Primality testing

Johannes Buchmann

Volker Müller

Universität des Saarlandes
Im Stadtwald 15
6600 Saarbrücken
Germany

02/92

Contents

Chapter 1

Pseudo primes, probable primes

1.1 The Fermat test

Suppose that we want to test a rational integer for primality and compositeness. The easiest (but most expensive) test is **trial division**: For every integer $m \leq \sqrt{n}$ check whether m is a divisor of n. If no divisor is found in this way, then n is known to be a prime number. Of course, we do not have to use all numbers $m \leq \sqrt{n}$ but we can restrict ourselves to those $m \leq \sqrt{n}$ which are prime numbers. In any case, this test requires approximately $\sqrt{n}$ divisions which is feasable only for relatively small numbers. As soon as n gets larger we must use more elaborate techniques. It turns out that it is much easier to find out that n is not prime than to actually prove its primality. One of those **non-primality tests** is based on

Proposition 1.1 (Fermat's little theorem)
Let $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then we have $a^{\varphi(n)} \equiv 1 \bmod n$.

Proof: [Ke82] □

Since we know that for a prime number p the value of the Euler φ-function is

$$\varphi(p) = p - 1,$$

this means that n can only be prime if for any $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$ we have $a^{n-1} \equiv 1 \bmod n$. Based on this observation one obtains the **Fermat test** for non-primality: Pick $a \in \mathbb{Z}$ and compute $a^{n-1} \bmod n$. If $a^{n-1} \not\equiv 1 \bmod n$ then n is not a prime number, i.e. n is composite. After having checked "a few" values for a and having found no error, we are almost sure that n is a prime number. Note that this test does not yield a non trivial factor of n.

In order to make this test efficient, it is necessary to have a procedure to quickly determine $a^{n-1} \bmod n$, i.e. a fast exponentiation method. There are several methods of this kind, for a detailed discussion we refer to the book of Knuth ([Kn81]). Here we only mention one variant.

Suppose that we want to determine a^d for some element a in an abelian semigroup S with some exponent $d \in \mathbb{Z}_{\geq 0}$. For doing this we first determine the binary representation of d as $d = \sum_{i=0}^{s} \beta_i \cdot 2^i$ with $\beta_i \in \{0, 1\}$. Then we have

$$a^d = a^{\sum_{i=0}^{s} \beta_i \cdot 2^i} = \prod_{\beta_i = 1} a^{2^i}.$$

Using this equality we obtain the following algorithm:

Algorithm 1.1 (Fast exponentiation)

Input: $a, d \in S$.

Output: $b = a^d$.

1. *Initialize* $d' = d, \ b = 1, \ c = a$.
2. *If* d' *is odd, then set* $b = b \cdot c, \ d' = d' - 1$.
3. *If* $d' = 0$ *terminate with solution* b.
4. *Set* $d' = \frac{d'}{2}, \ c = c \cdot c$ *and goto (2).*

Proposition 1.2 *The determination of* a^d *mod* n *requires* $O(\log d)$ *elementary operations in* $\mathbb{Z}/n\mathbb{Z}$.

It would, of course, be very nice if the Fermat criterion were not only necessary for n being prime but also sufficient. This is, unfortunately, wrong. For example, we have

$$2^{340} \equiv 1 \bmod 341$$

in spite of the fact that

$$341 = 11 \cdot 31.$$

A number, which is composite but satisfies the Fermat criterion with base a is called a **pseudoprime for the base** a. In this terminology 341 is a pseudoprime for the base 2. If n is a pseudoprime for all $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$, then n is called a **Carmichael number**. The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$. The existence of such numbers is a motivation to look for more sophisticated primality tests.

1.2 The Euler test

In order to explain the Euler test, we introduce the Legendre and the Jacobi symbol. Let p be an odd prime and let $a \in \mathbb{Z}$. If $\gcd(a,p) = 1$ and if there is a solution x of the congruence

$$x^2 \equiv a \bmod p,$$

then a is called a **quadratic residue mod p**. If $\gcd(a,p) = 1$ but there is no such solution, then a is called a **quadratic non residue mod p**.

The **Legendre symbol** is defined as follows

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue mod } p; \\ 0 & \text{if } p \mid a; \\ -1 & \text{if } a \text{ is a quadratic non residue mod } p. \end{cases}$$

The **Jacobi symbol** is a generalization of the Legendre symbol. Let n be odd and let

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

be its unique decompositon into a power product of prime numbers. Then the Jacobi symbol is defined as

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

The Euler test is based on the following

Proposition 1.3 (Euler criterion)
If n is an odd prime and if $a \in \mathbb{Z}$ with $\gcd(a,n) = 1$, then

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n.$$

Proof: If $\left(\frac{a}{n}\right) = 1$, then there exists x such that $x^2 \equiv a \bmod n$ and so

$$a^{(n-1)/2} \equiv x^{n-1} \equiv 1 \bmod n.$$

To prove the converse, we observe that the equation $x^{(n-1)/2} \equiv 1 \bmod n$ has precisely $\frac{n-1}{2}$ solutions, namely the quadratic residues mod n. Hence, we have that $\left(\frac{a}{n}\right) \equiv 1 \bmod n$ if and only if $a^{(n-1)/2} \equiv 1 \bmod n$. But since $a^{n-1} - 1 \equiv (a^{(n-1)/2} - 1) \cdot (a^{(n-1)/2} + 1) \bmod n$ we see that the only other value of $a^{(n-1)/2} \bmod n$ can be -1. □

Again we have a new primality test. We can check first whether $a^{(n-1)/2} \equiv \pm 1 \bmod n$. If this congruence fails to hold, we know that n is not prime. Otherwise we have a further chance of showing that n is not prime by evaluating the Jacobi symbol and by comparing its value with $a^{(n-1)/2} \bmod n$.

In order to compute the Jacobi symbol we need

Proposition 1.4 (Law of quadratic reciprocity)
Let r, s be odd positive integers and let a, $b \in \mathbb{Z}$ with $\gcd(a,r) = 1 = \gcd(b,r)$. *Then we have*

$$\begin{aligned}
\left(\frac{a \cdot b}{r}\right) &= \left(\frac{a}{r}\right) \cdot \left(\frac{b}{r}\right), \\
\left(\frac{-1}{r}\right) &= (-1)^{(r-1)/2}, \\
\left(\frac{2}{r}\right) &= (-1)^{(r^2-1)/8}, \\
\left(\frac{r}{s}\right) &= \left(\frac{s}{r}\right) \cdot (-1)^{(r-1)(s-1)/4}.
\end{aligned}$$

Proof: [Ke82, section 3.6] □

If a composite number satisfies the condition of Proposition 1.3, it is called a **Euler pseudoprime for the base** a. We write n is $epsp(a)$. The smallest Euler pseudoprime for the base 2 is again 561.

1.3 The test of Solovay-Strassen

The test of Solovay-Strassen is based on

Proposition 1.5 *Let n be composite. Then*

$$\#\{a \in \mathbb{Z} \mid 1 < a < n,\ \gcd(a,n) = 1, n\ epsp(a)\} \ \leq\ \frac{n}{2}.$$

Proof: [Kr86, Th. 2.28, page 67] □

The test of Solovay and Strassen works as follows: Choose $a \in \{1, \ldots, n\}$ at random. Determine $d = \gcd(a,n)$. If $d \neq 1$, then n is not prime. Otherwise perform the Euler test. If the Euler criterion fails to hold, then n is not prime. Otherwise, the probability for n being composite is at most $\frac{1}{2}$.

If this test is applied k times, then n is either found to be composite or n is prime with probability at least $1 - \frac{1}{2^k}$.

1.4 The test of Miller

We now turn to Millers's Test.

Proposition 1.6 *Let $n = 1 + 2^t \cdot n_0$, where n_0 is odd and let $a \in \mathbb{Z}$. Then we have*

$$a^{n-1} - 1 = (a^{n_0} - 1) \cdot (a^{n_0} + 1) \cdot (a^{2n_0} + 1) \cdot \ldots \cdot (a^{2^{t-1}n_0} + 1).$$

Proof: We proceed by induction on t. For $t = 0$ and $t = 1$ the statement is trivially correct. Suppose we have proved the assertion for some $t \geq 1$. Let $n = 1 + 2^{t+1} \cdot n_0$. Then we have

$$a^{n-1} - 1 = a^{2^{t+1}n_0} - 1 = (a^{2^t n_0} - 1) \cdot (a^{2^t n_0} + 1)$$

and using the induction hypothesis we obtain our statement. □

Proposition 1.6 can be turned into a compositeness test since it implies

Proposition 1.7 *Let $n = 1 + 2^t \cdot n_0$ as in Proposition 1.6. If n is prime, then we either have $a^{n_0} \equiv 1 \bmod n$ or there is a $j \in \{0, 1, \ldots, t-1\}$, such that $a^{2^j n_0} \equiv -1 \bmod n$.*

Clearly, the decomposition

$$n - 1 = 2^t \cdot n_0$$

can be determined very quickly and hence Proposition 1.7 provides an efficient compositeness test. A composite number n which satisfies the criterion of Proposition 1.7 is called a **strong pseudoprime for the base** a. We write n is $spsp(a)$.

In order to estimate the probability for the primality of n which satisfies the criterion of Miller sufficiently frequently, we need

Proposition 1.8 (Miller)
If $n > 9$ is odd and composite, then

$$\#\{a \in \mathbb{Z} \mid 1 < a < n,\ \gcd(a, n) = 1 \text{ and } n\ sqsq(a)\} \ \leq\ \frac{n}{4}.$$

Proof: [Kr86, Th. 2.33, page 72] □

This means that a number which passes Miller's test k times is prime with probability $1 - \frac{1}{4^k}$ which is even better than the probability obtained from the test of Solovay-Strassen.

Chapter 2

Elementary primality proofs

2.1 Pocklington's theorem

Even though the compositeness tests discussed in the previous section provide good evidence for a number being prime, it is of course more satisfactory to be able to actually prove the primality of a probable prime. A first primality proof is based on

Proposition 2.1 (Pocklington's theorem)
Let s be a positive divisor of $n-1$, $s > \sqrt{n}$. Suppose there is an integer a satisfying

$$\begin{aligned} &a^{n-1} \equiv 1 \bmod n \\ &\gcd(a^{(n-1)/q} - 1, n) = 1 \end{aligned}$$

for each prime q dividing s. Then n is prime.

Proof: Assume on the contrary that n is not prime and let p be a prime factor of n which is at most $\sqrt{n}$. Set $b \equiv a^{(n-1)/s} \bmod n$. Then

$$b^s \equiv (a^{(n-1)/s})^s \equiv a^{n-1} \equiv 1 \bmod n.$$

Thus we also have $b^s \equiv 1 \bmod p$. On the other hand we know that

$$b^{s/q} \not\equiv 1 \bmod p$$

for all prime divisors q of s. Supposed for one prime divisor q' of s we had $b^{s/q'} \equiv 1 \bmod p$, we would know that p is a divisor of $b^{s/q'} - 1 = a^{(n-1)/q'} - 1$ and so we had a contradiction to the assumption that $\gcd(a^{(n-1)/q}, n) = 1$ for all prime divisors q of s. Hence s is the exact order of b modulo p. By Fermat's theorem we know that

$$b^{p-1} \equiv 1 \bmod p$$

and so s must be a divisor of $p-1$. But this is a contradiction because $s > \sqrt{n}$ and $p \leq \sqrt{n}$. □

This famous theorem can be used to prove the primality of an arbitrary probable prime n. The problem of a method based on this theorem is to find the factorization of $n-1$. It is however sufficient to determine a large probable prime factor s of $n-1$ whose primality is recursively proved by the same method.

2.2 Primality proofs for numbers of special form

Pocklington's theorem can be used to prove the primality of arbitrary numbers. In this section we want to prove the primality of numbers of a special form. First we ask when numbers of the form $k \cdot 2^l + 1$ with $k \in \mathbb{Z}_{\geq 1}$ and $l \in \mathbb{Z}_{\geq 2}$ are prime. Therefore we have

Proposition 2.2 (Proth)
Let $l \in \mathbb{Z}_{\geq 2},\ k \in \mathbb{Z}_{\geq 1},\ 3 \not| k$ and $k \leq 2^l + 1$.

Then $n = k \cdot 2^l + 1$ is prime if and only if $3^{k \cdot 2^{l-1}} \equiv -1 \bmod n$.

Proof: Assume that $3^{k \cdot 2^{l-1}} \equiv -1 \bmod n$. Put $s = 2^l$, $a = 3$ and $n = k \cdot 2^l + 1$. Then by assumption

$$a^{n-1} = 3^{k \cdot 2^l} \equiv 1 \bmod n$$

and

$$a^{(n-1)/2} \equiv -1 \not\equiv 1 \bmod n,$$

which by Pocklington's theorem shows that n is prime.

Now we prove the converse. Assume that n is prime. By Euler's criterion it is sufficient to show that 3 is a quadratic non residue modulo n. Since $3 \not| k$ and n is prime we have $k \cdot 2^l + 1 \equiv 2 \bmod 3$. Hence

$$\left(\frac{3}{k \cdot 2^l + 1}\right) = \left(\frac{k \cdot 2^l + 1}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

□

Using this Proposition we can give a criterium for the primality of the well known Fermat numbers.

Proposition 2.3 (Pepin)
For each $l \in \mathbb{Z}_{\geq 1}$ the **Fermat number** *$F_l = 2^{2^l} + 1$ is prime if and only if*

$$3^{(F_l - 1)/2} \equiv -1 \bmod F_l.$$

Proof: This statement is an immediate consequence of Proth's Proposition. □

Next we want to explain the **Lucas-Lehmer test** for proving the primality of a so called **Mersenne number** $M_n = 2^n - 1$ with $n \in \mathbb{N}$. The following Proposition is needed in the proof of the correctness of the Lucas-Lehmer test.

Proposition 2.4 *Let A be a commutative ring with an unit element 1 which contains $\mathbb{Z}/n\mathbb{Z}$ as a subring and let $s > 0$ be an integer. Further assume that there exists an element $\alpha \in A$ such that $\alpha^s = 1$ but for all primes q with $q \mid s$ we have that $\alpha^{s/q} - 1$ is invertible in A . If for some integer $t > 0$ the polynomial*

$$p(x) = \prod_{i=0}^{t-1} (x - \alpha^{n^i})$$

has coefficients in $\mathbb{Z}/n\mathbb{Z}$, then for any divisor r of n there exists an exponent $i \geq 1$ such that $r \equiv n^i \bmod s$.

Proof: Let r be a divisor of n. Without loss of generality we assume that r is a prime number. By $\overline{x}$ we denote the image of $x \in \mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z} \subseteq A$.

Since $r \mid n$, we have $r \cdot k = n$ for some $k \in \mathbb{Z}$, i.e. $\overline{r} \cdot \overline{k} = \overline{0}$, which means that $\overline{r}$ and $\overline{k}$ are zero divisors of A. Consider the maximal ideal $M \subset A$ containing the annulator

$$\mathrm{Ann}\,(\overline{k}) = \{\beta \in A \mid \beta \cdot \overline{k} = 0\}.$$

Then A/M is a field with prime field $\mathbb{Z}/r\mathbb{Z}$ and the (multiplicative) order of α in this field is precisely s. The canonical map $A \to A/M$ maps $\mathbb{Z}/n\mathbb{Z}$ onto $\mathbb{Z}/r\mathbb{Z}$. Hence the canonical image of $p(x)$ in A/M has coefficients in $\mathbb{Z}/r\mathbb{Z}$. Now the field $\mathbb{Z}/r\mathbb{Z}$ is invariant under the Frobenius automorphism $\overline{x} \longmapsto \overline{x}^r$ which means that α^r is a zero of $p(x) \bmod M$. We then have $\alpha^r \equiv \alpha^{n^i} \bmod M$ for some i, but since s is the order of $\alpha \bmod M$, we have $r \equiv n^i \bmod s$ for some i. $\square$

In order to be able to test Mersenne numbers $M_m = 2^m - 1$ for primality, we introduce the sequence $(e_j)_{j \in \mathbb{N}}$ which is defined by

$$e_1 = 4 \quad \text{and} \quad e_{k+1} = e_k^2 - 2.$$

So we get

Proposition 2.5 *Let $m \in \mathbb{Z}_{>2}$. Then the Mersenne number $M_m = 2^m - 1$ is a prime number if and only if $e_{m-1} \equiv 0 \bmod M_m$.*

Proof: We first remark that M_m can only be a prime number if m is prime. In fact, suppose that $m = a \cdot b$ is a non trivial factorization of m. Then we define $x = 2^a$ and we find the non trivial factorization

$$2^m - 1 = x^b - 1 = (x-1) \cdot (x^{b-1} + x^{b-2} + \ldots + x + 1).$$

To prove our Proposition, we first consider the case where m is even. In this case we must show that $e_{m-1} \not\equiv 0 \bmod M_m$. Write $m = 2 \cdot k$ and note that

$$M_m \;=\; 2^m - 1 \;=\; 2^{2k} - 1 \;=\; (2^k)^2 - 1 \;\equiv\; 0 \bmod 3.$$

It is therefore sufficient to prove that $e_{m-1} \not\equiv 0 \bmod 3$. But obviously we have $e_l \equiv -1 \bmod 3$ for $l \geq 2$.

Now assume that m is odd and write $n = M_m$ and $a = 2^{(m+1)/2}$. Then we have

$$a^2 \equiv 2^{m+1} \equiv 2 \cdot (2^m - 1) + 2 \equiv 2 \bmod n. \tag{2.1}$$

Consider the factor ring

$$A = (\mathbb{Z}/n\mathbb{Z}[x]) \Big/ \left(x^2 - \overline{a}x - \overline{1}\right)(\mathbb{Z}/n\mathbb{Z}[x]).$$

We can write $A = (\mathbb{Z}/n\mathbb{Z})[\alpha]$, where α is a formal zero of the polynomial

$$g(x) = x^2 - \overline{a}x - \overline{1}.$$

This means that all the elements $\xi \in A$ are of the form $\xi = \overline{s} + \overline{t} \cdot \alpha$, where $\overline{s}$ and $\overline{t}$ belong to $\mathbb{Z}/n\mathbb{Z}$ and where the number α satisfies the equation

$$\alpha^2 - \overline{a} \cdot \alpha - \overline{1} = \overline{0}.$$

Put $\beta = \overline{a} - \alpha$. Then we have

$$\begin{aligned}
(x - \alpha) \cdot (x - \beta) &= (x - \alpha) \cdot (x - \overline{a} + \alpha) \\
&= x^2 - \overline{a} \cdot x + (-\alpha^2 + \overline{a} \cdot \alpha) \\
&= x^2 - \overline{a} \cdot x - \overline{1} \\
&= g(x).
\end{aligned}$$

This shows that β is the other zero of $g(x)$ in A and we also find that $\alpha + \beta = \overline{a}$ and $\alpha \cdot \beta = -\overline{1}$.

Lemma 2.1 *For $k \in \mathbb{Z}_{\geq 1}$ we have $\alpha^{2^k} + \beta^{2^k} = \overline{e}_k$.*

Proof: (Lemma)
We use induction on k. For $k = 1$ we have

$$\begin{aligned}
\alpha^2 + \beta^2 &= \alpha^2 + \overline{a}^2 - \overline{2} \cdot \overline{a} \cdot \alpha + \alpha^2 \\
&= \overline{2} \cdot \alpha^2 + \overline{a}^2 - \overline{2} \cdot \overline{a} \cdot \alpha \\
&= \overline{2} \cdot \overline{a} \cdot \alpha + \overline{2} + \overline{a}^2 - \overline{2} \cdot \overline{a} \cdot \alpha.
\end{aligned}$$

Using (2.1) it follows that $\alpha^2 + \beta^2 = \overline{4}$ as asserted.

For the induction step assume that $\alpha^{2^k} + \beta^{2^k} = \overline{e}_k$. Then we have

$$\begin{aligned}
\overline{e}_{k+1} &= \overline{e}_k^2 - 2 \\
&= (\alpha^{2^k} + \beta^{2^k})^2 - 2 \\
&= \alpha^{2^{k+1}} + \beta^{2^{k+1}} + 2 \cdot (\alpha \cdot \beta)^{2^k} - 2 \\
&= \alpha^{2^{k+1}} + \beta^{2^{k+1}}.
\end{aligned}$$

$\square$ (Lemma)

Using Lemma 2.1 we are now able to prove the rest of the Proposition:

First assume that n is prime. Since $m \equiv 1 \bmod 2$, it follows that $n = 2^m - 1 \equiv 1 \bmod 3$ and because $m \geq 3$ we have $n \equiv -1 \bmod 8$. Then we use the law of quadratic reciprocity which tells us that

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = (-1)^{(n-1)(n+1)/8} = 1$$

and

$$\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right) \cdot (-1)^{(3-1)(n-1)/4} = \left(\frac{1}{3}\right) \cdot (-1) = -1.$$

Hence $\left(\frac{6}{n}\right) = -1$.

Coming back to the field A we remark that there are only two possibilities for the field A: Either A has only n elements, which is true if and only if $g(x)$ has a root in A or A has n^2 elements which is true if $g(x)$ has no root in A. Now $g(x)$ has a root in A if and only if its discriminant is a square in A. The discriminant of $g(x)$ is $\overline{6}$, but since $\left(\frac{6}{n}\right) = -1$, $\overline{6}$ is not a square in A. Hence A must be a field of n^2 elements and

$$\begin{array}{ccc} A & \longrightarrow & A, \\ \gamma & \longmapsto & \gamma^n \end{array}$$

is a non trivial automorphism of A. Automorphisms map zeros of $g(x)$ onto zeros of $g(x)$ and thus $\alpha^n = \beta$ and $\beta^n = \alpha$. Hence $\beta^{n+1} = \alpha^{n+1} = \alpha \cdot \beta = -\overline{1}$ and we have by Lemma 2.1

$$\begin{aligned} \overline{e}_{m-1}^2 &= \left(\alpha^{2^{m-1}} + \beta^{2^{m-1}}\right)^2 \\ &= \alpha^{2^m} + \beta^{2^m} + \overline{2} \cdot (\alpha \cdot \beta)^{2^{m-1}} \\ &= \alpha^{n+1} + \beta^{n+1} + \overline{2} \\ &= \overline{0}. \end{aligned}$$

This shows that $n \mid e_{m-1}^2$, but since n is prime this also means that $n \mid e_{m-1}$.

Conversely, let us assume that $e_{m-1} \equiv 0 \bmod n$. Then by Lemma 2.1 and since $\alpha \cdot \beta = -\overline{1}$ we have

$$\alpha^{2^{m-1}} = -\beta^{2^{m-1}} = -\alpha^{-2^{m-1}}.$$

This shows that $\alpha^{2^m} = -1$ and $\alpha^{2^{m+1}} = 1$. We now apply Proposition 2.4 with $s = 2^{m+1}$ and $t = 2$. The assertion of this Proposition implies that for every divisor r of n we have $r \equiv n^i \bmod s$ for some $i \in \mathbb{Z}_{\geq 1}$. Since

$$n^2 \equiv 2^{2m} - 2^{m+1} + 1 \equiv 1 \bmod s,$$

this implies that either $r \equiv 1 \bmod s$ or $r \equiv n \bmod s$. But $|r| \leq n$ and $s > 2 \cdot n$ and so

$$\max\{r - 1\ ,\ |r - n|\} < s$$

and we have proved that n is prime. $\square$

Proposition 2.5 provides a very efficient test for Mersenne primes. There are similar tests for numbers of similar shape. However, the Lucas-Lehmer test for Mersenne primes so produced the largest known prime numbers. Here is a table of Mersenne primes:

p with $2^p - 1$ prime	Discoverer	Year	Machine
19	Cataldi	1588	-
31	Euler	1722	-
61	Pervushin	1883	-
89	Powers	1911	-
107	Powers	1911	-
127	Lucas	1876	-
521 607 1279 2203 2281	Lehmer-Robinson	1952	SWAC
3217	Riesel	1957	BESK
4253 4423	Hurwitz-Selfridge	1961	IBM 7090
9689 9941 11213	Gilles	1963	ILIAC 2
19937	Tuckerman	1971	IBM 360
21701	Nickel-Noll	1978	CYBER 174
23209	Noll	1978	CYBER 174
44497	Slowinsky-Nelson	1979	CRAY-1
86243	Slowinsky	1982	CRAY
216091	Slowinsky	1985	CRAY-XMP
756839	Cray	1992	CRAY 2

The last of those numbers has 227832 digits.

Chapter 3

Primality proving with elliptic curves

We remark that the problem of the algorithm which is based on Pocklington's theorem is the following: Once we fail to find a divisor s of $n-1$ for the probable prime n which satisfies the assumptions of Pocklington's theorem, the algorithm fails to work. Because we are working in the group $(\mathbb{Z}/n\mathbb{Z})^*$ the order of the group is fixed with n. If we fail we have no chance to change the underlaying group. As in the elliptic curve factoring method it is useful to replace the group of primitive residues modulo n by the group of points of an elliptic curve modulo n. This leads to the elliptic curve primality proving algorithm which is the goal of this chapter.

3.1 Elliptic curves over rings

We first introduce elliptic curves over rings. Assume that $6 \not| \; n$. Let $a, b \in \mathbb{Z}$ and assume that for $\Delta = 4a^3 + 27b^2$ we have $\gcd(\Delta, n) = 1$. Consider the congruence

$$y^2 \cdot z \quad \equiv \quad x^3 + \overline{a} \cdot x \cdot z^2 + \overline{b} \cdot z^3 \bmod n \tag{3.1}$$

and the set

$$\mathbb{E}'_n \quad = \quad \left\{ (\overline{x}, \overline{y}, \overline{z}) \in (\mathbb{Z}/n\mathbb{Z})^3 \mid (x, y, z) \text{ satisfy } (3.1) \right\}.$$

Given any $\overline{u} \in (\mathbb{Z}/n\mathbb{Z})^*$ we see that the map

$$\begin{array}{rcl} \mathbb{E}'_n & \longrightarrow & \mathbb{E}'_n \\ (\overline{x}, \overline{y}, \overline{z}) & \longmapsto & (\overline{u} \cdot \overline{x}, \overline{u} \cdot \overline{y}, \overline{u} \cdot \overline{z}) \end{array}$$

is a bijection of $\mathbb{E}'_n$ onto $\mathbb{E}'_n$. We therefore introduce an equivalence relation on $\mathbb{E}'_n$ by writing for $(\overline{x}, \overline{y}, \overline{z})$, $(\overline{x}', \overline{y}', \overline{z}') \in \mathbb{E}'_n$

$$(\overline{x}, \overline{y}, \overline{z}) \sim (\overline{x}', \overline{y}', \overline{z}') \quad \Leftrightarrow \quad \exists\, \overline{u} \in (\mathbb{Z}/n\mathbb{Z})^* : \; (\overline{x}, \overline{y}, \overline{z}) \; = \; (\overline{u} \cdot \overline{x}', \overline{u} \cdot \overline{y}', \overline{u} \cdot \overline{z}').$$

Denote by $\mathbb{E}_n$ the set of equivalence classes of $\mathbb{E}'_n$ and the equivalence class of an element $(\overline{x}, \overline{y}, \overline{z})$ by $(\overline{x}\colon \overline{y}\colon \overline{z})$.

In section 3.3 we will introduce on $\mathbb{E}_n$ an addition with zero element $O := (\overline{0}\colon \overline{1}\colon \overline{0})$. Together with this addition, $\mathbb{E}_n$ becomes the abelian **group of points on the elliptic curve** $(\overline{a}, \overline{b})$.

3.2 Analogue to Pocklington's theorem

The idea of the Goldwasser-Kilian-Atkin test is to replace $(\mathbb{Z}/n\mathbb{Z})^*$ in the Pocklington test by the group $\mathbb{E}_n$. As in the elliptic curve factoring method the use of the group of points $\mathbb{E}_n$ opens the possibility of varying the group order by varying the elliptic curve.

In the following we denote by $\mathbb{E}_m$ the group of points of the elliptic curve $\mathbb{E}$ over the ring $\mathbb{Z}/m\mathbb{Z}$. In the same way we will denote points. Then we can formulate the following analogue of Pocklington's theorem, which is the theoretical base of the Goldwasser-Kilian-Atkin test.

Proposition 3.1 *Let $n \in \mathbb{Z}$ with $\gcd(6, n) = 1$ and let $\mathbb{E}_n$ be the group of points on an elliptic curve $\mathbb{E}$ over $\mathbb{Z}/n\mathbb{Z}$. Let m and s be two integers such that $s \mid m$. Suppose we have found a point P_n on $\mathbb{E}_n$ that satisfies*

$$m \cdot P_n \;=\; O_n \quad \textit{and} \quad \frac{m}{q} \cdot P_n \;=\; (\overline{x}\colon \overline{y}\colon \overline{1}) \quad \textit{for every prime factor } q \textit{ of } s.$$

Then for every prime divisor p of n we have $|\mathbb{E}_p| \equiv 0 \bmod s$.

Proof: Let p be a prime divisor of n. We set $Q_n = \left(\frac{m}{s}\right) \cdot P_n$. Then we have $s \cdot Q_n = O_n$ and, because $Q_p = (Q_n)_p \in \mathbb{E}_p$, we see that $s \cdot Q_p = O_p$. Hereby we write $(Q_n)_p$ for reducing the coordinates of the point Q_n modulo p. Since for every prime divisor q of s we have by assumption

$$\left(\frac{s}{q}\right) \cdot Q_p \;=\; \left(\frac{s \cdot m}{q \cdot s}\right) \cdot P_p \;=\; \left(\frac{m}{q}\right) \cdot P_p \;=\; (\overline{x} : \overline{y} : \overline{1})_p \;\neq\; O_p,$$

we see that the order of Q_p in $\mathbb{E}_p$ is precisely s. But the order of an element divides the group order which proves our assertion. □

In the practical use of the primality test the integer m will be the number of points on $\mathbb{E}_n$. For estimating the size of the groups $\mathbb{E}_n$ we use the famous theorem of Hasse.

Proposition 3.2 *Let p be a prime number and $\mathbb{E}_p$ an elliptic curve modulo p. Then*

$$|\mathbb{E}_p| \;=\; p + 1 + t \quad \textit{with} \quad |t| \;\leq\; 2\sqrt{p}.$$

Proof: [Si86] □

The proof that n really is a prime number can now be accomplished by the following Proposition.

Proposition 3.3 *If under the assumptions of Proposition 3.1 we have $s > (\sqrt[4]{n}+1)^2$, then n is a prime number.*

Proof: If n is not a prime number, then there is a prime divisor p of n with $p \leq \sqrt{n}$. Hence, we have by Proposition 3.1 and Hasse's theorem

$$s \;\leq\; |\mathbb{E}_p| \;\leq\; p+1+2\sqrt{p} \;=\; (\sqrt{p}+1)^2 \;\leq\; (\sqrt[4]{n}+1)^2,$$

which is a contradiction. □

The Goldwasser-Kilian-Atkin primality proving test is based on this Proposition. Before we can formulate the algorithm we have to give solutions for some problems: we have not yet said how we actually compute in the group of points of an elliptic curve, i.e. how we add two points. Further we have not yet said how to find a suitable number m. The number of points can be computed by the algorithm of Schoof ([Scho85]), but this algorithm is in practice extremly slow. But there is a solution to our problem: we compute a "suitable" order and try to find an elliptic curve such that the group of points possesses exactly this order. This can be done if we restrict to special elliptic curves, the so called elliptic curves with complex multiplication. In the following sections we give a more detailled description of the solutions for these problems.

3.3 Addition on elliptic curves

Let $P_n = (\overline{x}\colon\overline{y}\colon\overline{z})$ be a non zero point on the elliptic curve $\mathbb{E}_n$. P_n can be written in the form $P_n = (\overline{x}'\colon\overline{y}'\colon\overline{1})$ if and only if $\gcd(z,n) = 1$. We will be only concerned with non zero points of such a form, because otherwise we would have found a non trivial factor of n. Moreover if n really is a prime number, then every non zero point is of this form because then $\mathbb{Z}/n\mathbb{Z}$ is a field. These points can also be written as $P_n = (\overline{x},\overline{y})$ and their coordinates satisfy the inhomogenous congruence

$$y^2 \;\equiv\; x^3 + a\cdot x + b \bmod n.$$

In the following we will use this representation for the equation of an elliptic curve. More generally, if $\mathbb{F}$ is a field of characteristic different from 2 or 3 and if a, $b \in \mathbb{F}$, then the set of all $(x,y) \in \mathbb{F}^2$ satisfying

$$\mathbb{E}: \qquad y^2 \;=\; x^3 + a\cdot x + b$$

together with a single point denoted by $O = O_{\mathbb{E}}$ is called the **set of points** $\mathbb{E}_{\mathbb{F}}$ of the elliptic curve $\mathbb{E}$. O is called the **point at infinity**. It can be shown that this set forms an abelian (commonly additively written) group ([Si86]).

In order to explain the group law we consider the case where $\mathbb{F} = \mathbb{R}$. Let $\mathbb{E}_{\mathbb{R}}$ be the group of points of an elliptic curve over $\mathbb{R}$, for example the set of points on the elliptic curve

$$\mathbb{E}: \quad y^2 = x^3 - 10 \cdot x + 10.$$

The graph of this special elliptic curve can be seen in figure 3.1. The group law can be explained geometrically:

(1) O is the neutral element in $\mathbb{E}_{\mathbb{R}}$ and so we set $-O = O$ and for any $P \in \mathbb{E}_{\mathbb{R}}$ we define $P + O = P$.

(2) For $O \neq P = (x, y)$ we define $-P = (x, -y)$.

(3) If $Q = -P$ set $P + Q = O$.

(4) If P, $Q \in \mathbb{E}_{\mathbb{R}}$ have different x-coordinates, then the line through P and Q intersects the curve in exactly one more point R (unless that line is tangent to the curve at P, in which case take $R = P$ or at Q, in which case take $R = Q$). Then define $P + Q$ to be $-R$.

(5) If $P = Q$, let l be the tangent line to the curve at P. Let R be the only other intersection of l with the curve and define $P + Q = -R$.

An illustration of these geometric rules can also be seen in figure 3.1. From these geometric rules we can obtain formulas for the group law.

Suppose there are given two non zero points $P_i = (x_i,\ y_i)$, $i = 1, 2$. We present only the formulas for the "interesting" cases of the point addition:

If $x_1 = x_2$ and $y_1 = y_2$, i.e. $P_2 = P_1$, set

$$\lambda = \frac{3 \cdot x_1^2 + a}{2 \cdot y_1},$$

if $x_1 \neq x_2$ and so $P_2 \neq \pm P_1$, set

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}.$$

Then compute $P_3 = P_1 + P_2 := (x_3, -y_3)$ with

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

Remark: These addition formulas are valid for all fields with characteristic $\neq 2, 3$. In our application we are working with elliptic curves over $\mathbb{Z}/n\mathbb{Z}$, where we do not know

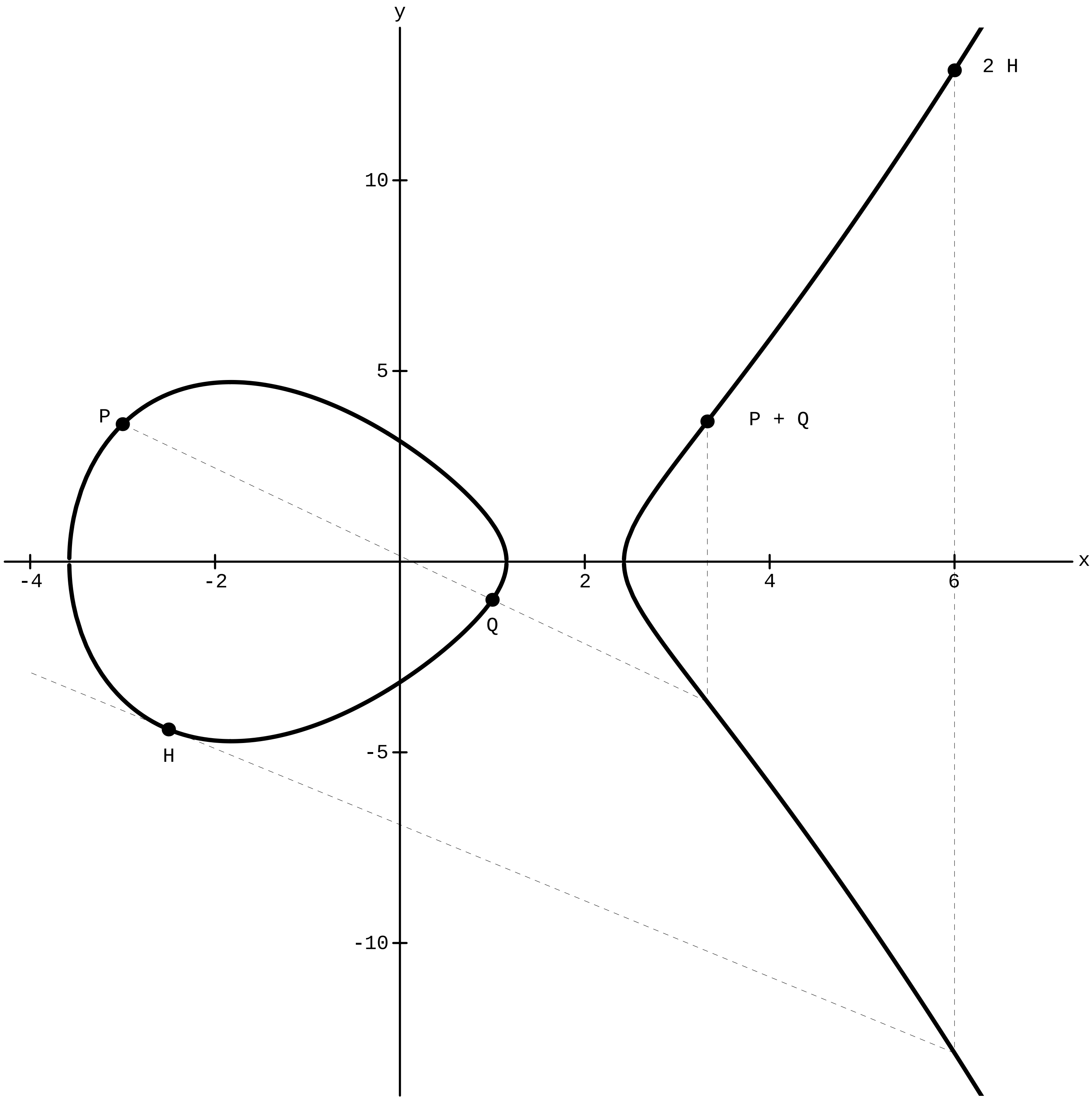

Figure3.1: Elliptic curve $y^2 = x^3 - 10 \cdot x + 10$ over $\mathbb{R}$

whether this is a field. On the contrary this shall be proved. But we can for two points of the form (x_1, y_1) and (x_2, y_2) try to determine the sum $P_3 = (x_3, y_3)$ by means of the addition formulas given above. This fails if and only if either $x_1 - x_2$ or $2 \cdot y_1$ is not invertible in $\mathbb{Z}/n\mathbb{Z}$. But then one has found a nontrivial divisor of n and n can't be a prime number.

Algorithm 3.1 (Addition on elliptic curves)

Input: $\mathbb{E}_n : \ y^2 \ = \ x^3 + a \cdot x + b \bmod n$ *and* $P_1 = (x_1, y_1), \ P_2 = (x_2, y_2) \in \mathbb{E}_n$.

Output: $P_3 \ = \ P_1 + P_2 \in \mathbb{E}_n$ *or a divisor* $d > 1$ *of* n.

1. *If* $P_1 = O$ *return* P_2*; if* $P_2 = O$ *return* P_1.
2. *If* $x_1 \ = \ x_2$ *and* $y_1 \ = -\, y_2$, *set* $P_3 = O$ *and return.*
3. *If* $x_1 \neq x_2$, *goto (3a), else goto (3b).*

   (3a) Determine by the extended euclidean algorithm $s, t \in \mathbb{Z}$ *such that*

   $$s \cdot (x_1 - x_2) + t \cdot n \ = \ d \ = \ \gcd(x_1 - x_2, n).$$

   If $d > 1$, *stop with divisor* d. *Else set* $\lambda \ = \ s \cdot (y_1 - y_2)$.

   (3b) Determine by the extended euclidean algorithm $s, t \in \mathbb{Z}$ *such that*

   $$2 \cdot s \cdot y_1 + t \cdot n \ = \ d \ = \ \gcd(2 \cdot y_1, n).$$

   If $d > 1$, *stop with divisor* d. *Else set* $\lambda \ = \ s \cdot (3 \cdot x_1^2 + a)$.
4. *Set* $x_3 \ \equiv \ \lambda^2 - x_1 - x_2 \bmod n$ *and* $y_3 \ \equiv \ \lambda \cdot (x_3 - x_1) + y_1 \bmod n$ *and return the point* $P_3 \ = \ (x_3, -y_3)$.

Using this algorithm and a variant of the fast exponentiation we can compute in the group of points of an elliptic curve. There remains the problem to find a suitable number m and an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ with order m (under the assumption that n is prime). Therefore we use elliptic curves with complex multiplication. For understanding the computation of such elliptic curves we need some background in algebraic number theory. In the next section we introduce the necessary details.

3.4 Quadratic orders

Let $D \in \mathbb{Z}$, $D \equiv 0, 1 \bmod 4$ and D not a square in $\mathbb{Z}$. Set

$$\omega \ = \ \frac{D + \sqrt{D}}{2}.$$

Then the **quadratic order of discriminant** D is defined as

$$\mathcal{O} \;=\; \mathcal{O}_D \;=\; \mathbb{Z}[\omega] \;=\; \{x + y \cdot \omega \mid x,\, y \in \mathbb{Z}\}.$$

It can be shown that $\mathcal{O}$ is a domain with quotient field

$$\mathbb{K} \;=\; \mathbb{K}_D \;=\; \mathbb{Q}(\sqrt{D}) \;=\; \{x + y \cdot \sqrt{D} \mid x,\, y \in \mathbb{Q}\}.$$

Such a field $\mathbb{K}$ is called a **quadratic number field**. D is called the **discriminant** of the field $\mathbb{K}$.

An **invertible ideal** $\mathcal{A}$ of $\mathcal{O}$ is a subset $\mathcal{A}$ of $\mathbb{K}$ of the form

$$\mathcal{A} \;=\; \alpha \cdot \left(\mathbb{Z} \cdot a + \mathbb{Z} \cdot \frac{b + \sqrt{D}}{2} \right)$$

with $\alpha \in \mathbb{K}^*,\ a, b \in \mathbb{Z},\ a > 0,\ c = \frac{b^2 - D}{4a} \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$.

Example 3.1 *The set* $\mathcal{O} = \mathbb{Z} + \mathbb{Z} \cdot \frac{D + \sqrt{D}}{2}$ *is an invertible ideal of* $\mathcal{O}$ *itself with* $a = 1,\ b = D$ *and* $\alpha = 1$.

Two ideals $\mathcal{A}$, $\mathcal{A}'$ are called **equivalent** if $\mathcal{A} = \mathcal{A}' \cdot \gamma$ with a $\gamma \in \mathbb{K}^*$. We will now consider the case where $D < 0$ and we will present an algorithm which for any invertible ideal

$$\mathcal{A} = \mathbb{Z} \cdot a + \mathbb{Z} \cdot \frac{b + \sqrt{D}}{2}$$

computes a **reduced ideal** equivalent to the ideal $\mathcal{A}$. A reduced ideal is defined by the properties

$$|b| \le a \le c \qquad \text{and} \qquad b \ge 0 \quad \text{if } |b| = a \ \text{ or } \ a = c. \tag{3.2}$$

Note that equivalent ideals have the same discriminant $D = b^2 - 4 \cdot a \cdot c$. The reduction algorithm consists of two steps. Firstly, b is replaced by $b + 2 \cdot m \cdot a$ with an appropriate $m \in \mathbb{Z}$ such that $b \in \{-a, \ldots, a\}$. This does not change $\mathcal{A}$ and might reveal that $\mathcal{A}$ is reduced. Then the algorithm terminates. The only reason for $\mathcal{A}$ not being reduced at this stage can be $c < a$ or b having the wrong sign. Then we multiply $\mathcal{A}$ by $\gamma = \frac{2 \cdot c}{b + \sqrt{D}}$. Thus we get

$$\frac{b + \sqrt{D}}{2} \cdot \gamma \;=\; c \quad \text{and} \quad a \cdot \gamma \;=\; a \cdot \frac{2 \cdot c}{b + \sqrt{D}} \;=\; \frac{2 \cdot a \cdot c \cdot (b - \sqrt{D})}{b^2 - D} \;=\; \frac{b - \sqrt{D}}{2}.$$

This means that a was replaced by c and b by $-b$. If the ideal is not yet reduced, repeat the first step. In the algorithm we denote an ideal $\mathcal{A} = \mathbb{Z} \cdot a + \mathbb{Z} \cdot \frac{b + \sqrt{D}}{2}$ by the tripel (a, b, c) with $c = \frac{b^2 - D}{4 \cdot a}$.

Algorithm 3.2 (Reduction of ideals)

Input: *ideal* $\mathcal{A} = (a, b, c)$.
Output: *reduced ideal equivalent to* $\mathcal{A}$.

1. *Replace* b *by* $b + 2 \cdot m \cdot a$ *with* m *such that* $-a \leq b + 2 \cdot m \cdot a \leq a$.

2. *If* (a, b, c) *is not reduced, then replace* (a, b, c) *by* $(c, -b, a)$ *and goto 1.*

3. *Return ideal* (a, b, c).

It can be shown that no more than $O\left(\max\left\{1, \log \frac{|a|}{\sqrt{|D|}}\right\}\right)$ iterations of those two steps are necessary to reduce an ideal $\mathcal{A} = \mathbb{Z} \cdot a + \mathbb{Z} \cdot \frac{b+\sqrt{D}}{2} = \left(a, b, \frac{b^2-D}{4 \cdot a}\right)$. It can also be shown that the reduced ideal in an equivalence class is uniquely determined. Moreover, it can be proved that for reduced ideals (a, b, c) we have

$$0 < a < \sqrt{\frac{|D|}{3}}. \tag{3.3}$$

By (3.2) and (3.3) it is possible to find a full system of representatives for all invertible ideals in a finite number of steps.

Example 3.2 *Let* $D = -7$. *Then by (3.3) we must choose* a *only in the range* $0 < a < \sqrt{7/3} < 1.6$. *So the only possible value for* a *is* $a = 1$. *Then the only possible values for* b *are* $b = 0$ *and* $b = 1$. *For any value of* b *we must check whether* c *is an element of* $\mathbb{Z}$, *i.e. whether* $4 \cdot a = 4$ *divides* $b^2 - D$. *For* $b = 0$ *we get* $b^2 - D = 7$ *which is not divisible by* 4. *For* $b = 1$ *we have* $b^2 - D = 1 - (-7) = 8$. *So* $b^2 - D$ *is divisible by* 4 *and we get* $c = 2$ *which is also compatible with (3.2). Thus we have found precisely one reduced ideal, namely*

$$\mathcal{A} = \mathbb{Z} + \mathbb{Z} \cdot \frac{1 + \sqrt{-7}}{2}$$

and it is easy to verify that $\mathcal{A} = \mathcal{O}_{-7}$.

The equivalence classes of invertible ideals also form a group, the **class group** $H = H_D$. The order of this group H is called the **class number** of $\mathcal{O}$ and denoted by $h = h_D$. So we know how to find a complete system of representatives for the class group of $\mathcal{O}$ if D is not too large. We remark that this problem becomes much more difficult for $D > 0$.

For determining elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ with complex

multiplication we must find a number in $\mathcal{O}$ of 'norm' n. Thereby we assume that n is a conjectural prime number. Before we give an algorithm which solves the problem of finding such a number we present the necessary theoretical background:

For any $\xi = x + y \cdot \sqrt{D} \in \mathbb{K}$ we call $\xi' = x - y \cdot \sqrt{D} \in \mathbb{K}$ the **(algebraic) conjugate** of ξ. The **norm** of a number ξ is defined as

$$N(\xi) \; := \; \xi \cdot \xi' \; = \; x^2 - y^2 \cdot D$$

and the **trace** of ξ as

$$Tr(\xi) \;:=\; \xi + \xi' \;=\; 2 \cdot x.$$

Note that norm and trace of algebraic numbers (i.e. numbers in $\mathbb{K}$) are rationals. Also note that

$$(x - \xi) \cdot (x - \xi') \;=\; x^2 - Tr(\xi) \cdot x + N(\xi).$$

So ξ and ξ' are both zeros of the same polynomial with rational coefficients. Moreover if ξ belongs to the order $\mathcal{O}$, then both its norm and trace are rational integers. In fact, if $\xi = x + y \cdot \omega$ with $x,\, y \in \mathbb{Z}$, then

$$Tr(\xi) \;=\; 2 \cdot x + y \cdot D$$

and

$$N(\xi) \;=\; \left(x + \frac{y}{2} \cdot D\right)^2 - \left(\frac{y}{2}\right)^2 \cdot D \;=\; x^2 + x \cdot y \cdot D + y^2 \cdot \frac{D \cdot (D-1)}{4}. \tag{3.4}$$

From the last equation we see that for $D < 0$ the norm of $\xi \neq 0$ always is positive. But how can we compute a number in $\mathcal{O}$ with norm n? And is it always guaranteed that such a number exists? We immediately see by the norm formula (3.4) that not every rational integer n can be written as a norm of an element in $\mathcal{O}$, but only those for which the diophantine equation

$$4 \cdot n \;=\; 4 \cdot x^2 + 4 \cdot x \cdot y \cdot D + y^2 \cdot D^2 - y^2 \cdot D \;=\; (2 \cdot x + y \cdot D)^2 - y^2 \cdot D \tag{3.5}$$

has a solution $(x, y) \in \mathbb{Z}^2$. So a necessary condition for the solvability of (3.5) is $\left(\frac{D}{n}\right) = 1$.

In order to present an efficient algorithm for determining elements of given norm we introduce a different interpretation for the norm of a number $\beta \in \mathcal{O}$. For this purpose we define the **norm of an invertible ideal** $\mathcal{A} = \alpha \cdot \left(\mathbb{Z} \cdot a + \mathbb{Z} \cdot \frac{b+\sqrt{D}}{2}\right)$ as

$$N(\mathcal{A}) \;=\; |N(\alpha)| \cdot a.$$

Note that $N(\mathcal{O}) = 1$. If the principal ideal $(\beta) = \beta \cdot \mathcal{O}$ is given as

$$\beta \cdot \mathcal{O} \;=\; \beta \cdot \left(\mathbb{Z} + \mathbb{Z} \cdot \frac{D + \sqrt{D}}{2}\right),$$

then we have $N(\beta \cdot \mathcal{O}) \;=\; |N(\beta)| \cdot 1 \;=\; |N(\beta)|$.

It is easily seen that for $\alpha \in \mathcal{O}$ with $(\alpha) = m \cdot \left(\mathbb{Z} \cdot a + \mathbb{Z} \cdot \frac{b+\sqrt{D}}{2}\right)$ with $a, b, m \in \mathbb{Z}$ and $a, m > 0$ we have $|N(\alpha)| = m^2 \cdot a$. Thus there is an element in $\mathcal{O}$ of norm n if there is an integral ideal $\mathbb{Z} \cdot n + \mathbb{Z} \cdot \frac{b+\sqrt{D}}{2}$ in $\mathcal{O}$ of norm $|n|$ which is principal. If $D < 0$, then the norms of all the elements in $\mathcal{O}$ are nonnegative. Hence, the converse of this statement is also true.

A way of solving norm equations is, therefore, to find all the ideals of the norm in question, to check, if one of those ideals is principal, in the case of principality to find a generator and to determine its norm. Let us consider the special case where n is a prime number. Then any invertible ideal

$$\mathcal{A} = \alpha \cdot \left(\mathbb{Z} \cdot a + \mathbb{Z} \cdot \frac{b + \sqrt{D}}{2} \right)$$

of norm n must have $\alpha = 1$ and $a = n$, because for $\alpha = n$ and $a = 1$ we would have $N(\mathcal{A}) = N(\alpha) \cdot 1 = n^2$. Hence, such an ideal exists if and only if there exists $b \in \mathbb{Z}$ such that $4 \cdot n$ divides $b^2 - D$. Because we chose $D \equiv 0, 1 \bmod 4$ this means that D must be a quadratic residue modulo n and b a square root of $D \bmod n$. We can check the existence of b by computing a Legendre symbol and computing a square root modulo n. This can be done with Shanks Algorithm which we present in the next section. Note that this algorithm assumes n to be prime. If an error occurs during the computation of the square root, then n can not be prime.

As soon as we have found an ideal

$$\mathcal{P} \;=\; \mathbb{Z} \cdot n + \mathbb{Z} \cdot \frac{b + \sqrt{D}}{2}$$

with norm n we must decide whether it is principle or not. To be principle means to be in the equivalence class of the invertible ideal $\mathcal{O}$. So we apply the reduction algorithm 3.2 to find an element $\pi \in \mathbb{K}^*$ such that $\frac{1}{\pi} \cdot \mathcal{P}$ is reduced. Analogously find an element $\kappa \in \mathbb{K}^*$ such that $\frac{1}{\kappa} \cdot \mathcal{O}$ is reduced. If $\frac{1}{\pi} \cdot \mathcal{P} = \frac{1}{\kappa} \cdot \mathcal{O}$, then $\mathcal{P} = \frac{\pi}{\kappa} \cdot \mathcal{O}$. So check whether the element $\tau = \frac{\pi}{\kappa} \in \mathcal{O}$. If this condition is fulfilled we have

$$n \;=\; N(\mathcal{P}) \;=\; N(\tau \cdot \mathcal{O}) \;=\; N(\tau),$$

i.e. τ is an element of $\mathcal{O}$ with norm n.

3.5 Square roots modulo p

Suppose that p is a prime number and that $a \in \mathbb{Z}$ is known to be a square modulo p. The order of the group $\mathbb{F}_p^*$ of primitive residues modulo p is $p-1$ and this group is cyclic. Write $p - 1 \;=\; 2^{s_0} \cdot (2 \cdot k + 1)$. Then

$$\mathbb{F}_p^* \;=\; G_1 \times G_2,$$

where $G_1 \;=\; \langle \overline{g}_1 \rangle$ is a cyclic group of order 2^{s_0} and $G_2 \;=\; \langle \overline{g}_2 \rangle$ a cyclic group of order $2 \cdot k + 1$. Hence, $\overline{a}$ can be written as

$$\overline{a} \;=\; \overline{g}_1^{\lambda_1} \cdot \overline{g}_2^{\lambda_2}$$

and since $\overline{a}$ is a square in $\mathbb{F}_p^*$, λ_1 and λ_2 must both be even. If we knew $\overline{g}_1$, $\overline{g}_2$, λ_1, λ_2, then we could easily extract the square root of $\overline{a}$. But those generators and exponents are hard to find.

Suppose for a moment that $\lambda_1 = 0$; so the order of $\overline{a}$ is odd, i.e. $\overline{a}$ belongs to G_2. Then extracting the square root is very easy because we only must put $\overline{r} = \overline{a}^{k+1}$. Then

$$\overline{r}^2 = \overline{a}^{2\cdot k+2} = \overline{a}^{2\cdot k+1} \cdot \overline{a} = \overline{a}.$$

What happens if the order of $\overline{a}$ is not odd? Put

$$\overline{r}_0 = \overline{a}^{k+1} \quad \text{and} \quad \overline{n}_0 = \overline{a}^{2\cdot k+1}.$$

Then we have

$$\overline{r}_i^2 = \overline{a} \cdot \overline{n}_i \quad \text{and} \quad \overline{n}_i \in G_1 \tag{3.6}$$

for $i = 0$. Hence, we have computed an 'approximation' to the square root, the 'error' belongs to G_1 which we can control. If $\overline{n}_0 = \overline{1}$, we are done. Otherwise we compute a generator of G_1: Choose a quadratic non residue z mod p and put

$$\overline{c}_0 = \overline{z}^{2\cdot k+1}.$$

Then $\overline{c}_0$ is a generator for G_1 (Exercise!). Hence we have

$$\overline{n}_0 = \overline{c}_0^{2^{t_0}\cdot(2\cdot m_0-1)}.$$

How to determine t_0? We will always know that in iteration i the order of $\overline{c}_i$ is 2^{s_i} with a number s_i (for $i = 0$ true, because $\overline{c}_0$ generates G_1). Therefore the order of $\overline{n}_i$ is $2^{s_i-t_i}$. If we keep squaring $\overline{n}_i$, we can easily determine $s_i - t_i$ and thus t_i.

Now we want to define $\overline{r}_{i+1}$ such that in (3.6) the new $\overline{n}_{i+1}$ will have a lower order than $\overline{n}_i$. Define

$$\overline{r}_{i+1} = \overline{r}_i \cdot \overline{b}_i \quad \text{and} \quad \overline{b}_i = \overline{c}_i^{2^{t_i-1}}.$$

Then

$$\begin{aligned}\overline{r}_{i+1}^2 &= \overline{a} \cdot \overline{c}_i^{2^{t_i}\cdot(2\cdot m_i-1)} \cdot \overline{c}_i^{2^{t_i}} \\ &= \overline{a} \cdot \overline{c}_i^{2^{t_i+1}\cdot m_i}\end{aligned}$$

and clearly, with $\overline{n}_{i+1} = \overline{n}_i \cdot \overline{b}_i^2$ the order of $\overline{n}_{i+1}$ is at most half the order of $\overline{n}_i$. Finally, we note that for $\overline{c}_{i+1} = \overline{b}_i^2$ (and so $s_{i+1} = s_i - t_i$) we have $\overline{n}_{i+1} \in \langle \overline{c}_{i+1} \rangle$ and $t_{i+1} > 0$ as long as $\overline{n}_{i+1} \neq \overline{1}$ because $\overline{a}$ is a square in $\mathbb{F}_p$. Now we have to iterate this process until $\overline{c}_i = \overline{1}$. Then $\overline{r}_i$ is a square root of $\overline{a}$ modulo p.

3.6 Complex multiplication

In this section we define "complex multiplication". Often we just present facts without proofs; for a detailled description of the theory we refer to the book of Silverman ([Si86]). Then we give a first idea how to compute elliptic curves with complex multiplication. How is this important? We know the following fundamental fact:

An elliptic curve $\mathbb{E}$ has **complex multiplication** by an order O if the endomorphism ring of $\mathbb{E}$ is isomorph to O and greater than $\mathbb{Z}$. If the elliptic curve $\mathbb{E}_n$ has complex multiplication by a quadratic order $\mathcal{O}$ of discriminant $D < 0$ and if n is prime and a norm of an element $\pi \in \mathcal{O}$, i.e. $n = \pi \cdot \pi'$ with the conjugate π' of π, then

$$|\mathbb{E}_n| \;=\; n + 1 - (\pi + \pi').$$

To compute elliptic curves over a finite prime field with complex multiplication by a given order we do the analogous computations for elliptic curves over $\mathbb{C}$. Therefore We will consider first lattices in the field $\mathbb{C}$ of complex numbers and we will show that there is a 1-1 correspondence between those lattices and elliptic curves. A **lattice** L in $\mathbb{C}$ is a subgroup of $\mathbb{C}$ of the form

$$\begin{aligned} L \;&=\; \mathbb{Z} \cdot \omega_1 + \mathbb{Z} \cdot \omega_2 \\ &=\; \{ x \cdot \omega_1 + y \cdot \omega_2 \mid x,\, y \in \mathbb{Z} \}, \end{aligned}$$

where $\omega_1,\, \omega_2 \neq 0$ and $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$.

For a lattice L of $\mathbb{C}$ we define the **Weierstraß $\wp$-function** as

$$\begin{array}{ccl} \mathbb{C}\backslash \mathrm{L} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \wp(z) = \frac{1}{z^2} + \sum\limits_{l \in L,\, l \neq 0} \left(\frac{1}{(z-l)^2} + \frac{1}{l^2} \right). \end{array}$$

(Of course, one has to prove appropriate convergence for the series on the right hand side, but this will be taken for granted here.)

The Weierstraß $\wp$-function has very nice properties. It is 'meromorphic', in particular we can form the derivative

$$\wp'(z) \;=\; -2 \cdot \sum_{l \in L} \frac{1}{(z-l)^3}$$

and both the $\wp$-function and its derivative are periodic on L, i.e. we have for every $z \in \mathbb{C}\backslash L$ and for every $l \in L$

$$\wp(z+l) \;=\; \wp(z) \quad \text{and} \quad \wp'(z+l) \;=\; \wp'(z).$$

Finally, $\wp(z)$ satisfies the differential equation

$$\wp'^2(z) \;=\; 4 \cdot \wp(z)^3 - g_2(L) \cdot \wp(z) - g_3(L),$$

where $g_2(L),\, g_3(L) \in \mathbb{C}$. The discriminant of the cubic polynomial on the right hand side is non zero. We immediately see the connection with elliptic curves: Consider the equation

$$y^2 \;=\; 4 \cdot x^3 - g_2(L) \cdot x - g_3(L).$$

This equation defines an elliptic curve $\mathbb{E}_L$ over $\mathbb{C}$ (we can use a variable substitution to transform this equation into the normal form $y^2 = x^3 + a \cdot x + b$). Conversely, if we are given an elliptic curve $\mathbb{E}$ over $\mathbb{C}$ by the Weierstraß equation $y^2 = 4 \cdot x^3 - a_2 \cdot x - a_3$ then we consider the differential equation

$$\wp'(z)^2 = 4 \cdot \wp(z)^3 - a_2 \cdot \wp(z) - a_3.$$

Its solution is a Weierstraß $\wp$-function with a period lattice $L_{\mathbb{E}}$ and we have $\mathbb{E}_{L_{\mathbb{E}}} = \mathbb{E}$.

Hence, there is a 1-1 correspondence between the lattices in $\mathbb{C}$ and elliptic curves over $\mathbb{C}$. Elliptic curves come from the differential equation of a $\wp$-function of a lattice. Lattices are period lattices of the $\wp$-function which solves an elliptic differential equation.

Theorem 3.1 *Let L be a lattice in $\mathbb{C}$. Then the map*

$$\begin{array}{l} \mathbb{C} \longrightarrow \mathbb{E}_L \\ z \longmapsto \begin{cases} (\wp(z), \wp'(z)) & \text{if } z \notin L \\ O_{\mathbb{E}_L} & \text{otherwise} \end{cases} \end{array}$$

is an epimorphism with kernel L.

As a consequence, $\mathbb{C}/L$ is isomorphic to the group of points on $\mathbb{E}_L$. This provides us with a very simple addition law for points which are given as $P = (\wp(z), \wp'(z))$.

We now observe that for a lattice L in $\mathbb{C}$ and an element $\gamma \in \mathbb{C}^*$ the map

$$\begin{array}{ccc} \mathbb{C}\big/L & \longrightarrow & \mathbb{C}\big/\gamma \cdot L \\ z + L & \longmapsto & \gamma \cdot z + \gamma \cdot L \end{array}$$

is an (well defined) isomorphism of groups. Hence, the elliptic curves $\mathbb{E}_L$ and $\mathbb{E}_{\gamma \cdot L}$ are isomorphic. We can ask which of those isomorphisms map L to L, i.e. which isomorphisms are, in fact, automorphisms. Every number $\gamma \in \mathbb{C}$ with $\gamma \cdot L \subseteq L$ is called a **multiplier** of L. Non zero multipliers of L induce automorphisms of $\mathbb{E}_L$. The multipliers of L form a commutative ring with unit element and it can be shown that this ring is either $\mathbb{Z}$ or an imaginary quadratic order $\mathcal{O}$. In the latter case, $\mathbb{E}_L$ is said to have **complex multiplication** by this order $\mathcal{O}$.

Isomorphism is an equivalence relation and "to have complex multiplication by $\mathcal{O}$" is a property of an isomorphism class, i.e. an elliptic curve has complex multiplication by $\mathcal{O}$ if and only if any elliptic curve in its isomorphism class has complex multiplication by $\mathcal{O}$. We want to exhibit one representative of each isomorphism class which has complex multiplication by an order $\mathcal{O}$. Without loss of generality, this representative can be chosen as

$$L = \mathbb{Z} + \mathbb{Z} \cdot \gamma$$

with $\gamma \in \mathbb{C}^*$. Since the order $\mathcal{O}$ is the ring of multipliers of L, it follows that L is an invertible ideal of $\mathcal{O}$. Moreover, two curves are isomorphic if the corresponding lattices, which are now discovered to be invertible ideals, are equivalent. So we can pick the reduced (ideal) representative

$$L = \mathbb{Z} + \mathbb{Z} \cdot \frac{b + \sqrt{D}}{2 \cdot a}$$

for each equivalence class and for any such L the corresponding curve over $\mathbb{C}$ has complex multiplication by $\mathcal{O}$.

But what we need for primality proving are elliptic curves defined over $\mathbb{Z}/n\mathbb{Z}$ which have complex multiplication by $\mathcal{O}$. In this case, complex multiplication is a little bit harder to define. But there is a close connection between elliptic curves over $\mathbb{C}$ and elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ which have complex multiplication.

For an elliptic curve $\mathbb{E}: \; y^2 \;=\; 4 \cdot x^3 - a \cdot x - b$ defined over a field $\mathbb{K}$ we define the **j-invariant** as

$$j(\mathbb{E}) \quad = \quad 2^6 \cdot 3^3 \cdot \frac{a^3}{a^3 - 27 \cdot b^2}.$$

The j-invariant is in fact an invariant of the isomorphy class of an elliptic curve.

So take a full system of representatives $L_1, \ldots, L_h$ of lattices in $\mathbb{C}$ with complex multiplication by $\mathcal{O}$. This means to choose a full system of representatives for the class group H. Then the **Hilbert polynomial**

$$G(x) \quad = \quad \prod_{i=1}^{h} (x - j(\mathbb{E}_{L_i}))$$

has integer coefficients. If n is a prime number and a norm in $\mathcal{O}$, then $G(x) \bmod n$ is a product of linear factors

$$G(x) \quad \equiv \quad \prod_{i=1}^{h} (x - j_i) \bmod n$$

and the $j_i \bmod n$ are the j-invariants of all elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ which have complex multiplication by $\mathcal{O}$. Hence, if we know $G(x)$, we can factor $G(x)$ over $\mathbb{Z}/n\mathbb{Z}$ and obtain the j-invariants of all elliptic curves over $\mathbb{Z}/n\mathbb{Z}$ with complex multiplication by $\mathcal{O}$. In practice we just need one root of $G(x) \bmod n$. In the next section we present an algorithm to factor a polynomial modulo a prime number.

3.7 Factoring polynomials over finite prime fields

Let p be a prime number. We will work over the finite prime field $\mathbb{F}_p$. Let $u(x) \in \mathbb{F}_p[x]$ be a monic reducible polynomial. Our goal is to express $u(x)$ in the form

$$u(x) \;=\; p_1(x)^{e_1} \cdot \ldots \cdot p_r(x)^{e_r},$$

where $p_1(x), \ldots, p_r(x)$ are distinct, monic irreducible polynomials.

As a first step, we can use a standard technique to determine whether any of the exponents $e_1, \ldots, e_r$ is greater than one. If $u(x) \;=\; u_n \cdot x^n + \ldots + u_0$ with $u_i \in \mathbb{F}_p$, $0 \leq i \leq n$, then the **derivative** of $u(x)$ is defined as

$$u'(x) \;=\; n \cdot u_n \cdot x^{n-1} + (n-1) \cdot u_{n-1} \cdot x^{n-2} + \ldots + u_1.$$

Proposition 3.4 *If* $u(x) = v(x)^2 \cdot w(x)$ *with* $v(x), w(x) \in \mathbb{F}_p[x]$, *then we have*

$$u'(x) = v(x) \cdot (2 \cdot v'(x) \cdot w(x) + v(x) \cdot w'(x)).$$

Proof: Exercise. □

By Proposition 3.4 we see that any polynomial whose square divides $u(x)$ must also divide $u'(x)$ and so the gcd of $u(x)$ and $u'(x)$. How to compute polynomial gcd's? Since $\mathbb{F}_p[x]$ is an euclidean domain with respect to the degree, we can use euclids algorithm. For division with remainder of polynomials we refer to the book of Knuth ([Kn81]). We illustrate the computation of a polynomial gcd by an example:

Example 3.3 *Let* $p = 3$ *and* $u(x) \equiv x^3 - x^2 - x + 1 \bmod 3$. *We want to determine the square factors of* $u(x) \bmod 3$. *For this purpose we form* $u'(x) \equiv x - 1 \bmod 3$. *Now we must find* $\gcd(u(x), u'(x)) = \gcd(x^3 - x^2 - x + 1, x - 1)$. *Division with remainder leads to* $u(x) = (x^2 - 1) \cdot u'(x) + 0$. *Hence, we have* $\gcd(u(x),\ u'(x)) = x - 1$ *and so* $(x-1)^2$ *is a divisor of* $u(x)$. *In fact, we have*

$$u(x) = (x-1)^2 \cdot (x+1),$$

which is already the complete factorization of $u(x)$.

After computing $d(x) = \gcd(u(x), u'(x))$ we either have $d(x) = 1$ in which case $u(x)$ is a square free polynomial or $d(x) = u(x)$ or $d(x) \neq 1, u(x)$. In the last case we have found a proper divisor of $u(x)$ and $\frac{u(x)}{d(x)}$ is square free. Finally, if $d(x) = u(x)$, then $u'(x) = 0$ which means that $u_k \neq 0$ if and only if k is a multiple of p. In this case we have

$$u(x) \equiv (v(x))^p \bmod p$$

with $v(x) \in \mathbb{F}_p[x]$ which is also a non trivial factorization of $u(x)$. The practical computation of $v(x)$ is left as an exercise.

Iterating this process, we can come up with a factorization of $u(x)$ which is of the form

$$u(x) = \prod_{i=1}^{k} (u_i(x))^i, \tag{3.7}$$

where $u_i(x) \in \mathbb{F}_p[x]$ is a squarefree polynomial for $1 \leq i \leq k$. So the problem of factoring a polynomial reduces to the problem of factoring a squarefree polynomial. Let us therefore assume that

$$u(x) = p_1(x) \cdot p_2(x) \cdot \ldots \cdot p_r(x)$$

is a product of distinct, monic, irreducible polynomials.

Proposition 3.5 *Let $q(x) \in \mathbb{F}_p[x]$ be irreducible and of degree d. Then $q(x)$ is a divisor of $x^{p^d} - x$, but $q(x)$ is not a divisor of $x^{p^c} - x$ for $c < d$.*

The proof of this Proposition is based on the algebraic theory of finite fields and is omitted here ([Hu74]). It can be used to find the product of all the irreducible factors of each degree of $u(x)$.

Algorithm 3.3 (Factorization of a square free polynomial)

Input: *a square free, monic polynomial $u(x) \in \mathbb{F}_p[x]$*
Output: *the product $g_d(x) \in \mathbb{F}_p[x]$ of all the irreducible factors of $u(x)$ of degree d for $1 \le d \le \deg u(x)$.*

1. *Set $v(x) = u(x)$, $w(x) = x$, $d = 0$.*
2. *If $d + 1 > \frac{1}{2} \cdot \deg v(x)$, the procedure terminates since we either have $v(x) = 1$ or $v(x)$ is irreducible.*
   Otherwise increase d by 1 and replace $w(x)$ by $w(x)^p \bmod v(x)$.
3. *Find $g_d(x) = \gcd(w(x) - x, v(x))$.*
4. *If $g_d(x) \neq 1$, replace $v(x)$ by $\frac{v(x)}{g_d(x)}$ and $w(x)$ by $w(x) \bmod v(x)$. Return to step 2..*

For the correctness of this algorithm note that for every d in step 2. we have $w(x) = x^{p^d} \bmod v(x)$ and that all irreducible factors of $v(x)$ are distinct and have degree greater d.

In order to split the polynomials $g_d(x)$ into a product of irreducible polynomials, we use the identity

$$g_d(x) \;=\; \gcd(g_d(x), t(x)) \cdot \gcd\left(g_d(x), t(x)^{(p^d-1)/2} + 1\right) \cdot \gcd\left(g_d(x), t(x)^{(p^d-1)/2} - 1\right)$$

for all polynomials $t(x) \in \mathbb{F}_p[x]$. Since for every $t(x) \in \mathbb{F}_p[x]$ and for every $d \in \mathbb{Z}_{\ge 0}$ the polynomial $t(x)^{p^d} - t(x)$ is a multiple of every irreducible polynomial in $\mathbb{F}_p[x]$ of degree d, we see that there is a good chance that some of the irreducible factors are divisors of $t(x)^{(p^d-1)/2} + 1$, some of $t(x)^{(p^d-1)/2} - 1$ and some of $t(x)$. Applied to our problem, it is sufficient to choose $d = 1$ since we know that the polynomial $G(x)$ can be decomposed into linear factors over $\mathbb{F}_p$.

3.8 Determination of the j-invariants

The situation is now this: We fix a discriminant $D < 0$. Then we determine all reduced ideals of $\mathcal{O}_D$, say $\mathcal{A}_i = \mathbb{Z} + \mathbb{Z} \cdot \frac{b_i + \sqrt{D}}{2 \cdot a_i}$ for $1 \le i \le h$ and we have to determine the j-invariants $j(\mathbb{E}_{\mathcal{A}_i})$ for all $1 \le i \le h$. This last step must now be explained.

For any $\tau \in \mathbb{C}$ with $\Im(\tau) > 0$ and for a lattice $L = \mathbb{Z} + \mathbb{Z} \cdot \tau$ we have

$$j(\mathbb{E}_L) \;=\; j(\tau).$$

Choosing the variable transformation $q = e^{2\pi \cdot i \cdot \tau}$ we obtain

$$j(q) \;=\; 1728 \cdot \frac{E_4^3(q)}{E_4^3(q) - E_6^2(q)}$$

where

$$\begin{aligned} E_4(q) &= 1 + 240 \cdot \sum_{n \geq 1} \sigma_3(n) q^n \\ E_6(q) &= 1 - 504 \cdot \sum_{n \geq 1} \sigma_5(n) q^n \end{aligned}$$

and where

$$\sigma_r(n) \;=\; \sum_{d|n} d^r \qquad \text{for } r \in \mathbb{Z}_{\geq 0},\ n \in \mathbb{Z}_{>0}.$$

The formulas for E_4 and E_6 are called **q-expansions** for E_4 and E_6 and from those q-expansions one can deduce a q-expansion for j which can be used for the calculations. This q-expansion of the j-invariant is known to be of the form

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

In order to be able to compute those coefficients, we make use of the arithmetic with Taylor series. We first compute the denominator and the numerator using the formulas

$$\sum_{i=0}^{\infty} a_i \cdot x^i + \sum_{i=0}^{\infty} b_i \cdot x^i \;=\; \sum_{i=0}^{\infty} (a_i + b_i) \cdot x^i$$

and

$$\left(\sum_{i=0}^{\infty} a_i \cdot x^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i \cdot x^i \right) \;=\; \sum_{i=0}^{\infty} \left(\sum_{j+k=i} a_j \cdot b_k \right) \cdot x^i.$$

Then we determine the quotient

$$\frac{\sum_{i=0}^{\infty} a_i \cdot x^i}{\sum\limits_{i=0}^{\infty} b_i \cdot x^i} \;=\; \sum_{i=0}^{\infty} c_i \cdot x^i$$

by writing

$$a_i \;=\; \sum_{j+k=i} b_j \cdot c_k$$

which will give a recursive method for computing the c_k. If we know "enough" c_k's, we can compute the j-invariants with a special precision (using floating point arithmetic).

3.9 Computing the curves

Suppose we have chosen a discriminant D. We want to find an elliptic curve of the form $y^2 = x^3 + a \cdot x + b$ with complex multiplication by $\mathcal{O}_D$. Its j-invariant is

$$j = 2^6 3^3 \cdot \frac{4 \cdot a^3}{4 \cdot a^3 + 27 \cdot b^2}.$$

Using the methods of the last sections we can compute the j-invariant j_0 of an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ which has complex multiplication by $\mathcal{O}$. But how can we compute the representation of the elliptic curve itself?

Therefore put

$$k \equiv j_0 \cdot (1728 - j_0)^{-1} \bmod n$$

and choose a quadratic non residue $c \in (\mathbb{Z}/n\mathbb{Z})^*$. Then consider the elliptic curves

$$\begin{aligned} \mathbb{E}\colon \quad y^2 &= x^3 + 3 \cdot k \cdot x + 2 \cdot k + 3^3 \\ \mathbb{E}'\colon \quad y^2 &= x^3 + 3 \cdot k \cdot c^2 \cdot x + 2 \cdot k \cdot c^3 \end{aligned}$$

Both elliptic curves have j-invariant j_0. They are not isomorphic and the number of points on it is $m = n + 1 - \pi - \pi'$, $m' = n + 1 + \pi + \pi'$, respectively, where $\pi \in \mathcal{O}_D$ is an element with norm n. Since we do not know whether m is the number of points on $\mathbb{E}$ or on $\mathbb{E}'$, we choose a point P on $\mathbb{E}$ and we determine $m \cdot P$. If $m \cdot P = O$ we are convinced that $|\mathbb{E}| = m$, otherwise we have $|\mathbb{E}'| = m$.

For choosing a random point on an elliptic curve $\mathbb{E} : \; y^2 = x^3 + a \cdot x + b$ we can use the following method: randomly choose a number $x \in \mathbb{F}_n$, compute $d = x^3 + a \cdot x + b$ and test with the Legendre symbol whether d is a square modulo n. If not, choose a new x and iterate the process. Else compute with Shanks RESSOL algorithm a square root y and $P = (x, y)$ is a point of $\mathbb{E}$.

3.10 The elliptic curve primality proving algorithm (ECPP)

In this section we formulate the ECPP-algorithm of Goldwasser-Kilian-Atkin for proving the primality of a number. This algorithm is based on the ideas we stated in the previous sections. Morain has implemented this algorithm and an exact description of its theory and practice can be found in [AtMo90]. In addition he describes a lot of practical improvements for solutions of the partial problems.

Assume that we are "almost" sure that a number n is a prime, i.e. we have done several positive probable prime number tests. Then we try to prove the primality of the number n. The ECCP algorithm uses the so called downrun-strategy: The first part of the algorithm consists of finding (under the assumption that n is prime) a sequence

$$n = N_0 > N_1 > \ldots > N_k$$

of probable primes N_i which are suited for the test. The numbers N_i should fulfill the conditions of proposition 3.1 and 3.3. The sequence of N_i stops when N_k is less than some bound N_{small}. We assume that all prime numbers less than this bound are stored in a file. So the primality of N_k can be proved by a lookup. In the second part of the algorithm the primality of each N_i is proven. This is done by the same method: we prove the primalty of $n = N_i$ with $s = N_{i+1}$ (n and s as in proposition 3.1).

Algorithm 3.4 (ECCP)

Input: *a probable prime n.*

Output: *Proof of primality.*

1. *set $i := 0, N_0 := n$;*
2. *building the sequence:*

   While $(N_i > N_{small})$

   (a) *find a discriminant $D_i < 0$ such that there exists an element $\pi_i \in \mathcal{O}_{D_i}$ with $N(\pi_i) = \pi_i \cdot \pi_i' = N_i$.*

   (b) *set $m_i = N_i + 1 - (\pi_i + \pi_i')$ and test whether m_i factors as $m_i = F_i \cdot N_{i+1}$ with a probable prime $N_{i+1} > (\sqrt[4]{N_i} + 1)^2$. If not, go back to 2(a).*

   (c) *store $\{i, N_i, D_i, \pi_i, m_i, F_i\}$, set $i = i + 1$ and go to step 2.*
3. *proving:*

   For $k := 0$ to $i - 1$ do

   (a) *compute all reduced ideals $\mathcal{A}_l$ of $\mathcal{O}_{D_k}$, the j-invariants $j(\mathbb{E}_{\mathcal{A}_l})$ and the corresponding Hilbert polynomial $G_k(x)$.*

   (b) *compute a root j of $G_k(x)$.*

   (c) *compute the equation of the curve E_k of invariant j whose cardinality modulo N_k is m_k.*

   (d) *find a point P_k on E_k.*

   (e) *check the conditions of Proposition 3.1 with $s = N_{k+1}$ and $m = m_k$.*

We mention a few details of Morains implementation:

Morain uses all negative discriminants with $|D| < 10^6$ with class number $h(-D) < 50$ (10630 possibilities). These discriminants and other useful datas are stored in a file. For factoring he uses several ideas, for example Pollard's ρ-method and ECM. Writing a distributed version of the algorithm Morain was able to prove the primality of the "titanic prime" $(2^{3539} + 1)/3$, a number of 1065 digits and the primality of the partition number $p(1840926)$, a number with 1505 digits.

Bibliography

[AtMo90] A.O.L. Atkin, F. Morain: *Elliptic curves and Primality Proving,* to appear

[Hu74] Th.W. Hungerford: *Algebra,* Graduate Texts in Mathematics, 73, Springer, 1974

[Ke82] H.L. Keng: *Introduction to number theory,* Springer, 1982

[Kn81] D. Knuth: *The art of computer programming,* vol. II, Addison Wesley, 1981

[Kr86] E. Kranakis: *Primality and Cryptography,* Wiley-Teubner Series in Computer Science, 1986

[Scho85] R. Schoof: *Elliptic curves over finite fields and the computation of square roots mod p,* Math. Comp., 44, 1985, 483-494

[Si86] J.H. Silverman: *The arithmetic of elliptic curves,* Graduate Texts in Mathematics, 106, Springer, 1986