which was proposed in 1997 by Hoffstein, Pipher and Silverman. This cryptosystem uses polynomials, more precisely, the ring $R = \mathbb{Z}[x]/\langle x^n - 1\rangle$ (of "n-truncated" polynomials). On the elements of R, the operation of cyclic convolution is defined. Then the reduction of such obtained polynomials over two relatively prime moduli p and q is used. Let us mention that there are some potential attacks to the NTRU cryptosystem that use the LLL algorithm for finding the smallest vector in the corresponding lattice (see [219, Chapter 6]).

There are also the post-quantum cryptographic algorithms based on the properties of isogenies of supersingular elliptic curves, out of which, one of the most interesting is the protocol for key exchange SIDH (supersingular isogeny Diffie-Hellman key exchange) (see [235]).

15.9 Primality proving using elliptic curves

If a positive integer n passes several good primality tests (e.g. the Miller-Rabin test from Chapter 3.9 with respect to a few different bases), then we can be quite confident that n is prime. However, those tests do not provide a *proof* that n is prime. Concerning the relevance of this problem for applications in cryptography, two different ways in which the need for large prime numbers occurs in cryptography should be distinguished. When choosing secret prime numbers p and q for each user in the RSA cryptosystem, we want to generate such numbers as fast as possible, and then it is satisfactory if there is a high probability that those numbers are prime. On the other hand, when choosing a finite field which will be used in the ElGamal cryptosystem, we are dealing with the prime number which might be recommended as a standard and used for a few years, so in this case, we want to be sure (to have a proof) that the number is indeed prime. Now, we will say something about the methods with which it can be proved that a given (large) positive integer is prime.

Theorem 15.21 (Pocklington, 1914)**.** *Let n be a positive integer and let s be a divisor of $n-1$ which is greater than $\sqrt{n}$. Assume that there is a positive integer a such that*

$$a^{n-1} \equiv 1 \pmod{n},$$

$$\gcd(a^{(n-1)/q} - 1, n) = 1, \quad \textit{for each prime divisor } q \textit{ of } s.$$

Then n is prime.

Proof: Let us assume the opposite, i.e. that n is composite. Then it has a prime factor $p \leq \sqrt{n}$. Put $b = a^{(n-1)/s}$. Then

$$b^s \equiv a^{n-1} \equiv 1 \pmod{n},$$

so $b^s \equiv 1 \pmod{p}$. We claim that s is the order of b modulo p. Indeed, let us assume that for a prime divisor q of s, we have $b^{s/q} \equiv 1 \pmod{p}$. Then p divides n and $b^{s/q} - 1$, i.e. $a^{(n-1)/q} - 1$, which is a contradiction with the assumption that n and $a^{(n-1)/q} - 1$ are relatively prime. Since from Fermat's little theorem we have $b^{p-1} \equiv 1 \pmod{p}$, we conclude that s divides $p - 1$. However, this is impossible because $s > \sqrt{n}$, and $p \leq \sqrt{n}$. □

Example 15.16. *Let us prove that the number $n = 256877$ is prime.*

Solution: We have $n - 1 = 2^2 \cdot 149 \cdot 431$, so we can take $s = 4 \cdot 149$. The prime divisors of s are 2 and 149. We can take $a = 2$ because $2^{n-1} \equiv 1 \pmod{n}$, $\gcd(2^{(n-1)/2} - 1, n) = 1$, $\gcd(2^{(n-1)/149} - 1, n) = 1$. Therefore, from Pocklington's theorem, it follows that n is prime. Here, we implicitly used the fact that 149 is prime. To prove the primality of 149, we can proceed in the same manner. We have $149 - 1 = 148 = 2^2 \cdot 37$, so we take $s = 37$. Then from $2^{148} \equiv 1 \pmod{149}$ and $\gcd(2^4 - 1, 149) = 1$, it follows that 149 is prime (under the assumption that 37 is prime). ♢

In the previous example, we saw that by applying Pocklington's theorem, the question of primality of one number is reduced to the same question for one or more smaller numbers and that process is continued until the numbers become small enough.

In order to prove the primality of a number n by Pocklington's theorem, we have to know at least partial factorization of the number $n-1$. However, the factorization of large numbers is generally a difficult problem. Still, this method is very suitable in the case of numbers of a special form, for which the factorization of a large enough divisor of $n - 1$ is known.

There are methods for proving primality which are based on the factorization of $n + 1$, instead of $n - 1$. Let us just mention the *Lucas-Lehmer algorithm* for proving primality of Mersenne numbers (for a proof, see [97, Chapter 5.4.2]).

Theorem 15.22 (Lucas-Lehmer)**.** *Let the sequence (v_k) be given by*

$$v_0 = 4, \quad v_{k+1} = v_k^2 - 2.$$

Let p be an odd prime number. Then $M_p = 2^p - 1$ is prime if and only if M_p divides v_{p-2}.

As we already mentioned, the problem with the application of Pocklington's theorem is in the fact that it requires (partial) factorization of the number $n-1$. The number $n-1$ can be understood as the order of the group $(\mathbb{Z}/n\mathbb{Z})^*$ (if n is prime). One of the ideas how to solve this problem is replacing the group $(\mathbb{Z}/n\mathbb{Z})^*$ by the group $E(\mathbb{Z}/n\mathbb{Z})$, where E is an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$. Namely, with the possible orders of the group $E(\mathbb{Z}/n\mathbb{Z})$, we have greater flexibility so we can hope that we will find an elliptic curve whose order will be easy to factorize. The idea of using elliptic curves for proving primality was introduced by Goldwasser and Kilian in 1986.

Hence, we will consider elliptic curves over the ring $\mathbb{Z}/n\mathbb{Z}$. Since n does not need to be prime, it can happen that we will not be able to add some points on $E(\mathbb{Z}/n\mathbb{Z})$ because, in the formula for addition of points, a number which is not invertible modulo n occurs in the denominator. However, this will not be a problem for us because it will mean that n is a composite number. Moreover, we will be able to find its non-trivial factor by calculating the greatest common divisor of that denominator and the number n.

Theorem 15.23. *Let E be an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$, where $\gcd(6,n)=1$ and $n>1$, given by the equation $y^2=x^3+ax+b$. Let m be a positive integer which has a prime factor $q>(n^{1/4}+1)^2$. If there is a point $P\in E(\mathbb{Z}/n\mathbb{Z})$ such that*

$$[m]P=\mathcal{O} \quad \textit{and} \quad [m/q]P\neq\mathcal{O},$$

then n is prime.

Proof: If n is composite, then it has a prime factor $p\leq\sqrt{n}$. Let us consider the elliptic curve E' over $\mathbb{F}_p$ given by the same equation as E. Let m' be the order of the group $E'(\mathbb{F}_p)$. According to Hasse's theorem, we have

$$m'\leq p+1+2\sqrt{p}=(\sqrt{p}+1)^2\leq(n^{1/4}+1)^2<q.$$

Therefore, $\gcd(m',q)=1$, so there is $u\in\mathbb{Z}$ such that $uq\equiv 1 \pmod{m'}$. Let $P'\in E'(\mathbb{F}_p)$ be the point obtained from P by the reduction of coordinates modulo p. Since, by the assumptions of the theorem, $[m/q]P$ is defined and it is different from $\mathcal{O}$ modulo n, by the same procedure modulo p, we see that $[m/q]P'\neq\mathcal{O}$. However, on the other side, we have

$$[m/q]P'=[uq\cdot\frac{m}{q}]P'=[um]P'=[u]([m]P')=\mathcal{O},$$

so we obtained a contradiction. □

Example 15.17. *Let us prove that the number $n=1237$ is prime.*

Solution: Let E be an elliptic curve given by the equation $y^2 = x^3 + 25x + 1$ over $\mathbb{Z}/n\mathbb{Z}$. The order of $E(\mathbb{Z}/n\mathbb{Z})$ is $m = 1273 = 67 \cdot 19$. Let us take $P = (0, 1)$ and $q = 67$. Then $[19]P = (647, 476) \neq \mathcal{O}$ and $[1273]P = [67]([19]P) = \mathcal{O}$. Since $67 > (1237^{1/4} + 1)^2$, from this, it follows that the number 1237 is prime (if it is known that 67 is prime). $\diamondsuit$

In real applications, with large numbers n, the most problematic part of the algorithm is finding an elliptic curve for which the order of the group $E(\mathbb{Z}/n\mathbb{Z})$, and that will be the number m from the theorem, has a large enough prime factor. One possibility is randomly choosing curves, and then calculating their order by Schoof's algorithm. In order to estimate what is the probability of finding a suitable curve, we should know something about distribution of prime numbers in an interval of the form $(x + 1 - 2\sqrt{x}, x + 1 + 2\sqrt{x})$. Unfortunately, we only have unproven conjectures about that. If it would hold

$$\pi(x + 1 + 2\sqrt{x}) - \pi(x + 1 - 2\sqrt{x}) > A\frac{\sqrt{x}}{\ln x},$$

for a constant A (this conjecture, motivated by the prime number theorem, is believed to hold), then the expected number of operations in Goldwasser-Kilian's algorithm would be $O(\ln^{10} n)$. We could say that the interval from Hasse's theorem is large enough in practice, but not for the present state of theory.

In 1993, Atkin and Morain [15] proposed a variant of primality proving using elliptic curves which is at present considered as the most efficient in practice. By this method, the primality of numbers with approximately 1000 digits can be efficiently proved. The method uses elliptic curves with *complex multiplication*, with the corresponding imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. These are curves with a non-trivial endomorphism (trivial endomorphisms are $P \mapsto mP$ for $m \in \mathbb{Z}$). For example, the elliptic curve $y^2 = x^3 + x$ has a non-trivial endomorphism $(x, y) \mapsto (-x, iy)$ with the corresponding imaginary quadratic field $\mathbb{Q}(i)$ (see [203, Chapters 18 and 19], [415, Chapter 10]). For such curves E, if $4p = x^2 + dy^2$, then the possible orders of E over $\mathbb{Z}/p\mathbb{Z}$ are the numbers $p + 1 \pm x$. Hence, these numbers can be efficiently calculated, and we can see if they have sufficiently large prime factor. When we find a satisfactory order, the curve itself is constructed by using the theory of complex multiplication, especially *j-invariants* (for details, see [48, Chapter 8]).

Let us also mention that in 2004, Agrawal, Kayal and Saxena [7] found the first polynomial time algorithm for proving primality, called the *AKS*

algorithm. As most algorithms for testing or proving primality, the AKS algorithm is also based on a variant of Fermat's little theorem. Its initial point is the following result. Let a and n be integers, $n \geq 2$ and $\gcd(a, n) = 1$. Then the number n is prime if and only if

$$(X + a)^n \equiv X^n + a \pmod{n}, \tag{15.42}$$

i.e. if and only if the corresponding coefficients of the polynomials on the left and right-hand side of congruence (15.42) are congruent modulo n.

15.10 Elliptic curve factorization method

If a positive integer n does not pass some of primality tests, then we know that n is certainly composite. However, those tests usually do not give any non-trivial factor of n. Therefore, the question is, how to find a non-trivial factor of a large composite number. This is considered to be a hard problem, and on its hardness, some of the most important public-key cryptosystems are based.

The methods of factorization can be divided into general and special. With the general methods, the expected number of operations depends only on the size of the number n, while with the special methods, it also depends on properties of the factors of n.

The naïve method of factorization is dividing n by all prime numbers $\leq \sqrt{n}$. The number of needed divisions is in the worst case around $\frac{2\sqrt{n}}{\ln n}$, so the complexity of this method is $O(\sqrt{n} \ln n)$. This method is very inefficient for large n's. However, it is good to use it in combination with better methods of factorization, for removing possible small factors of n.

Pollard's $p - 1$ *method* from 1974 belongs to the special factorization methods. Its initial point is again Fermat's little theorem. Let n be a composite number which we want to factorize and let p be one of its prime factors. Then $a^{p-1} \equiv 1 \pmod{p}$ for $\gcd(a, p) = 1$. Moreover, $a^m \equiv 1 \pmod{p}$ for any multiple m of $p - 1$. If we find m, then $\gcd(a^m - 1, n)$ gives us a factor (we hope a non-trivial one) of n. However, the question is how to find a multiple of $p-1$ when we do not know p. This can be efficiently done in the case when $p - 1$ has only small prime factors. We say that a positive integer is B*-smooth* if all of its prime factors are $\leq B$. Let us assume in addition that all prime powers which divide $p - 1$ are $\leq B$. Then for m we can take the least common multiple of the numbers $1, 2, \ldots, B$.