# 12 Primality proving

In this lecture, we consider the question of how to efficiently determine whether a given integer $N$ is prime. This question is intimately related to the problem of factoring $N$; without a method for determining primality, we have no way of knowing when we have completely factored $N$. This is an important issue for probabilistic factorization algorithms such as the elliptic curve method (ECM): if we attempt to factor a prime with ECM, the algorithm will never terminate.

Even if we are able to guarantee termination, there is still the issue of correctness. If a Monte Carlo algorithm claims that an integer $N$ is the product of two primes $p$ and $q$, it is easy verify that $N = pq$, but how do we know that this is the *complete* factorization of $N$? We need to be able to *prove* that $p$ and $q$ are both prime, and we would like to do so in a way that can be efficiently verified. Factoring is a lot harder than multiplication, and we might similarly expect that proving an integer is prime is harder than verifying the result, provided the prover can provide a "paper trail" that can easily verified. This leads to the notion of a *certificate* for primality, and these can be constructed using elliptic curves.

## 12.1 Classical primality tests

The most elementary approach to primality proving is trial division: we attempt to divide $N$ by every integer $p \le \sqrt{N}$. If no such $p$ divides $N$, then $N$ is prime. This takes $O(\sqrt{N}\,\mathsf{M}(\log N))$, which is impractical for large $N$, but it serves as a useful base case for more sophisticated recursive methods that we will consider.

**Remark 12.1.** This complexity bound can be slightly improved. Using fast sieving techniques [8, Alg. 3.2.2], we can enumerate the primes $p$ up to $\sqrt{N}$ in $O(\sqrt{N}\log N/\log\log N)$ time and then perform trial divisions by just the primes $p \le \sqrt{N}$, rather than every integer $p \le \sqrt{N}$. Applying the prime number theorem and the Schönhage-Strassen bound, the sieving time dominates the cost of the divisions and the overall complexity of trial division is then $O(\sqrt{N}\log N/\log\log N)$.

Many classical primality tests are based on Fermat's little theorem.

**Theorem 12.2** (Fermat)**.** *If $N$ is prime, then for all $a \in \mathbb{Z}/N\mathbb{Z}$:*

$$a^N = a.$$

This implies that if $a^N \neq a$ for some $a \in \mathbb{Z}/N\mathbb{Z}$, then $N$ cannot be prime. This gives us a way to efficiently prove that certain integers are composite. For example, $N = 91$ is not prime because

$$2^{91} \equiv 37 \bmod 91.$$

But this does not always work. For example, $341 = 11 \cdot 31$ is not clearly not prime, but

$$2^{341} \equiv 2 \bmod 341.$$

In this case, using a different value of $a$ will work. If we take $a = 3$ we find that

$$3^{341} \equiv 168 \bmod 341,$$

which proves that 341 is not prime.

However, for certain composite integers $N$ there is *no* choice of $a$ that will work. Thus even if $a^N \equiv a \bmod N$ for every integer $a$, we cannot be sure that $N$ is prime.

**Definition 12.3.** A *Carmichael number* is a composite integer $N$ such that $a^N \equiv a \bmod N$ for every integer $a$.

The first four Carmichael numbers are $561, 1105, 1729$, and $2821$; see sequence A002997 in the On-Line Encyclopedia of Integer Sequences (OEIS) for more examples, or this site for statistics regarding the 20,138,200 Carmichael numbers less than $10^{21}$. The largest known Carmichael number has about 300 billion decimal digits and more than 10 billion distinct prime factors [5]. The question of whether or not there are infinitely many Carmichael numbers was open for more than 80 years and finally settled in 1994.

**Theorem 12.4** (Alford-Granville-Pomerance)**.** *The set of Carmichael numbers is infinite.*

*Proof.* See [6]. □

The infinitude of Carmichael numbers implies that any approach based on Fermat's little theorem is doomed to fail for an infinite set of integers. We would like a criterion that holds if, *and only if*, $N$ is prime. One candidate is the following theorem, which uses the Euler function $\phi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times$, which we recall is multiplicative (meaning that $\phi(ab) = \phi(a)\phi(b)$ for all $a \perp b$), by the Chinese remainder theorem.

**Theorem 12.5.** *A positive integer $N$ is prime if and only if $\phi(N) = N - 1$.*

*Proof.* The forward implication is clear: if $N$ is prime, then $\phi(N) = N-1$. For the converse, we first note that $\phi(1) = 1 \neq 1 - 1$ and 1 is not prime. If $N = p^k$ is a power of a prime $p$ with $k > 1$ then

$$\phi(N) = \phi(p^k) = p^k - p^{k-1} < p^k - 1 = N - 1.$$

In all other cases, we may write $N = ab$ with $a \perp b$. The multiplicativity of $\phi$ implies

$$\phi(N) = \phi(ab) = \phi(a)\phi(b) \leq (a-1)(b-1) < ab - 1 = N - 1.$$ □

One approach suggested by this theorem is to simply compute $\phi(N)$ and check whether it is equal to $N - 1$. However, computing $\phi(N)$ is very difficult, in general.[1] Fortunately, we can use Theorem 12.5 in a less obvious way, via the following lemma. We restrict our attention to odd integers greater $N > 1$, since it is easy to tell whether an even integer is prime or not (and 1 is not prime).

**Lemma 12.6.** *Let $p = 2^s t + 1$ be prime, with $t$ odd, and let $a$ be an integer that is nonzero modulo $p$. Exactly one of the following holds:*

(i) $a^t \equiv 1 \bmod p$;

(ii) $a^{2^i t} \equiv -1 \bmod p$, *for some* $0 \leq i < s$.

*Proof.* Consider the endomorphism $\varphi\colon x \mapsto x^t$ of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ of order $2^s t$; the kernel and image of $\phi$ are cyclic subgroups of orders $t$ and $2^s$, respectively. For each $a \in (\mathbb{Z}/p\mathbb{Z})^\times$, either $a \in \ker \phi$, in which case (i) holds, or $\varphi(a) = a^t$ has order $2^k$ for some $0 < k \leq s$, in which case $a^{2^{k-1}t}$ has order 2 and must be equal to $-1$, the unique element of order 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$, so (ii) holds with $i = k - 1$. □

[1] If $N$ is the product of two primes, it is easy to show that computing $\phi(N)$ is as hard as factoring $N$, and under the Extended Riemann Hypothesis, this is true in general [13].

**Definition 12.7.** Let $N = 2^s t + 1$ be an odd integer, with $t$ odd. An integer $a \not\equiv 0 \bmod N$ is a *witness* for (the compositeness of) $N$ if both of the following hold:

$$\text{(i) } a^t \not\equiv 1 \bmod N \qquad \text{(ii) } a^{2^i t} \not\equiv -1 \bmod N \text{ for } 0 \le i < s.$$

If $a$ is a witness for an odd integer $N > 1$, then Lemma 12.6 implies that $N$ is composite. Prime numbers clearly have no witnesses. It is not immediately clear that every odd composite integer $N$ necessarily has a witness, but this is true. In fact, if we pick $a$ at random it is quite likely to be a witness, as independently proved by Monier [14] and Rabin [18].

**Theorem 12.8** (Monier–Rabin)**.** *Let $N$ be an odd composite integer. The probability that a random integer $a \in [1, N-1]$ is a witness for $N$ is at least $3/4$.*

The theorem suggests that if $N$ is composite and we pick, say, 100 random integers $a \in [1, N-1]$, then we are almost certainly going to find a witness for $N$. On the other hand, if $N$ is prime then we will not find a witness. This doesn't actually *prove* that $N$ is prime (unless we try more than $1/4$ of all $a \in [1, N-1]$), but we can at least view it as strongly supporting this possibility.

*Proof.*[2] Let $N = 2^s t + 1$ be an odd composite number with $t$ odd, and let $N = q_1 \cdots q_r$ be its unique factorization into prime powers $q_j$. Let $b := a^t$ and let $b_j := b \bmod q_j$. If $a$ is not a witness then either $b \equiv 1 \bmod N$, in which case $b_j \equiv 1 \bmod q_j$ for all $j$, or $b^{2^i} \equiv -1 \bmod N$ for some $0 \le i < s$, in which case $b_j^{2^i} \equiv -1 \bmod q_j$ for all $j$. If we put $i := -1$ in the first case, then each $b_j$ is an element of order $2^{i+1}$ in the 2-Sylow subgroup $S_j$ of $(\mathbb{Z}/q_j\mathbb{Z})^\times$.

We will bound the probability that every $b_j$ is an element of $S_j$ of order $2^{i+1}$ by $1/4$. Note that $b_j$ need not be uniformly distributed modulo $q_j$, so some care is required.

Case 1: $N$ is divisible by a square. Then some $q_j = p^k$ with $k > 1$. Since $p$ is odd, the group $(\mathbb{Z}/p^k\mathbb{Z})^\times$ is cyclic of order $\phi(p^k) = p^{k-1}(p-1)$, and $t$ is coprime to $p$ (since it is coprime to $N$), so the probability that $b_j$ lies in $S_j$ at most $1/p^{k-1}$; this is less than $1/4$ except when $p^k = 3^2 = 9$. For $q_j = 9$ we have $t \equiv \pm 1 \bmod 6$, and $(\mathbb{Z}/q_j\mathbb{Z})^\times$ has order $\phi(q_j) = 6$, so $b_j \in S_j = \{\pm 1\}$ if and only if $a \bmod q_j$ lies in $S_j$, which occurs with probability at most $2/8 = 1/4$, since $a$ can take any nonzero value modulo 9.

Case 2: $N$ is a product of $r \ge 3$ distinct primes $q_j$. Each 2-Sylow subgroup $S_j$ is a cyclic of order $2^{k_j}$, for some $k_j > 1$, and at most half the elements in $S_j$ can have any particular order. If we assume each $b_j$ actually lies in $S_j$ then they are uniformly distributed in $S_j$ (since $t$ is odd), and the probability they all have the same order is at most $1/4$.[3]

Case 3: $N = q_1 q_2$ is a product of 2 distinct primes. Let $q_1 = 2^{s_1} t_1 + 1$, and $q_2 = 2^{s_2} t_2 + 1$, with $s_1 \ge s_2$ and $t_1, t_2 \perp 2$. Define the random variable $X_j$ to be $-1$ if $b_j$ does not lie in $S_j$, otherwise let $X_j = i$ where $b_j$ has order $2^i$ in $S_j$. We wish to show $\Pr[X_1 = X_2 \ge 0] \le 1/4$.

Suppose $s_1 > s_2$. Half the elements in $S_1$ have order $2^{s_1} > 2^{s_2}$, so $\Pr[0 \le X_1 \le s_2] \le 1/2$, and $\Pr[X_2 = X_1 | 0 \le X_1 \le s_2] \le 1/2$; therefore $\Pr[X_1 = X_2 \ge 0] \le 1/4$.

Now suppose that $s_2 = s_2$. We have

$$2^s t = N - 1 = q_1 q_2 - 1 = (q_1 - 1)(q_2 - 1) + (q_1 - 1) + (q_2 - 1) = 2^s t_1 t_2 + 2^{s_1} t_1 + 2^{s_2} t_2,$$

thus if $t_1$ divides $t$ then it also divides $t_2$, and conversely. It $t_1$ and $t_2$ both divide $t$, then $t_1 = t_2$ and $q_1 = q_2$, a contradiction. So assume $t_1 \nmid t$. Then $t_1 \ne 1$ must be divisible by a power of an odd prime $\ell \ge 3$ that does not divide $t$. It follows that $\Pr[X_1 \ge 0] \le 1/3$, and we also have $\Pr[X_1 = X_2 | X_1 \ge 0] \le 1/2$, therefore $\Pr[X_1 = X_2 \ge 0] \le 1/6 < 1/4$. □

[2] The proof we give here is a bit different (and more elementary) than the proofs of Monier and Rabin.

[3] This rules out all Carmichael numbers, since they all have at least 3 distinct prime factors.

Theorem 12.8 yields the following probabilistic primality test, due to Gary Miller [13] and Michael Rabin [18]

**Algorithm 12.9** (Miller-Rabin)**.** Given an odd integer $N > 1$:

1. Pick a random integer $a \in [1, N-1]$.
2. Write $N = 2^s t + 1$, with $t$ odd, and compute $b = a^t \bmod N$.
   If $b \equiv \pm 1 \bmod N$, return **true** ($a$ is not a witness, $N$ could be prime).
3. For $i$ from 1 to $s-1$:
   a. Set $b \leftarrow b^2 \bmod N$.
   b. If $b \equiv -1 \bmod N$, return **true** ($a$ is not a witness, $N$ could be prime).
4. Return **false** ($a$ is a witness, $N$ is definitely not prime).

**Example 12.10.** For $N = 561$ we have $561 = 2^4 \cdot 35 + 1$, so $s = 4$ and $t = 35$, and for $a = 2$ we find that

$$2^{35} \equiv 263 \bmod 561,$$

which is not $\pm 1 \bmod 561$ so we continue and compute

$$263^2 \equiv 166 \bmod 561,$$
$$166^2 \equiv 67 \bmod 561,$$
$$67^2 \equiv 1 \bmod 561.$$

None of these values is congruent to $-1$, so $a = 2$ is a witness for $N = 561$ and we return **false**, meaning that 561 is definitely not prime. Note the contrast with the Fermat test, which jumps immediately to the last value computed above and does not detect that 561 is composite.

The Miller-Rabin test is a Monte Carlo algorithm with 1-sided error. If $N$ is prime the algorithm will always correctly output **true**, and if $N$ is composite the algorithm will correctly output **false** with probability at least $3/4$. The running time of the algorithm is $O(n\,\mathsf{M}(n))$, quasi-quadratic in $n = \log N$. This makes it extremely efficient, and it is the most widely used method for testing primality. In practical implementations, one performs several iterations of the Miller-Rabin test (choosing a new random integer $a$ each time), and if they all return **true**, conclude that $N$ is "probably prime".

But we should be careful how we interpret this. Any particular integer $N$ is either prime or not; it makes no sense to say that $N$ is prime with some probability. But if $N$ is a randomly distributed over some interval, then it does make sense to ask for the probability that $N$ is prime, given that it passed a Miller-Rabin test. If $N$ is selected from a large interval, say $[1, e^{1000}]$, then the probability that $N$ is prime is quite small, approximately $1/1000$. In this situation, we need to be careful, since false positives are more likely than primes. It might appear to require several Miller-Rabin tests before we could say with better than 50% confidence that a large random integer $N$ is prime. However, the Miller-Rabin test is far more powerful than Theorem 12.8 suggests.

**Theorem 12.11** (Damgård-Landrock-Pomerance)**.** *Let $N$ be a random odd integer in $[2^{k-1}, 2^k]$. Let $a$ be a random integer in $[1, N-1]$. Then, if $a$ is not a witness for $N$, then*

$$\Pr[N \text{ is prime}] \geq 1 - k^2 \cdot 4^{2-\sqrt{k}}.$$

*Proof.* See [9, Thm. 2]. □

For large $N$, Theorem 12.11 gives excellent bounds on the probability that a random integer $N$ is prime, given that it passes a single Miller-Rabin test. For example:

$$k = 256: \qquad 1 - k^2 \cdot 4^{2-\sqrt{k}} = 1 - 2^{-12},$$
$$k = 4096: \qquad 1 - k^2 \cdot 4^{2-\sqrt{k}} = 1 - 2^{-100}.$$

Thus when $k$ is large it only takes a few successful Miller-Rabin tests to become astronomically confident that a randomly chosen integer $N$ is prime.

## 12.2 Elliptic Curve Primality Proving

We now consider a method to unequivocally *prove* that a given integer $N$ is prime or composite using elliptic curves. Elliptic curve primality proving (ECPP) was introduced by Goldwasser and Kilian in 1986 [10]. Like Lenstra's elliptic curve method (ECM) for integer factorization [11] which appeared at roughly the same time, it takes advantage of the fact that elliptic curves provide a way to generate abelian groups of varying orders over a fixed finite field. To simplify the statement of the Goldwasser-Kilian theorem, we first make the following definitions.

**Definition 12.12.** Let $P = (P_x : P_y : P_z)$ be a projective point on an elliptic curve $E/\mathbb{Q}$, with $P_x, P_y, P_z \in \mathbb{Z}$, and let $N$ be a nonzero integer. If $P_z \equiv 0 \bmod N$ then $P$ is *zero mod* $N$; otherwise, $P$ is *nonzero mod* $N$. If $\gcd(P_z, N) = 1$ then $P$ is *strongly nonzero mod* $N$.

Note that if $P$ is strongly nonzero mod $N$, then $P$ is nonzero mod $p$ for every prime $p|N$. When $N$ is prime, the notions of nonzero and strongly nonzero coincide. We now state the theorem, using $\Delta(E) := -16(4A^3 + 27B^2)$ to denote the discriminant of an elliptic curve $E\colon y^2 = x^3 + Ax + B$ in short Weierstrass form.

**Theorem 12.13** (Goldwasser-Kilian)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, and let $M, N > 1$ be integers with $M > (N^{1/4} + 1)^2$ and $N \perp \Delta(E)$, and let $P \in E(\mathbb{Q})$. If $MP$ is zero mod $N$ and $(M/\ell)P$ is strongly nonzero mod $N$ for every prime $\ell|M$ then $N$ is prime.*

*Proof.* Suppose for the sake of contradiction that the hypothesis holds and $N$ is composite. Then $N$ has a prime divisor $p \le \sqrt{N}$, and $E$ has good reduction at $p$ since $N \perp \Delta(E)$. Let $M_p$ be the order of the reduction of $P$ on $E$ modulo $p$. The point $MP$ is zero mod $N$ and therefore zero mod $p$, so $M_p|M$; and we must have $M_p = M$, since $(M/\ell)P$ is strongly nonzero mod $N$ and therefore nonzero mod $p$, for every prime $\ell|M$. Thus $P$ has order $M$ on the reduction of $E$ modulo $p$, and by the Hasse bound, $M \le (\sqrt{p} + 1)^2$. But we also have $M > (N^{1/4} + 1)^2 \ge (p^{1/2} + 1)^2$, which is our desired contradiction. □

In order to apply the theorem, we need to know the prime factors $q$ of $M$. In particular, we need to be sure that these $q$ are actually prime! To simplify matters, we restrict ourselves to the case that $M = q$ is prime, and introduce the notion of a *primality certificate*.

**Definition 12.14.** A *primality certificate* for $p$ is a tuple of integers

$$(p, A, B, x_1, y_1, q),$$

where $P = (x_1 : y_1 : 1)$ is a point on the elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{Q}$, the integer $p > 1$ is prime to $\Delta(E)$, and $qP$ is zero mod $p$ with $q > (p^{1/4} + 1)^2$.

Note that $P = (x_1 : y_1 : 1)$ is strongly nonzero mod $p$, since its $z$-coordinate is 1. Theorem 12.13 implies that if there exists a primality certificate $(p, \ldots, q)$ for $N = p$ in which $M = q$ is prime, then $p$ is prime. Thus a primality certificate $(p, \ldots, q)$ reduces the question of $p$'s primality to the question of $q$'s primality. Using a chain of such certificates, we can reduce to a case in which $q$ is so small that we are happy to test its primality via trial division. This leads to the following recursive algorithm.

**Algorithm 12.15** (Goldwasser-Kilian ECPP)**.** Given an odd integer $p$ (a candidate prime), and a bound $b$, with $p > b > 5$, either construct a primality certificate $(p, A, B, x_1, y_1, q)$ with $q \le (\sqrt{p}+1)^2/2$ or prove that $p$ is composite.

1. Pick random integers $A, x_0, y_0 \in [0, p-1]$, and set $B = y_0^2 - x_0^3 - Ax_0$.
   Repeat until $\gcd(4A^3 + 27B^2, p) = 1$, then define $E\colon y^2 = x^3 + Ax + B$.
2. Use Schoof's algorithm to compute the number of points $m$ on the reduction of $E$ modulo $p$, assuming that $p$ is prime. If anything goes wrong (which it might if $p$ is actually composite), or if $m \notin \mathcal{H}(p)$, then return **composite**.
3. Write $m = cq$, where $c$ is $b$-smooth and $q$ is $b$-coarse (all prime factors greater than $b$). If $c = 1$ or $q \le (p^{1/4}+1)^2$, then go to step 1.
4. Perform a Miller-Rabin test on $q$. If it returns **false** then go to step 1.
5. Compute $P = (P_x : P_y : P_z) = c \cdot (x_0 : y_0 : 1)$ on $E$, working modulo $p$.
   If $\gcd(P_z, p) \ne 1$, go to step 1, else let $x_1 \equiv P_x/P_z \bmod p$ and $y_1 \equiv P_y/P_z \bmod p$.
6. Compute $Q = (Q_x : Q_y : Q_z) = q \cdot (x_1 : y_1 : 1)$ on $E$, working modulo $p$.
   If $Q_z \not\equiv 0 \bmod p$ then return **composite**.
7. If $q > b$, then recursively verify that $q$ is prime using inputs $q$ and $b$; otherwise, verify that $q$ is prime by trial division. If $q$ is found to be composite, go to step 1.
8. Output the certificate $(p, A, \tilde{B}, x_1, y_1, q)$, where $\tilde{B} \equiv B \bmod p$ is chosen so that we have $y_1^2 = x_1^3 + Ax_1 + \tilde{B}$ (over $\mathbb{Z}$ not just modulo $p$).

Note that step 4 is not strictly necessary, a composite $q$ would eventually be detected in the recursive call, but it greatly reduces the probability that we will waste time in the recursive call, which speeds up the algorithm.

When the input to Algorithm 12.15 is prime, it will output a sequence of certificates, one for each recursive call, that reduce the question of $p$'s primality to that of a prime $q < b$ that has been proved prime via trial division. Taken together, the sequence of primality certificates constitute a *primality proof* for $p$. The complexity of this algorithm, and the complexity of verifying the primality proof it generates, are considered in the problem set, under the heuristic assumption that the integer $m$ behaves like a random integer of similar size in terms of its factorization into $b$-smooth and $b$-coarse parts.

Without any heuristic assumptions, Goldwasser and Kilian proved that for almost all inputs $p$ of a given size (all but a subexponentially small fraction), the expected running time of this algorithm is polynomial in $\log p$. Heuristically, this is believed to be true for all inputs, but we cannot prove this. Adleman and Huang later came up with a clever work-around to this problem that yielded an algorithm with a provably polynomial expected running time for all inputs [4]. Their strategy is to "reduce" the problem of proving the primality of the given input $p$ that of proving the primality of a *larger* prime $p' \approx p^2$. The key point it that the prime $p'$ is obtained in a random way that makes it very likely that the Goldwasser-Kilian algorithm can prove its primality within a polynomial time bound (and

if this does not happen we can always generate a different $p'$ and try again). In practice the algorithm of Adleman and Huang is never used, since it is believed that it in fact it is always faster to just use the original Goldwasser-Kilian algorithm, no matter what $p$ is, and the correctness of the Goldwasser-Kilian is guaranteed. But the Adleman-Huang result was theoretically significant, because it proved that primes could be recognized in polynomial time by a randomized algorithm (of course we can now do so deterministically, as discussed below, but this was a major open question at the time).

**Remark 12.16.** In [4] Adleman and Huang obtain the prime $p'$ as the order of a randomly chosen abelian variety $J_C$ of dimension 2 that is associated to a genus 2 curve $C$ over $\mathbb{F}_p$ (assuming that $p$ is prime). The abelian variety $J_C$ is called the *Jacobian* of the curve $C$. It is analogous to the group of points on an elliptic curve (an abelian variety of dimension 1), except that when $C$ has genus 2 the "points" on $J_C$ actually correspond to pairs of points on the curve $C$. There is a generalization of Hasse's theorem due to Weil that implies that the cardinality of $J_C(\mathbb{F}_p)$ is on the order of $p^2$ and lies within an interval of width $\approx 8p^{3/2}$. This interval is large enough (relative to $p^2$) that we can prove that it contains many primes, roughly as many as implied by the prime number theorem. Adleman and Huang show that for a random curve $C$, the cardinality of $J_C(\mathbb{F}_p)$ is reasonably likely to be any one of a large subset of these primes, yielding a prime $p'$ that is very likely to be one that the Goldwasser-Kilian algorithm can certify in polynomial time. In order to make this all work, Adleman and Huang modify the Goldwasser-Kilian algorithm slightly to make the proportion of bad inputs even smaller, and they also use the fact that $\#J_C(\mathbb{F}_p)$ can be computed in polynomial time using an analog of Schoof's algorithm due Pila [16].

In fact, the original algorithm of Goldwasser-Kilian is no longer used; there is a much faster ECPP algorithm due to Atkin and Morain that uses the CM method to construct an elliptic curve $E$ modulo $p$ with suitable order $m$ (assuming that $p$ is prime), eliminating the need to generate many random curves, and use of Schoof's algorithm [3]. Like the Goldwasser-Kilian algorithm, this algorithm has not been proved to run in expected polynomial time, but in practice it is very fast. When combined with a further optimization due to Shallit [15], its expected running time is heuristically believed to be $\tilde{O}(n^4)$, where $n = \log p$. This makes it the current method of choice for general purpose primality proving. We will examine the Atkin-Morain algorithm more closely after we have studied the theory of complex multiplication.

We should note that there is now a deterministic polynomial-time algorithm for proving primality due to Agrawal, Kayal, and Saxena [2]. This is an important theoretical result, but it is not used in practice. The time bound proved in [2] is $\tilde{O}(n^{10.5})$; this can be improved to $\tilde{O}(n^6)$ (see [12]), but even with this improvement it is still much slower than the $\tilde{O}(n^4)$ heuristic complexity of ECPP. There is a randomized version of the AKS algorithm due to Bernstein [7] that runs in $\tilde{O}(n^4)$ time, but the constant factors appear to make it slower than ECPP, and it requires substantially more memory. The certificates it produces also take longer to verify.

The current record for general purpose proving involves a 34,987 digit prime and was set using ECPP in November 2017 (see [17] for an up-to-date list of ECPP records). There are of course much larger integers that have been proved prime (for example, the 24 million digit Mersenne prime $2^{82589933}-1$), but these are all of a form that permits specialized $\tilde{O}(n^2)$-time algorithms to be used. There are also specialized forms of elliptic curve primality proving that run in $\tilde{O}(n^2)$-time and these have been used to prove the primality of some large primes that no non-elliptic curve based method can feasibly handle [1].

## References


[1] A. Abatzoglou, A. Silverberg, A.V. Sutherland, and A. Wong, *A framework for deterministic primality proving using elliptic curves with complex multiplication*, Mathematics of Computation **85** (2016), 1461–1483.

[2] M. Agrawal, N. Kayal, N. Saxena, *Primes is in P*, Annals of Math. **160** (2004), 781–793.

[3] A.O.L. Atkin and F. Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993),29–68.

[4] L. Adleman and M-D. A. Huang, *Primality testing and abelian varieties over finite fields*, Lecture Notes in Mathematics **1512**, Springer, 1992.

[5] W. Alford, J. Grantham, S. Hayman, and A. Shallue, *Constructing Carmichael numbers through improved subset-product algorithms*, Mathematics of Computation **83** (2014), 889–915.

[6] W.R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics **140** (1994), 703–722.

[7] D.J. Bernstion, *Proving primality in essentially quartic random time*, Mathematics of Computation **76** (2007), 389–403.

[8] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, 2nd edi-tion, Springer, 2005.

[9] I. Damgård, P. Landrock, and C. Pomerance, *Average case error estimates for the strong probable prime test*, Mathematics of Computation **61** (1993), 177–194.

[10] S. Goldwasser and J. Kilian, *Almost all primes can be quickly certified*, Proceedings of the Eighteenth ACM Symposium on the Theory of Computing (1986), 316–329.

[11] H. Lenstra, *Factoring integers with elliptic curves*, Annals of Math. **126** (1987), 649–673

[12] H. Lenstra and C. Pomerance, *Primality testing with Gaussian periods*, Journal of the European Mathematical Society, to appear.

[13] G. L. Miller, *Riemann's hypothesis and tests for primality*, Journal of Computer and System Sciences **13** (1976), 300-317.

[14] L. Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoretical Computer Science **12** (1980), 97–108.

[15] F. Morain, *Implementing the asymptotically fast version of the elliptic curve primality proving algorithm*, Mathematics of Computation **76** (2007), 493–505.

[16] J. Pila, *Frobenius maps of abelian varieties and finding roots of unity in finite fields*, Math. Comp. **55** (1990), 745–763.

[17] C.K. Caldwell, *The top twenty elliptic curve primality proofs*, Prime Pages website, accessed March 16, 2019.

[18] M.O. Rabin *Probablistic algorithm for testing primality*, Journal of Number Theory **12** (1980), 128–138.

# 18.783 Elliptic Curves

Spring 2019