zeta \bmod \pi \Rightarrow N = n + 1 - \pi - \pi' = m$.

As a consequence, the curve $y^2 \equiv x^3 + b \bmod n$, with b satisfying $(4b)^{\frac{n-1}{6}} \equiv -\zeta \bmod \pi$ has m points.

The condition on $\mathcal{B}$ yields: $\mathcal{B} = -(r + s\rho) + (u + v\rho)(A + B\rho)$, with u and v in $\mathbf{Z}$. We deduce that:

$$(A - B)v + Bu = s, \tag{7.6}$$

$$\mathcal{B} = -r + Au - Bv. \tag{7.7}$$

We solve (7.6) by Bezout's algorithm. We plug the values of u and v in (7.7) and we find $\mathcal{B}$. By trial and error, we find a c such that $c^{\frac{n-1}{6}} \equiv \mathcal{B} \bmod n$. Eventually, we compute $b \equiv 4^{-1}\,c \bmod n$. We remark that

$$2x \equiv y \bmod n \quad \Leftrightarrow \quad x = \left\lfloor \frac{y}{2} \right\rfloor \bmod n \text{ if y is even}, \tag{7.8}$$

$$x = \left\lfloor \frac{y}{2} \right\rfloor + \frac{n+1}{2}, \text{ is y is odd}. \tag{7.9}$$

Example
Let $n = 103$. We find $\pi = 11 + 2\rho$, and successively:

$$\begin{aligned} \zeta &= -\rho, \\ \mathcal{B} &= 46, \\ 7^{\frac{103-1}{6}} &\equiv 46 \bmod 103, \\ b &= 79. \end{aligned}$$

The curve of equation $y^2 = x^3 + 79$ has $104 - 20 = 84$ points in $\mathbf{F}_{103}$.

D = 4.

The invariant is 1728. The curve E has the equation:

$$y^2 \equiv x^3 + ax \bmod p, \tag{7.10}$$

where a is a non zero element of $\mathbf{F}_p$. This curve has complex multiplication by $\mathcal{O}_4 = \mathbf{Z}[i]$. We know that

$$p = \pi\pi' \text{ in } \mathbf{Z}[i].$$

Lemma 7.4.2 *There is exactly one solution to the equation $\omega\omega' = p$ that satisfies:*

$$\omega \equiv 1 \bmod (2+2i). \tag{7.11}$$

This element ω is called primitive.

Proof. We start from $\pi\pi' = p$ and we are looking for a fourth root of unity ξ such that $\omega = \xi\pi \equiv 1 \bmod (2+2i)$. Since ξ is a unit in $\mathbf{Z}[i]$, we may write $\pi \equiv \xi^{-1} \bmod (2+2i)$. All we have to do is to compute a unit ζ such that $\pi \equiv \zeta \bmod (2+2i)$. We put $\pi = A + Bi$ and $\zeta = r + si$, with $rs = 0$ and r and s elements of $\{-1, 0, 1\}$. We want to determine α and β in $\mathbf{Z}$ such that

$$A + Bi = (r + si) + 2(1+i)(\alpha + i\beta). \tag{7.12}$$

This is equivalent to:

$$\begin{aligned} A &= r + 2(\alpha - \beta) \\ B &= s + 2(\alpha + \beta). \end{aligned} \tag{7.13}$$

This implies in particular:

$$A - B \equiv r - s \bmod 4. \tag{7.14}$$

We now prove that this equation characterizes the solutions. First, we have:

$$\pi\pi' = p \Longleftrightarrow A^2 + B^2 = p.$$

Hence A and B are of different parity. If A is even, we deduce that $r \equiv 0 \bmod 2$ and thus $r = 0$. Since B is odd, $A - B$ is also odd and the equation $s \equiv A - B$ characterizes s. We then check that the system (7.13) has rational integer solutions α and β. If B is even, we do the same work. It is then easy to compute $\xi = \zeta^{-1}$. ■

We have then the following result:

Theorem 7.4.2 *If $p \not| a$, then the number of points on the curve (7.10) is:*

$$N = p + 1 - \overline{\left(\frac{-a}{\pi}\right)_4}\pi - \left(\frac{-a}{\pi}\right)_4 \pi', \tag{7.15}$$

where π satisfies (7.11), and:

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{p-1}{4}} \bmod \pi. \tag{7.16}$$

Application to Atkin's test. We are in the case $n \equiv 1 \bmod 4$. We have computed an element π such that $n = \pi\,\pi'$, and $m = (\pi - 1)(\pi' - 1)$ is B-nicely factored. We want *one* equation of the curve having m points. We know that π has a unique associate ω such that $\omega \equiv 1 \bmod (2 + 2\,i)$. We write $\pi = \zeta\omega$, with ζ computed as in lemma (7.4.2).

Determination of a. We have seen that if $n \equiv 1 \bmod 4$, n prime, n may be written as $\omega\,\omega'$, with ω primitive, and:

$$N = n + 1 - \overline{\left(\frac{-a}{\omega}\right)_4}\,\omega - \left(\frac{-a}{\omega}\right)_4\,\omega'. \tag{7.17}$$

We remark that if π and ω are associates, then: $(\frac{\div}{\pi})_4 = (\frac{\div}{\omega})_4$. We put $\omega = \pi\zeta$ and $\mathcal{A} = (\frac{-a}{\omega})_4 \bmod n$. We deduce that the number of points on the elliptic curve of equation $y^2 \equiv x^3 + ax \bmod n$ is:

$$N = n + 1 - \overline{\mathcal{A}}\,\pi\,\zeta^{-1} - \mathcal{A}\,\overline{\pi\,\zeta^{-1}}.$$

We then see that: $\mathcal{A} \equiv \zeta \bmod \pi \Rightarrow N = n + 1 - \pi - \pi' = m$.

As a conclusion, the curve $y^2 \equiv x^3 + ax \bmod n$, with a satisfying $(-a)^{\frac{n-1}{4}} \equiv \zeta \bmod \pi$ has its number of points equal to m.

The condition on $\mathcal{A}$ may be written in the form $\mathcal{A} - (r - is) = (u + iv)(A + iB)$, with u and v in $\mathbf{Z}$. We deduce that

$$Av + Bu = s, \tag{7.18}$$

$$\mathcal{A} = r + Au - Bv. \tag{7.19}$$

The equation (7.18) may be solved using Bezout's algorithm. Plugging the values of u and v in (7.19), we can compute $\mathcal{A}$. Then, we search for a value of a such that $(-a)^{\frac{n-1}{4}} \equiv \mathcal{A} \bmod n$. This is done by trial and error.

Example

Let $n = 101$. We find $\pi = 10 - i$. Then:

$$\begin{aligned}\zeta &= i,\\ \mathcal{A} &= 91,\\ (-2)^{\frac{101-1}{4}} &\equiv 91 \bmod 101,\\ a &= 2.\end{aligned}$$

The curve of equation $y^2 = x^3 + 2x$ has $102 - 20 = 82$ points in $\mathbf{F}_{101}$.

7.4.2 $D \geq 7$

Given j_0 in $\mathbf{Z/nZ}$, we put $k = \frac{j_0}{1728 - j_0}$. If c is any non zero element of $\mathbf{Z/nZ}$, then the j-invariant of the curve:

$$y^2 = x^3 + 3kc^2x + 2kc^3 \tag{7.20}$$

is precisely j_0.

When $D \geq 7$, we know that there are only two classes of curve having the same invariant j_0, which is any root of $P_D(X) \equiv 0 \bmod n$. Their equations are:

$$E \;:\; y^2 = x^3 + 3kx + 2k, \tag{7.21}$$

or

$$E' \;:\; y^2 = x^3 + 3kc^2x + 2kc^3, \tag{7.22}$$

where c is a quadratic non residu modulo n. We remark that E and E' are not isomorphic, since they do not satisfy (5.1.1).

Their respective number of points are $m = n + 1 - \pi - \pi'$ and $m' = n + 1 + \pi + \pi'$. Since we do not know which point corresponds to which equation, we use the following algorithm. We first choose a point on the first curve and compute mP. If we find O_E, then we have the right equation, providing that the actual order of P is not too small (more precisely, we must verify that $gP \neq O_E$, where $g = \gcd(m, m')$). Otherwise we choose a non residu c and try to compute mP' on E'. Then, we can check the conditions of the theorem.

7.5 Computing on elliptic curves

7.5.1 Choosing a point on a curve

Suppose E is given by the equation:

$$y^2 = x^3 + ax + b \bmod n. \tag{7.23}$$

We select a point on E as follows. We start from a value x_0 and we increment it until the Jacobi symbol $\left(\frac{x^3+ax+b}{n}\right)$ is equal to $+1$. We then extract a square root of this expression with the algorithm of [2].

7.5.2 Formulas for the group law

The formulas of addition on the curve E of equation

$$y^2 = x^3 + ax + b, \tag{7.24}$$

are easily derived from the expressions (5.11) and (5.12). We find that the coordinates $(x_3 : y_3 : z_3)$ of the sum $M_3 = M_1 + M_2$, starting with $M_1 = (x_1 : y_1 : 1)$ and $M_2 = (x_2 : y_2 : 1)$ are:

$$x_3 = \lambda^2 - x_1 - x_2, \tag{7.25}$$

$$y_3 = \lambda(x_1 - x_3) - y_1, \tag{7.26}$$

with:

$$\lambda = (y_2 - y_1)(x_2 - x_1)^{-1}, \text{ if } x_2 \neq x_1, \tag{7.27}$$

$$\lambda = (3x_1^2 + a)(2y_1)^{-1}, \text{ otherwise.} \tag{7.28}$$

Then kM is computed using the well-known binary method (Cf. [67]). Alternatively, one can use addition-subtraction chains ([87]).

7.6 Primality proof for n

We now explain the use of the theorem (5.5.1). The idea is to look for a point whose order is greater than $(n^{\frac{1}{4}} + 1)^2$.

We consider the number of points written $m = kq$, with q pprime. There are two cases according to whether $q > (n^{\frac{1}{4}} + 1)^2$ or not. In the first case, we look for a point P on E and compute $Q = kP$. If $Q = O_E$, we choose another P. Else, we compute qQ. If we do not get O_E, n is composite, else it is prime, because we found a point of order q.

In the second case, we look for P on E and we compute its order on the curve. If this order be greater than $(n^{\frac{1}{4}} + 1)^2$, we win, else we look for another P.

There are some cases for which we cannot reach a conclusion. For instance if $m = M^2$ is a perfect square and E is isomorphic to $\mathbf{Z/MZ} \times \mathbf{Z/MZ}$.

7.7 Schemes for the program ATK

7.7.1 First idea

We introduced in chapter 2 the set $\mathcal{F}$. We now define:

$$\begin{aligned}\mathcal{D} &= \{-1,1\} \cup \{D \mid -D \text{ fundamental discriminant}\}\\ &= \{-1,1,3,4,7,8,\ldots\}\end{aligned}$$

and:

$$\begin{aligned} next_{\mathcal{D}}: \mathbf{Z} &\longrightarrow \mathcal{D}\\ x &\longmapsto Min\{D \in \mathcal{D} \mid D > x\}.\end{aligned}$$

We then redefine $\mathcal{F}$ by

$$\mathcal{F} = \{f_D \mid D \in \mathcal{D}\}.$$

We can now describe the procedure PRIME that test whether an integer n is prime.

function PRIME(n):boolean;

1. $i := 0$; $l := \lfloor log_2 n \rfloor$; $n_0 := n$;

2.**for** $s := 0..l$
 $\mid D_s := -2$;

3. **while** $n_i > B^2$
   - $D_i := next_{\mathcal{D}}(D_i)$;
   - **while** $\mathcal{T}f_{D_i}(n_i) = ?$
     $\mid D_i := next_{\mathcal{D}}(D_i)$;
   - **if** $\mathcal{T}f_{D_i}(n_i) = TRUE$
     then
       $n_{i+1} := R(f_{D_i}(n_i), B)$;
       $i := i + 1$;
     else
       if $i = 0$
         then go to 4;
         else $i := i - 1$;

4. PRIME $:= \mathcal{T}f_{D_0}(n)$;

5. **end**.

This is the easiest way to program this algorithm.

7.7.2 A two-phases algorithm

Let us give a close look at function PRIME. At each step i, we look for a well suited test, then we check the conditions of the associated theorem. When we use an elliptic-curve test, this implies the computation of a root of a polynomial whose degree can be high. It may happen that during step $(i+1)$, we cannot find a test for n_{i+1}. This is because we have only a finite number of curves in our data base. It is not rare that all numbers of points we have to compute have simultaneously large prime factors. So we have to backtrack in our algorithm and thus we have lost all the computation time of step i.

This explains why we divide our program in two phases. The first one consists in finding all number of points that B-nice factored and the second one checks all the theorems.

Chapter 8

A few examples

8.1 167 is prime

Let us show that $n = 167$ is prime using Atkin's test.

We begin by looking for a fundamental discriminant $-D$ for which 167 is represented by a form of the principal genus. We find $D = 43$. We are sure that 167 is represented by the principal form since $h(-43) = 1$. We then solve the system:

$$\begin{cases} r^2 & \equiv & -43 \bmod 167, \\ r & \equiv & 1 \bmod 4. \end{cases}$$

Using the algorithm of [2], we find $r = 25$. We reduce the lattice $\mathfrak{p} = 167\mathbf{Z} + \frac{25-\sqrt{-43}}{2}\mathbf{Z}$ with procedure RED:

$$\vec{v} = \begin{pmatrix} 334 \\ 0 \end{pmatrix}, \ \|\vec{v}\| = 334^2 = 111556, \ \vec{u} = \begin{pmatrix} 25 \\ -1 \end{pmatrix}, \ \|\vec{u}\| = 25^2 + 43 \times (-1)^2 = 668,$$

$$\rho := \frac{334 \times 25}{668} = 12.5, \ m := 12, \ \epsilon = +1,$$

$$\vec{v} = \begin{pmatrix} 334 - 12 \times 25 \\ 0 - 12 \times (-1) \end{pmatrix} = \begin{pmatrix} 34 \\ 12 \end{pmatrix}, \ \|\vec{v}\| = 34^2 + 43 \times 12^2 = 7348.$$

Since $\|\vec{v}\| \geq \|\vec{u}\|$, we deduce that $\vec{u}$ is a shortest vector in P.

We now compute the possible numbers of points for the two elliptic curves having complex multiplication by $\mathcal{O}$:

$$m_+ = 167 + 1 - 2\,\frac{2 \times 13 - 1}{2} = 143 = 11 \times 13, m_- = 167 + 1 + 2\,\frac{2 \times 13 - 1}{2} = 193.$$

We choose m_+ and we now look for an equation of a curve having m_+ points in F_{167}. The corresponding j is $(-960)^3 \bmod 167$. We deduce:

$$k = 107 \times (1728 - 107)^{-1} \bmod 167 = 158,$$

$$a = 3\,k = 140,$$

$$b = 2\,k = 149.$$

We choose the point $P = (6:6:1)$ on E and we find:

$$143\,P = (0:1:0).$$

Therefore, the curve E of equation:

$$y^2 \equiv x^3 + 140x + 149 \bmod 167$$

has exactly 143 points in $\mathbf{F}_{167}$.

We verify the conditions of the theorem with $s = m = 143$:

$$\begin{array}{rcccl} \frac{143}{13}P & = & 11\,P & = & (140:147:1), \\ \frac{143}{11}P & = & 13\,P & = & (\ 12:\ \ 65:1). \end{array}$$

Hence 167 is prime.

8.2 Numbers taken from the Cunningham project

I implemented Atkin's algorithm on a SUN 3/60 using the language Le-Lisp 15.21 developed in INRIA. This language can handle arbitrarily large integers and the basic arithmetic routines are written in assembly. With that implementation, I was able to prove the primality of 43 numbers of [21]. Those numbers are listed below.

d	name	d	name
222	$2, 1958M$	284	$2, 2338M$
228	$2, 1594M$	284	$2, 1096+$
228	$2, 1874M$	286	$2, 2102M$
236	$2, 808+$	288	$2, 1049-$
237	$2, 979-$	294	$2, 2126L$
237	$2, 883+$	296	$2, 2122L$
237	$2, 1886L$	301	$2, 1061+$
245	$2, 844+$	307	$2, 2242M$
255	$2, 2366M$	312	$2, 1189+$
260	$2, 911+$	315	$2, 1093+$
264	$2, 1013+$	315	$2, 2314L$
264	$2, 2290L$	319	$2, 1117+$
265	$2, 1858M$	321	$2, 1112+$
266	$2, 2054M$	324	$2, 2234M$
268	$2, 1169-$	327	$2, 2342L$
268	$2, 1966L$	332	$2, 2258L$
271	$2, 2198M$	334	$2, 2374M$
277	$2, 1906L$		
279	$2, 1934L$		
284	$2, 2134L$		

My personal record is the certificate of the 564-digit factor of F_{11}. We now know that[1]:

$$F_{11} = 319489 \times 974849 \times 167988556341760475137 \times 3560841906445833920513 \times P_{564}.$$

The computations needed three weeks CPU time.

A little later, I proved the primality of the 572-digit number S_{1493}, where

$$S_p = \frac{(1+\sqrt{2})^p + (1-\sqrt{2})^p}{2}.$$

This number was introduced in [95] (see also [108]). The computation took nearly a month to complete.

[1]The second and third largest factors of this number were found by R. P. Brent in May 1988 using the elliptic curve method ([89]).

8.3 Primality certificate

The primality proof consists in blocks of numbers. Each block has the following structure :

$$\begin{array}{c} n_i \\ \textit{type} \\ \boxed{\begin{array}{c} \mathrm{P} \\ \mathrm{R} \\ \mathrm{O} \\ \mathrm{O} \\ \mathrm{F} \end{array}} \\ 0 \end{array}$$

where n_i is the number to be tested, *type* giving the type of theorem used to show the primality of n_i. This is an integer, choosen as follows :

-1	:	use of the factors of $n_i - 1$,
1	:	use of the factors of $n_i + 1$,
0	:	use of the factors of $n_i^2 - 1$,
D	:	an integer ($D > 2$) used in Atkin's test.

The primality proof of n_1 ends with a 0.

To each of the types corresponds a list of numbers used to complete the proof of n_i being prime, whenever the following block is valid.

We now describe the four possible lists :

1. type -1 :

$$\begin{array}{ll} p_0 & \\ \cdots & \text{the factors of } n-1 \\ p_k & \\ 0 & \\ b_0 & \\ \cdots & \text{the } b_i\text{'s of Theorem 1 in [133]} \\ b_k & \end{array}$$

2. type 1 :

$$\begin{array}{ll} q_0 & \\ \cdots & \text{the factors of } n+1 \\ q_l & \\ 0 & \\ P_0 & \\ Q_0 & \\ \cdots & \text{like in Theorem 2 in [133]} \\ P_l & \\ Q_l & \end{array}$$

3. type 0 (Cf. Theorem 2 in [133]) :

p_0
$\cdots$
p_k
0
b_0
$\cdots$
b_k
0
q_0
$\cdots$
q_l
0
P_0
Q_0
$\cdots$
P_l
Q_l

4. D :

D	the discriminant used
m	the number of points on the curve
r_0	
$\cdots$	the factors of m
r_k	
0	
a	the curve is E : $y^2 = x^3 + ax + b$
b	E has complex multiplication by $\mathcal{O}(\sqrt{-D})$
x	the coordinates of a point P on the curve
y	
f_1	
$\cdots$	the factorization of the order of P on E
f_l	

In all cases, the p_i, q_j and r_u are small primes ($< 10^6$), and they are listed in decreasing order, p_0 being the largest prime,...

In the proofs (except in the last type), a factor s that is larger than 10^6 is not listed in the blocks and must be reconstructed from the knowledge of the others. This is done in order to save some space.

We give in the appendix an example of a certificate.

Chapter 9

Statistical tests

9.1 Protocol

We follow [34]. We begin by choosing a number of digits, say d. For this d, we repeat 20 times the following pricedure.

1. choose a random odd number n with d digits;
2. increment n;
3. look for possible factors less than 10^4;
4. if we find a factor of n then go back to 2;
5. execute 4 Miller-Rabin tests on n;
6. if n is not a spsp then go back to 2;
7. use Atkin's test to prove that n is prime.

Each time we go through point 7, we keep the computation times of each phase of the algorithm and also the length of the primality chain and the maximum rank of discriminant used. We then make some statistics which are summarized below.

9.2 Results

The computations were done on a SUN 3/60 with version 2.3.4 of the program (June 20, 1988). The results are given in seconds of CPU. For each d, we have indicated on the first line the time needed to discover all prime factors of n below 10^4, on the second the time of 4 Miller-Rabin tests, on the third the time of Atkin's test, on the fourth the maximum rank of discriminant used and on the fifth one the length of the primality chain.

d	minimum	maximum	mean	deviation
50	0.7	0.8	0.7	0.0
	1.6	1.9	1.7	0.1
	76.9	715.6	383.6	192.4
	0.0	7.0	2.3	1.8
	2.0	8.0	5.6	1.6
100	0.8	0.8	0.8	0.0
	5.6	6.9	6.1	0.4
	1441.3	10407.1	4108.1	2181.7
	1.0	100.0	22.3	30.5
	6.0	14.0	9.8	2.4
120	0.8	0.8	0.8	0.0
	8.4	10.5	9.4	0.6
	2637.2	10504.4	6567.8	1965.2
	3.0	90.0	25.2	24.9
	7.0	20.0	13.1	2.8
140	0.8	0.9	0.8	0.0
	12.0	14.7	13.2	1.0
	4862.9	16651.3	10917.0	4648.3
	6.0	290.0	80.0	72.5
	12.0	19.0	15.8	2.1
160	0.8	0.9	0.8	0.0
	15.3	20.4	17.1	1.4
	8391.4	33091.7	17762.5	6423.1
	3.0	205.0	65.3	51.6
	14.0	25.0	18.2	3.0
180	0.8	0.9	0.9	0.0
	19.6	24.9	21.8	1.5
	13113.8	43803.5	27404.4	9327.9
	8.0	278.0	113.5	88.2
	15.0	26.0	21.4	3.0
200	0.8	0.9	0.9	0.0
	24.9	30.9	27.7	2.0
	18436.8	66597.8	36905.6	11212.0
	5.0	276.0	116.1	72.5
	21.0	30.0	24.5	2.4

Conclusion

We have described a primality testing algorithm that extends the oldest ones. This algorithm has benefited from a century of research. This algorithm is very fast and gives a certificate of primality.

It remains to give an exact analysis of Atkin's test. This seems to be a difficult problem, but I think there some possible ways of attack, that I will describe elsewhere. Recently, Atkin has indicated to me ([8]) that there are several improvements possible for his algorithm. They too, will be treated elsewhere.

The last point worth noting is the work of Adleman and Huang ([1]). They describe a primality test that uses algebraic curves of genus 2. It is a polynomial test, but it seems difficult to get a practical version of it.

Appendix A

Numerical Results

A.1 The coefficients of j

By section 6.1.2, it is necessary to compute the c_n up to $n = 160$. This computation was done using MAPLE on a SUN 3/60 in about 90s of CPU. I verified the results with theorem (5.2.7). The values found for $n \leq 100$ agree with that of [122].

0	744
1	196884
2	21493760
3	864299970
4	20245856256
5	333202640600
6	4252023300096
7	44656994071935
8	401490886656000
9	3176440229784420
10	22567393309593600
11	146211911499519294
12	874313719685775360
13	4872010111798142520
14	25497827389410525184
15	126142916465781843075
16	593121772421445058560
17	2662842413150775245160
18	11459912788444786513920
19	47438786801234168813250
20	189449976248893390028800
21	731811377318137519245696
22	2740630712513624654929920
23	9971041659937182693533820
24	35307453186561427099877376
25	121883284330422510433351500
26	410789960190307909157638144
27	1353563541518646878675077500
28	4365689224858876634610401280
29	13798375834642999925542288376
30	42780782244213262567058227200
31	130233693825770295128044873221
32	389608006170995911894300098560
33	1146329398900810637779611090240
34	3319627709139267167263679606784
35	9468166135702260431646263438600
36	26614365825753796268872151875584
37	73773169969725069760801792854360
38	201768789947228738648580043776000
39	544763881751616630123165410477688
40	1452689254439362169794355429376000

Table A.1: Values of c_n for $0 \leq n \leq 40$

41	3827767751739363485065598331130120
42	9970416600217443268739409968824320
43	25683334706395406994774011866319670
44	65452367731499268312170283695144960
45	165078821568186174782496283155142200
46	412189630805216773489544457234333696
47	1019253515891576791938652011091437835
48	2496774105950716692603315123199672320
49	6060574415413720999542378222812650932
50	14581598453215019997540391326153984000
51	34782974253512490652111111930326416268
52	82282309236048637946346570669250805760
53	193075525467822574167329529658775261720
54	449497224123337477155078537760754122752
55	1038483010587949794068925153685932435825
56	2381407585309922413499951812839633584128
57	5421449889876564723000378957979772088000
58	12255365475040820661535516233050165760000
59	27513411092859486460692553086168714659374
60	61354289505303613617069338272284858777600
61	135925092428365503809701809166616289474168
62	299210983800076883665074958854523331870720
63	654553043491650303064385476041569995365270
64	1423197635972716062310802114654243653681152
65	3076095473477196763039615540128479523917200
66	6610091773782871627445909215080641586954240
67	14123583372861184908287080245891873213544410
68	30010041497911129625894110839466234009518080
69	63419842535335416307760114920603619461313664
70	133312625293210235328551896736236879235481600
71	278775024890624328476718493296348769305198947
72	579989466306862709777897124287027028934656000
73	1200647685924154079965706763561795395948173320
74	2473342981183106509136265613239678864092991488
75	5070711930898997080570078906280842196519646750
76	10346906640850426356226316839259822574115946496
77	21015945810275143250691058902482079910086459520
78	42493520024686459968969327541404178941239869440
79	85539981818424975894053769448098796349808643878
80	171444843023856632323050507966626554304633241600

Table A.2: Values of c_n for $41 \leq n \leq 80$

81	342155525555189176731983869123583942011978493364
82	679986843667214052171954098018582522609944965120
83	1345823847068981684952596216882155845897900827370
84	2652886321384703560252232129659440092172381585408
85	5208621342520253933693153488396012720448385783600
86	10186635497140956830216811207229975611480797601792
87	19845946857715387241695878080425504863628738882125
88	38518943830283497365369391336243138882250145792000
89	74484518929289017811719989832768142076931259410120
90	143507172467283453885515222342782991192353207603200
91	275501042616789153749080617893836796951133929783496
92	527036058053281764188089220041629201191975505756160
93	1004730453440939042843898965365412981690307145827840
94	1908864098321310302488604739098618405938938477379584
95	3614432179304462681879676809120464684975130836205250
96	6821306832689380776546629825653465084003418476904448
97	12831568450930566237049157191017104861217433634289960
98	24060143444937604997591586090380473418086401696839680
99	44972195698011806740150818275177754986409472910549646
100	83798831110707476912751950384757452703801918339072000
101	155668193750688990263073298451234875129478434543218264
102	288303186787951198298816113296992617122316038101483520
103	532360384582564934616501236583995061891109488627959595
104	980138362015635064853029622650402721085223194498170880
105	1799337415283351057784679746927662437028848197411667200
106	3293814717594067150615059405642913451163618464253284352
107	6012628945306905638475933896845978280628197052031129310
108	10945239571973146355644316377974790144184665570787328000
109	19870021249929143399620419901633518864858002945671570872
110	35974914067272344165080069731483463647351003483134771200
111	64959906526239451003631207679783219244067157572973309165
112	116990520972038212694292103853261700870542959023866511360
113	210150650607452579599569241266223402742536169598850140520
114	376530684735414125523529312982816424375348668355995860992
115	672936445390958162789200232375699256427860729243275278200
116	1199681393661839026926928055463470424354390385916227584000
117	2133486254395087627066211294768723060158283934803591682840
118	3784943390783182045215204579988585449490852441694764032000
119	6698658178192740642445240413620216160411737678961227977333
120	11827368666877314043343176772350152158093158756436017152000

Table A.3: Values of c_n for $81 \leq n \leq 120$

121	2083401971581702422963876544461981100273140987951870597786O
122	36614667641297465631148164090265327830116953146702260817920
123	64201685070162147725464611749673657092707750583184564007140
124	112320501139624198948010798556804314935597620040020216250368
125	196067062984509187040951955197586503581394033288131187910000
126	341503183853729284527745542437450034191132793987024191963136
127	593527224934578104990955101074755370464156900515981460035760
128	1029326982786807780822262981773369664910194824346496663552000
129	1781327334607563553242155946942957911787915231543786544855872
130	3076255458121660274525842607461942502721486243667804049203200
131	5301512358998791842434783684140565672963212144540589846766730
132	9117716891510272645246866321916903552833089894324700932997120
133	15649173580646538023632483701212113986051179845148676081072000
134	26805600507843615676780348158506233745679095840358313631457280
135	45824545752897975638363067327021086978138050526337864068105250
136	78184160892692360692033106743351524493227376006503223904698368
137	133136363037979448419802190281354711972084964205919759749844360
138	226277328936119593410684227507299067090596382230940358427607040
139	383849364102110667918871300554352702001779875575109378311687238
140	649927414915107204189746056821613805195682334609541750934732800
141	1098403231975197618162311176531601274195935838151818755420426496
142	1852934958400944784442796335379663899730066804201679410906808320
143	3120098748434279557741977638004552939262820438627923690537304215
144	5244384362783084550505991237107663434068139738718177587933216768
145	8799272669010035139635788408275531605262723487998864772081386000
146	14737813753294520543203260468676056729565795540294581967508221952
147	24641161908405295029454883456868810746753999135187535773657492210
148	41128114800832056472193427901680195244842608500412778593407303680
149	68528854069293841520850278819906383394886596742476743833938452888
150	113991534440339214303055815358975788933153385224046103306861568000
151	189296894095711243511596757344199309221843546698914758259626164006
152	313829171558617091476645679676773650170102111122685815971708928000
153	519432505469337519910483996962754593807807386379002989717621971720
154	858337074911864194441021902465973211289758739151296158885919916032
155	1416075424321568658998716121949374369295392301441222953251282883200
156	2332498577634015943075501801916414647041675190944717865454457716736
157	3835919567106744967943382133370273180904167274393873623087469325560
158	6298501103182276920761494070150073057818043578349302767232585728000
159	10325972125458895112489938740970562151366569134784241868994861388333
160	16902736289392763393686481949937653722118982016482528463202916761600

Table A.4: Values of c_n for $121 \leq n \leq 160$

A.2 The coefficients of $j^{\frac{1}{3}}$

For the sake of curiosity, we computed the coefficients a_n of the expansion of $j^{\frac{1}{3}}$[1]. They are listed below.

[1] With the unvaluable help of P. Flajolet

0	1
1	248
2	4124
3	34752
4	213126
5	1057504
6	4530744
7	17333248
8	60655377
9	197230000
10	603096260
11	1749556736
12	4848776870
13	12908659008
14	33161242504
15	82505707520
16	199429765972
17	469556091240
18	1079330385764
19	2426800117504
20	5346409013164
21	11558035326944
22	24551042107480
23	51301080086528
24	105561758786885
25	214100032685072
26	428374478862400
27	846173187465216
28	1651298967150546
29	3185652564830016
30	6078963644150128
31	11480231806541824
32	21467177880529689
33	39764843702689336
34	72997137165153780
35	132850632324345216
36	239789319501693956
37	429388971394662400
38	763068418302358384
39	1346156250291692544
40	2358124102729916605

Table A.5: Values of a_n for $0 \leq n \leq 40$

41	4102886111983480016
42	7092013721210817960
43	12181659673477246976
44	20796676802261030704
45	35295598997521245568
46	59562101011874495480
47	99958912569056522240
48	166859205793906934725
49	277094035493060977616
50	457846796927164829644
51	752824055834234849792
52	1231993177206298051342
53	2006887024540451971552
54	3254564967545188642688
55	5254984221166437861376
56	8449072038631284807277
57	13528641219547382906880
58	21575122191088716659580
59	34272883507725150027776
60	54236148944092100035212
61	85508372157211839147200
62	134322619611238780551560
63	210255786410830905483264
64	327975307667040641422302
65	509874665522370694985616
66	790038401097295649534084
67	1220190367687966774807360
68	1878592406271125101826850
69	2883320664671775504158112
70	4412020319246554888052096
71	6731223196884016735290368
72	10239746206630909007114830
73	15532772283766353988621232
74	23496237940048719603978416
75	35445525499405116178184192
76	53328774255935088876042846
77	80024225913215197570007040
78	119774106067660824059137680
79	178816321332967892783308800
80	266302141435950687083385898

Table A.6: Values of a_n for $41 \leq n \leq 80$

81	395626464585099415963089432
82	586352076626848780324055868
83	866987343646345830897958656
84	1278987646997829708458075006
85	1882508106790653584486831264
86	2764657727253873829818087008
87	4051319627022611947623208960
88	5924045677593740492679605242
89	8644158584921556252765072640
90	12587072583726783877738645716
91	18291076185713333532765044736
92	26526546765920570822788875850
93	38393981309791172640582140288
94	55462599260838952202638766240
95	79965973974278151669445132288
96	115077692326257138869488942075
97	165299135663513669579964825600
98	237004094508424964729153350948
99	339202414826477820420315095168
100	484609065806766896282938482968
101	691138441600089052702411591904
102	983989817612649436669691786728
103	1398553400363731792138273996800
104	1984453790102172211090137629699
105	2811167715384595156580776052432
106	3975817581081717649606841502180
107	5613967994231286902030805696512
108	7914561136734092932391881774424
109	11140548680268370691910462784832
110	15657353594272677118695949314432
111	21972079777407156339515827556352
112	30787455424666221753488388089495
113	43075947987034599772855654621704
114	60181460106441112717662285030976
115	83958689700895620451017311468032
116	116963859237905549824916705653938
117	162715419527062258476018684695200
118	226049955585838792249236143298288
119	313607461020191720384154765193216
120	434492199579667713444383965500952

Table A.7: Values of a_n for $81 \leq n \leq 120$

121	601171604103733471011494341100144
122	830697498860633213455753416384040
123	1146363273870952303930084880089088
124	1579950026967464060191677004403394
125	2174767502582626014100470990503936
126	2989766396767913422897695805815400
127	4105093251310268960542963603120128
128	5629585677548807970979586777992337
129	7710874585380392479639157406420464
130	10548985436280083641789107175956044
131	14414630823291997610081658767241664
132	19673786429634071372183534147106166
133	26820674052322518367437907154160672
134	36521981720657265010493373341104104
135	49676088499595366678683799535752192
136	67492304843899802414958986406122325
137	91596786489072201699606922298163200
138	124173959966600654306613294406166400
139	168155180707388555789104892570643456
140	227470153401561503667255919349419838
141	307381671579243224863052347733548416
142	414930863195854442410224501710292520
143	559528864403412243525770128382287872
144	753742343253799109368091817263721781
145	1014335420294288881844760354458770304
146	1363650409832209162008303428426024192
147	1831435904468340865827030108248473600
148	2457264964996216372081345420227008626
149	3293731059511585227842181411905769248
150	4410668178543085797101556454430789400
151	5900718479526590969482843431500279808
152	7886671402073515781360956901059333150
153	10531129617119472694340504652678980848
154	14049228742397892242259801442890322284
155	18725361561021751188977256641891737600
156	24935149193335510230514215424857965558
157	33174281604635868193149797107675299840
158	44096344280510308280025843088905609600
159	58562390892916336176312504564409819136
160	77705857305943109983208336928208798419

Table A.8: Values of a_n for $121 \leq n \leq 160$

A.3 The $P_D(X)$ polynomials

I computed all the polynomials corresponding to all known values of discriminant D for which $h(-D) \leq 10$. We begin with some results concerning the number of these numbers. Then we give the smallest polynomials for given h.

A.3.1 Buell's tables

In [22], the author has made some statistics on discriminants of imaginary quadratic fields less than 4000000.

h	smallest D	largest	number of D
1	3	163	9
2	15	427	18
3	23	907	16
4	39	1555	54
5	47	2683	25
6	87	3763	51
7	71	5923	31
8	95	6307	131
9	199	10627	34
10	119	13843	87

Table A.9: Buell's tables.

We thus have a stock of 456 discriminants, making $6 + 4 + 2 \times 454 = 918$ (classes of) elliptic curves.

A.3.2 Some polynomials

$$\begin{aligned}
P_3 &= X \\
P_{15} &= X^2 + 191025X - 495^3 \\
P_{23} &= X^3 + 3491750X^2 - 5151296875X + 23375^3 \\
P_{39} &= X^4 + 331531596X^3 - 429878960946X^2 + 109873509788637459X + 2755377^3 \\
P_{47} &= X^5 + 2257834125X^4 - 9987963828125X^3 + 5115161850595703125X^2 \\
&\quad -14982472850828613281250X + 252209375^3 \\
P_{87} &= X^6 + 5321761711875X^5 + 85585228375218750X^4 + 28321090578679361484375000X^3 \\
&\quad +497577733884372638735595703125X^2 + 432181202257616392838287353515625X \\
&\quad +819225140625^3 \\
P_{71} &= X^7 + 313645809715X^6 - 3091990138604570X^5 + 98394038810047812049302X^4 \\
&\quad -823534263439730779968091389X^3 + 5138800366453976780323726329446X^2 \\
&\quad -425319473946139603274605151187659X + 903568991567^3 \\
P_{95} &= X^8 + 19874477919500X^7 - 688170786018119250X^6 + 395013575867144519258203125X^5 \\
&\quad -13089776536501963407329479984375X^4 \\
&\quad +352163322858664726762725228294921875X^3 \\
&\quad -1437415939871573574572839010971248046875X^2 \\
&\quad +21106316391166752679539154247640568847656 25X + 475911004500625^3 \\
P_{199} &= X^9 + 1765619027977093866 0X^8 + 1331303100189256816837434X^7 \\
&\quad +311741055246397228842310784103371345424X^6 \\
&\quad +23969299805117437326359388515188205981243787X^5 \\
&\quad +934682848803434155897358662478037099871861466271X^4 \\
&\quad -15361831050875895680622837467024669907518877308748738X^3 \\
&\quad +81311504213341585710631261056689664491326495914681965478X^2 \\
&\quad -262648565634938630871054990973171108239996044803712751064 59X \\
&\quad +182453173698107021391^3 \\
P_{119} &= X^{10} + 764872171216961X^9 - 702413556628089885 99X^8 \\
&\quad +58503581026213096953804360 6647X^7 \\
&\quad -528557124686794965810654876959425 73X^6 \\
&\quad +479493707132867076460954003979685794 7016X^5 \\
&\quad +12480611255809545689627144542329203076373873X^4 \\
&\quad +294940229205078963137666013133712856547227804 43X^3 \\
&\quad -292223928830848711011022637790896567674102040378617X^2 \\
&\quad +3464856262185617392921811727299239377112950044606542 34X \\
&\quad -226824153323972438 3^3
\end{aligned}$$

A.4 A certificate

Bibliography

[1] L. M. ADLEMAN, M. A. HUANG. Recognizing primes in random polynomial time. *Proc. CRYPTO 86.*

[2] L.M. ADLEMAN, K. MANDERS, G. L. MILLER. On taking roots in finite fields. *Proc. 18th Annual IEEE Symp. Foundations of Computer Science*, 1977, pp. 175-178.

[3] L. M. ADLEMAN, C. POMERANCE, R. S. RUMELY. On distinguishing prime numbers from composite numbers. *Annals of Math.*, **117**, 1983, pp. 173-206.

[4] A. O. L. ATKIN, J. N. O'BRIEN. Some properties of $p(n)$ and $c(n)$ modulo powers of 13. *Trans. Amer. Math. Soc.*, **126**, 1967, pp. 442-459.

[5] A. O. L. ATKIN. Proof of a conjecture of Ramanujan. *Glasgow Math. J.*, **8**, 1967, pp. 14-31.

[6] A. O. L. ATKIN. Congruences for modular forms. *Computers in mathematical research*, North Holland, 1968, pp. 8-19.

[7] A. O. L. ATKIN. Manuscript, August 1986.

[8] A. O. L. ATKIN. Private communications, September 1988.

[9] P. BEAUCHEMIN, G. BRASSARD, C. CRÉPEAU, C. GOUTIER, C. POMERANCE. The generation of random numbers that are probably prime. *J. Cryptology*, **1**, 1988, pp. 53-64.

[10] E. BEDOCCHI. Cubiche ellittiche su F_p. *Bollettino U. M. I.*, **5** (17-B), 1980, pp. 269-277.

[11] E. R. BERLEKAMP. Factoring polynomials over large finite fields. *Math. of Comp.*, **24**, 111, 1970, pp. 713-735.

[12] W. E. H. BERWICK. Modular invariants expressible in terms of quadratic and cubic irrationalities. *Proc. London Math. Soc. (2)*, **28**, 1928, pp. 53-69.

[13] E. BOMBIERI. Counting points on curves over finite fields (d'après S. A. Stepanov). *Séminaire Bourbaki*, **430**, 1972-1973.

[14] A. BOREL, S. CHOWLA, C. S. HERZ, K. IWASAWA, J. P. SERRE. *Seminar on complex multiplication.* Lect. Notes in Math., 21, Springer, 1966.

[15] Z. I. BOREVITCH, I. R. SHAFAREVITCH. *Théorie des nombres.* Gauthiers-Villars, Paris, 1967.

[16] W. BOSMA. Primality testing using elliptic curves. Report 85-12, Math. Instituut, Universeit van Amsterdam.

[17] R. P. Brent. An improved Monte Carlo factorization algorithm. *BIT*, **20**, 1980, pp. 176-184.

[18] R. P. Brent. Some integer factorization algorithms using elliptic curves. *Proc. 9th Australian Computer Science Conference*, Feb 1986.

[19] J. Brillhart. Note on representing a prime as a sum of two squares. *Math. of Comput.*, **26**, 120, 1972, pp. 1011-1013.

[20] J. Brillhart, D. H. Lehmer, J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. of Comp.*, **29**, 130, 1975, pp. 620-647.

[21] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers.* Contemporary Mathematics, **22**, AMS, 1983.

[22] D. A. Buell. Small class numbers and extreme values of L-functions of quadratic fields. *Math. of Comp.*, **31**, 139, 1977, pp. 786-796.

[23] H. Cartan. *Théorie élémentaire des fonctions analytiques d'une ou plusieurs variables complexes.* Hermann, Paris, 1978.

[24] J. W. S. Cassels. Diophantine equations with special references to elliptic curves. *J. London Math. Soc.*, **41**, 1966, pp. 193-291.

[25] J. W. S. Cassels, A. Frölich. *Algebraic number theory.* Proc. Int. Congress organized by the London Mathematical Society, 1967.

[26] J. Chailloux, M. Devin, J.-M. Hullot. *Le-Lisp: A Portble an Efficient Lisp System.* ACM Symposium on Lisp and Functional Programming, 1984, Austin, Texas.

[27] J. Chailloux, M. Devin, F. Dupont, J.-M. Hullot, B. Serpette, J. Vuillemin. *Le-Lisp version 15.2, le Manuel de référence.* Documentation INRIA, Mai 1987.

[28] K. Chandrasekharan. *Elliptic functions.* GRU 281, Springer-Verlag, 1985.

[29] B. W. Char, K. O. Geddes, G. H. Gonnet, S. M. Watt. *MAPLE Reference Manual, Fourth Edition.* Symbolic Computation Group, Department of Computer Science, University of Waterloo, 1985.

[30] D. V. Chudnovsky, G. V. Chudnovsky. Sequences of numbers generated by addition in formal groups and new primality and factorization tests. Research report RC 11262, IBM, Yorktown Heights, 1985.

[31] H. Cohen. Tests de primalité d'après Adleman, Rumely, Pomerance et Lenstra. *Séminaire de théorie des nombres*, Grenoble, 2, 11, et 18 juin 1981.

[32] H. Cohen. Cryptographie, factorisation et primalité : l'utilisation des courbes elliptiques. *Proc. of Journée annuelle de la SMF*, Paris, January 1987.

[33] H. Cohen, H. W. Lenstra, Jr. Primality testing and Jacobi sums. *Math. of Comp.*, **42**, 165, 1984, pp. 297-330.

[34] H. Cohen, A. K. Lenstra. Implementation of a new primality test. *Math. of Comp.*, **48**, 177, 1987, pp. 103-121.

[35] H. Cohn. *Advanced number theory.* Dover, New York, 1980.

[36] H. Cohn. *A classical invitation to algebraic numbers and class fields.* Universitext, Springer Verlag, 1978.

[37] H. Cohn. *Introduction to the construction of class fields.* Cambridge studies in advanced mathematics 6, Cambridge University Press, 1985.

[38] G. Cornacchia. Su di metodo per la risoluzione in numeri interi dell' equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$. *Giornale di Matematiche di Battaglini*, **46**, 1908, pp. 33-90.

[39] C. Couvreur, J.J. Quisquater. An introduction to fast generation of large prime numbers. Philips J. Research 37, 1982, pp. 231-264.

[40] H. Davenport, H. Hasse. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine und Angew. Math.*, **172**, 1935, pp. 151-182.

[41] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg*, **14**, 1941, pp. 197-272.

[42] M. Deuring. Die Klassenkörper der komplexen Multiplikation. *Enzyklopädie der mathematischen Wissenschaften mit Einschluss ihrer Anwendungen*, Bd 1, H. 10, T. 2, Teubner, Stuttgart, 1958.

[43] W. Diffie, M. E. Hellman. New directions in Cryptography. *IEEE Trans. on Information Theory*, vol IT-22-6, nov 1976.

[44] D. R. Dorman. Special values of the elliptic modular function and factorization formulae. *J. Reine und Angew. Math.*, **383**, 1988, pp. 207-220.

[45] W. J. Ellison, M. Mendès France. *Les nombres premiers.* Hermann, Paris, 1975.

[46] W. Fulton. *Algebraic curves.* Math. Lec. Note Series, W. A. Benjamin Inc., 1969.

[47] C. F. Gauss. *Disquisitiones Arithmeticae.* G. Fleischer, Leipzig, 1801; English translation by A. A. Clarke, Yale Univ. Press, New York, 1966; revised English translation by W. C. Waterhouse, Springer-Verlag, New York, 1986.

[48] A. O. Gel'fond, Yu. V. Linnik. *Elementary methods in the analytic theory of numbers.* Pergamon Press, Oxford, 1966.

[49] S. Goldwasser, J. Kilian. Almost all primes can be quickly certified. *Proc. 18th STOC*, Berkeley, 1986, pp. 316-329.

[50] A. G. Greenhill. Table of complex multiplication moduli. *Proc. London Math. Soc. (1)*, **21**, 1891, pp. 403-422.

[51] B. H. Gross, D. B. Zagier. On singular moduli. *J. Reine und Angew. Math.*, **355**, 1985, pp. 191-220.

[52] R. Gupta, M. Ram Murty. Primitive points on elliptic curves. *Compositio Mathematica*, **58**, 1986, pp. 13-44.

[53] R. K. GUY. How to factor a number. *Proc. fifth Manitoba Conference on numerical math.*, 1975, pp. 49-89.

[54] G. H. HARDY, E. M. WRIGHT. *An introduction to the theory of numbers.* 5th edition, Clarendon Press, Oxford, 1985.

[55] R. HARTSHORNE. *Algebraic geometry.* GTM 52, Springer, 1977.

[56] H. HASSE. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F. K. Smidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. *Ges. d. Wiss. Narichten. Math.-Phys. Klasse*, 1933, pp. 253-262.

[57] H. HASSE. Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. *Abh. Math. Sem. Univ. Hamburg*, **10**, 1934, pp. 325-348.

[58] H. HASSE. Zur Theorie der abstrakten elliptischen Funktionenkörper I, II, III. *J. Reine und Angew. Math.*, **175**, 1936.

[59] H. HASSE. Zur Geschlechtertheorie in quadratischen Zahlkörpern. *J. of the Math. Soc. of Japan*, **3**, 1, 1951, pp. 45-51.

[60] O. HERRMANN. Uber die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$. *J. Reine und Angew. Math.*, **274-275**, 1973.

[61] A. HURWITZ, R. COURANT. *Funktionentheorie.* GRU 3, Springer.

[62] D. HUSEMÖLLER. *Elliptic curves.* GTM 111, Springer, 1987.

[63] E. L. INCE. *Cycles of ideals in quadratic fields.* Mathematical Tables, vol. IV, British Association for the advancement of Science, Cambridge University Press, 1968.

[64] K. IRELAND, M. ROSEN. *A classical introduction to modern number theory.* GTM 84, Springer, 1982.

[65] B. S. KALISKI, JR. A pseudo-random Bit generator based on elliptic logarithms. *Proc. Crypto 86*, pp. 13-1, 13-21.

[66] N. M. KATZ. An overview of Deligne's proof of the Riemann hypothesis for varieties over finite fields. *Proc. Symposia in Pure Mathematics*, **28**, 1976, pp. 275-305.

[67] D. E. KNUTH. *Seminumerical algorithms.* The art of computer programming, T. II, Addison-Wesley.

[68] D. E. KNUTH, L. TRABB PARDO. Analysis of a simple factorization algorithm. *Theoretical Computer Science*, **3**, 1976, pp. 321-348.

[69] N. KOBLITZ. *Introduction to elliptic curves and modular forms.* GTM 97, Springer, 1984.

[70] N. KOBLITZ. Primality of the number of points on an elliptic curve over a finite field. *Pacific J. of Math.*, **131**, 1, 1988, pp. 157-165.

[71] S. LANG. *Elliptic functions.* Addison-Wesley Publishing Company Inc., 1973.

[72] S. Lang. *Introduction to algebraic and abelian functions.* Addison-Wesley Publishing Company Inc., 1972.

[73] S. Lang. *Elliptic curves, diophantine analysis.* Springer-Verlag, 1978.

[74] S. Lang, H. Trotter. *Frobenius distributions in GL_2 extensions.* Lect. Notes in Math., 540, Springer-Verlag, 1976.

[75] D. H. Lehmer. Computer technology applied to the theory of numbers. *Studies in number theory*, Mathematics Association of America, 1969, pp. 117-151.

[76] D. H. Lehmer. Ramanujan's function $\tau(n)$. *Duke Math. J.*, **10**, 1943, pp. 483-492.

[77] D. H. Lehmer. Properties of the coefficients of the modular invariant $J(\tau)$. *Amer. J. Math.*, **64**, 1942, pp. 488-502.

[78] J. Lehner. Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Amer. J. of Math.*, **71**, 1949, pp. 136-148.

[79] J. Lehner. Further congruence properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Amer. J. of Math.*, **71**, 1949, pp. 373-386.

[80] H. W. Lenstra, Jr. Primality testing algorithms (after Adleman, Rumely, Williams). *Séminaire Bourbaki*, **576**, 1980-1981.

[81] H. W. Lenstra, Jr. Elliptic curves and number theoretic algorithms. Report 86-19, Math. Inst., Univ. Amsterdam, 1986.

[82] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Math.*, **126**, 1987, pp. 649-673.

[83] K. Mahler. On a class of non-linear functional equations connected with modular functions. *J. Austral. Math. Soc.*, **22**, Ser. A, 1976, pp. 65-120.

[84] Yu. I. Manin. On cubic congruences to a prime modulus. *Amer. Math. Soc. Transl.*, **2**, 13, 1960, pp. 1-7.

[85] R. Merkle, M. E. Hellman. Hiding information and signature in trapdoor knapsacks. *IEEE Trans. on Information Theory*, IT-24-5, sep 1978.

[86] G. L. Miller. Riemann's hypothesis and tests for primality. *Proc. 7th annual ACM Symposium on the theory of computing*, 1975, pp. 234-239.

[87] F. Morain, J. Olivos. Speeding up the computations on an elliptic curve using addition-subtraction chains. *Preprint*, 1988.

[88] L. Monier. Evaluation and comparison of two efficient probabilistic primality testing algorithms. *Theoretical Computer Science*, **12**, 1980, pp. 97-108.

[89] P. Montgomery. Fermat number F11 factored. *Transaction on USENET.sci.math.*

[90] M. Ram Murty. On Artin's conjecture. *J. Number Theory*, **16**, 1983, pp. 147-168.

[91] M. Newman. Remarks on some modular identities. *Trans. Amer. Math. Soc.*, **73**, 1952, pp. 313-320.

[92] M. Newman. The coefficients of certain infinite products. *Proc. Amer. Math. Soc.*, **4**, 1953, pp. 435-439.

[93] M. Newman. An identity for the coefficients of certain modular forms. *J. London Math. Soc.*, **30**, 1955, pp. 488-493.

[94] M. Newman. Congruences for the coefficients of modular forms and for the coefficients of $j(\tau)$. *Proc. Amer. Math. Soc.*, **9**, 1958, pp. 609-612.

[95] Newman, Shanks, Williams. Simple groups of square order and an interesting sequence of primes. *Acta Arith.*, XXXVIII, 1980, pp. 129-140.

[96] H. Petersson. Über die Entwicklungskoeffizienten der automorphen Formen. *Acta Mathematica*, **58**, 1932, pp. 169-215.

[97] D. A. Plaisted. Fast verification, testing and generation of large primes. *Theoretical Computer Science*, **9**, 1979, pp. 1-16.

[98] J. M. Pollard. A Monte-Carlo method for factorization. *BIT*, **15**, 1975, pp. 331-334.

[99] C. Pomerance. On the distribution of pseudoprimes. *Math. of Comp.*, **37**, 156, 1981, pp. 587-593.

[100] C. Pomerance. Analysis and comparison of some integer factoring algorithms. *Computational methods in number theory*, H. W. Lenstra and R. Tijdeman Eds, Math. Centrum, Amsterdam, 1984, pp. 89-140.

[101] C. Pomerance. Fast, rigorous factorization and discrete logarithm algorithms. *Proc. of the Japan-US Joint Seminar, Discrete Algorithms and Complexity*, Academic Press, 1987.

[102] C. Pomerance. Very short primality proofs. *Math. of Comp.*, **48**, 177, 1987, pp. 315-??

[103] C. Pomerance, S.S. Wagstaff, Jr. The pseudoprimes to 25.10^9. *Math. of Comp.*, **35**, 151, 1980, pp. 1003-1026.

[104] V. R. Pratt. Every prime has a succint certificate. *SIAM J. Comput.*, **4**, 1975, pp. 214-220.

[105] M. O. Rabin. Probabilistic algorithms in finite fields. *SIAM J. Comput.*, **9**, 2, 1980, pp. 273-280.

[106] H. Rademacher. The Fourier coefficients of the modular invariant $J(\tau)$. *Amer. J. Math.*, **60**, 1938, pp. 501-512.

[107] H. Rademacher. The Fourier series and the functionnal equation of the absolute modular invariant $J(\tau)$. *Amer. J. Math.*, **61**, 1939, pp. 237-248.

[108] P. Ribenboim. *The book of prime number records.* Springer, 1988.

[109] R. L. Rivest, A. Shamir, L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. of the ACM*, **21**, 2, 1978, pp. 120-126.

[110] A. Robert. *Elliptic curves.* Lect. Notes in Math., 326, Springer, 1986.

[111] R. Schertz. Die singulären Werte des Weberschen Funktionen f, f_1, f_2, γ_2, γ_3. *J. Reine und Angew. Math.*, **286-287**, 1976, pp. 46-74.

[112] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod$p$. *Math. of Comp.*, **44**, 1985, pp. 483-494.

[113] J. P. Serre. *Cours d'arithmétique.* P. U. F., Paris, 1970.

[114] D. Shanks. Five number theoretic algorithms. *Proc. 2nd Manitoba Conference on Numerical Mathematics*, 1972, pp. 51-70.

[115] D. Shanks. Class number, a theory of factorization, and genera. *Proc. Symp. Pure Math.*, AMS, **20**, 1971, pp. 415-440.

[116] J. H. Silverman. *The arithmetic of elliptic curves.* GTM 106, Springer, 1986.

[117] R. Solovay, V. Strassen. A fast Monte-Carlo test for primality. *Siam J. Comput.*, **6**, 1, 1977, pp. 84-85. Erratum, ibid, **7**, 1, 1978.

[118] I. N. Stewart, D. O. Tall. *Algebraic number theory.* Second edition, Chapman and Hall, London, New-York, 1987.

[119] J. T. Tate. The arithmetic of elliptic curves. *Inventiones Math.*, **23**, 1974, pp. 179-206.

[120] J. T. Tate. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda). *Séminaire Bourbaki*, **352**, 1968-1969.

[121] B. Vallée. *Une approche géométrique des algorithmes de réduction des réseaux en petite dimension.* Thèse, Caen, 1986.

[122] A. van Winjgaarden. On the coefficients of the modular invariant $J(\tau)$. *Proc. Kon. Nederl. Akad. Wetensch. Ser. A*, **16**, 1953, pp. 389-400.

[123] G. N. Watson. Singular moduli. *Proc. London Math. Soc.*, **40**, 1936, pp. 83-142.

[124] G. N. Watson. Ramanujans Vermutung über Zerfällungsanzahlen. *J. Reine und Angew. Math.*, **179**, 1938, pp. 97-128.

[125] H. Weber. *Lehrbuch der Algebra I, II, III.* Chelsea Publishing Company, New York, 1902.

[126] H. Weber. Zur complexen Multiplication elliptischer Functionen. *Math. Annalen*, **33**, 1889, pp. 390-410.

[127] H. C. Williams. Primality testing on a computer. *Ars Combinatoria*, **5**, 1978, pp. 127-185.

[128] H. C. Williams, H. Dubner. The primality of $R1031$. *Math. of Comp.*, **47**, 176, 1986, pp. 703-711.

[129] H. C. Williams, R. Holte. Some observations on primality testing. *Math. of Comp.*, **32**, 143, 1978, pp. 905-917.

[130] H. C. Williams, J. S. Judd. Determination of the primality of N by using factors of $N^2 \pm 1$. *Math. of Comp.*, **30**, 133, 1976, pp. 157-172.

[131] H. C. Williams, J. S. Judd. Some algorithms for prime testing using generalized Lehmer functions. *Math. of Comp.*, **30**, 136, 1976, pp. 867-886.

[132] P. Wilker. An efficient algorithmic solution of the diophantine equation $u^2 + 5v^2 = m$. *Math. of Comp.*, **35**, 152, 1980, pp. 1347-1352.

[133] M. C. Wunderlich. A performance analysis of a simple prime-testing algorithm. *Math. of Comp.*, **40**, 162, 1983, pp. 709-714.

[134] M. C. Wunderlich, J. L. Selfridge. A design for a number theory package with an optimized trial division routine. *Comm. of the ACM*, **17**, 5, 1974, pp. 272-276.

[135] B. F. Wyman. Hilbert class fields and group extensions. *Scripta Mathematica*, **XXIX**, 1-2, pp. 141-149.

[136] J. Young, D. A. Buell. The twentieth Fermat number is composite. *Math. of Comp.*, **50**, 181, 1988, pp. 261-265.

[137] H. G. Zimmer. An elementary proof of the Riemann hypothesis for an elliptic curve over a finite field. *Pacific J. of Math.*, **36**, 1, 1971, pp. 267-278.

[138] H. S. Zuckerman. The computation of the smaller coefficients of $J(\tau)$. *Bull. AMS*, **45**, 1939, pp. 917-919.