In this lecture, we consider the following problem: given a positive integer N, how can we efficiently determine whether N is prime or not? 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 a serious issue for probabilistic factorization algorithms such as ECM: if we attempt to factor a prime number N with the ECM algorithm, the algorithm will never terminate. This problem is in not unique to ECM; currently every known factorization algorithm that achieves a subexponential running time (even heuristically) is a randomized algorithm; in the absence of an explicit primality test most of these algorithms will simply fail to terminate on prime inputs.

Even if we are able to ensure termination, there is still the issue of correctness. If a Monte Carlo algorithm outputs the factorization $N = pq$, it is easy to check whether the product of p and q is in fact equal to N. But how do we know that this is the *complete* factorization of N? We need a way to unequivocally *prove* that p and q are both prime.

13.1 Classical primality tests

The most elementary approach to the problem is trial division: attempt to divide N by every integer $p \le \sqrt{N}$. If no such p divides N, then N must be prime. This takes time $O(\sqrt{N}\mathsf{M}(\log N))$, which is exponential in $\log N$.

Remark 13.1. This complexity bound can be slightly improved. Using fast sieving techniques [6, 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 $p \le \sqrt{N}$. 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 becomes $O(\sqrt{N}\log N/\log\log N)$.

Many early primality tests were based on Fermat's little theorem.

Theorem 13.2 (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, since:

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

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:

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

proves that 341 is not prime.

However, for certain composite integers N, there is *no* choice of a that will allow us to prove that N is composite using this test. Conversely, even if $a^N \equiv a \bmod N$ for every integer a, we cannot say that N is prime.

Definition 13.3. A *Carmichael number* is a composite integer N such that $a^N \equiv a \bmod N$ for every integer a.

The first four Charmichael numbers are $561, 1105, 1729$, and 2821; for more, see sequence A002997 in the On-Line Encyclopedia of Integer Sequences (OEIS). The largest known Charmichael number has about 300 billion decimal digits and more than 10 billion distinct prime factors [4]. The question of whether or not there are infinitely many Charmichael numbers was open for more than 80 years and finally settled in 1994 [5].

Theorem 13.4 (Alford-Granville-Pomerance)**.** *The set of Carmichael numbers is infinite.*

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 is true if, *and only if*, N is prime. One candidate is the following theorem, which uses the Euler function $\phi(N) = |\mathbb{Z}/N\mathbb{Z}^*|$.

Theorem 13.5. *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 note that $\phi(1) = 1 \neq 1 - 1$ and 1 is not prime, and if $N = p^k$, for some prime p and integer $k > 1$, then we have

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

Otherwise, we may write $N = ab$ with $a \perp b$ and the multiplicativity of ϕ implies

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

One approach suggested by this theorem is to simply compute $\phi(N)$ and see whether it is equal to $N - 1$. However, computing $\phi(N)$ is very difficult, in general.[1] Fortunately, we can use Theorem 13.5 in a less obvious way, via the following lemma. We restrict our attention to odd integers, since it is easy to tell whether an even integer is prime or not.

Lemma 13.6. *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) $a^t \equiv 1 \bmod p$, *or*

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

Proof. The map $\pi(x) = x^t$ is an automorphism of the abelian group $(\mathbb{Z}/p\mathbb{Z})^*$. The group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $2^s t$, and it follows that the image of π is a cyclic group of order 2^s. For any $a \in \mathbb{Z}/p\mathbb{Z}^*$, either $\pi(a)$ is the identity, in which case (i) holds, or the order of $\pi(a)$ is 2^k for some positive $k < s$. In the latter case, for $i = k - 1$ the integer $a^{2^i t}$ has order 2 in $(\mathbb{Z}/p\mathbb{Z})^*$ and must be equal to -1, the unique element of order 2. In this case (ii) holds. $\square$

Definition 13.7. Let $N = 2^s t + 1$ be an odd integer, with t odd. An integer $a \not\equiv 0 \bmod N$ is said to be a *witness* for N if (i) $a^t \not\equiv 1 \bmod N$ and (ii) $a^{2^i t} \not\equiv -1 \bmod N$ for $0 \leq i < s$.

[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 [9].

This suggests the following probabilistic primality test: pick a random a and check whether it is a witness for N. If so, then N is composite, since Lemma 13.6 implies that there are can be no witnesses for a prime integer N. It may not be immediately clear that a given composite integer N necessarily has any witnesses, but it does; in fact, when N is composite most integers a are witnesses.

Theorem 13.8 (Monier–Rabin, 1980)**.** *Let N be an odd composite integer. Then, 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 won't find a witness. Note that this doesn't *prove* anything about the primality of N (unless we try more than $1/4$ of all $a \in [1, N-1]$, but that would take substantially more time than trial division).

Proof.[2]

Let N be an odd composite number of the form $N = 2^s t + 1$ with t is odd, and let $N = q_1 q_2 \cdots q_r$ be the factorization of N into powers of distinct primes. Let $b = a^t$ and suppose that a is not a witness. Then either $b \equiv 1 \bmod N$, in which case $b \equiv 1 \bmod q_j$ for all of the q_j, or $b^{2^i} \equiv -1 \bmod N$ for some $0 \le i < s$, in which case $b^{2^i} \equiv -1 \bmod q_j$ for all of the q_j. In either case, $b \bmod q_j$ is an element of the 2-Sylow subgroup of $(\mathbb{Z}/q_j\mathbb{Z})^*$ for all q_j, and it has the same order in $(\mathbb{Z}/q_j\mathbb{Z})^*$ for each q_j. We will show that the probability of this happening is at most $1/4$. We consider three cases.

Case 1: N is not square-free. Then some $q_j = p^k$ with $k > 1$. Since p is odd, the group $(\mathbb{Z}/p^k\mathbb{Z})^*$ is cyclic of order $\phi(p^k) = p^{k-1}(p-1)$. The prime p cannot divide t, since t divides $N-1$ and p divides N. It follows that if a has order divisible by p in $(\mathbb{Z}/p^k\mathbb{Z})^*$, then so does $b = a^t$, and in this case b cannot be an element of the 2-Sylow subgroup of $(\mathbb{Z}/p^k\mathbb{Z})^*$. Thus the probability that b lies in the 2-Sylow subgroup of $(\mathbb{Z}/p^k\mathbb{Z})^*$ is at most $1/p^{k-1}$, which is less than $1/4$ for all $p^k > 9$. For $p^k = 9$ one checks that for each of $t = 1, 2, 4, 5 \bmod 6$, at most $2/9 < 1/4$ of the possible values of $a \bmod 9$ yield $b = a^t = \pm 1 \bmod 9$, which is necessary for b to lie the 2-Sylow subgroup of $(\mathbb{Z}/9\mathbb{Z})^*$.

Case 2: $r \ge 3$. For each q_j the 2-Sylow subgroup G_j of $(\mathbb{Z}/q_j\mathbb{Z})^*$ is a cyclic of order 2^k, for some $k > 1$, and at most half the elements in G_j have any particular order. Assuming $b = a^t \bmod q_j$ lies in G_j for $j = 1, 2, 3$, the probability that it has the same order in each case is at most $1/4$.[3]

Case 3: $N = pq$ for distinct primes p and q. We may write $p = 2^{s_p} t_p + 1$, and $q = 2^{s_q} t_q + 1$, with t_p and t_q odd. Define the random variable X_p to be -1 if $b \bmod p$ does not lie in the 2-Sylow subgroup G_p of $(\mathbb{Z}/p\mathbb{Z})^*$, and otherwise let $X_p = i$, where $b \mod p$ has order 2^i in G_p. Similarly define the random variable X_q. We wish to show that $\Pr[X_p = X_q \ge 0] \le 1/4$.

We first suppose that $s_p > s_q$. Then $\Pr[0 \le X_p \le s_q] \le 1/2$, and we also have $\Pr[X_q = X_p | 0 \le X_p \le s_q] \le 1/2$, hence $\Pr[X_p = X_q \ge 0] \le 1/4$.

We now suppose that $s_p = s_q$, and assume that one t_p or t_q does not divide t; without loss of generality, assume $t_p \nmid t$. Then $\Pr[X_p \ge 0] \le 1/3$, since t_p has a prime factor $\ell \ge 3$ that does not divide t. As above, we also have $\Pr[X_q = X_p | X_p \ge 0] \le 1/2$, hence $\Pr[X_p = X_q \ge 0] \le 1/6 < 1/4$.

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

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

Lastly, we address the case where $s_p = s_q$ and both t_p and t_q divide t. We have

$$2^s t = N - 1 = pq - 1 = (p-1)(q-1) + (p-1) + (q-1) = 2^{2s_p} t_p t_q + 2^{s_p} t_p + 2^{s_p} t_q.$$

Since $s = s_p + s_q = 2s_p$, we can divide by 2^{s_p} to obtain

$$2^{s_p} t = 2^{s_p} t_p t_q + t_p + t_q. \tag{1}$$

Since $t_p | t$, the LHS of (1) is divisible by t_p, as are the first two terms on the RHS, so we must have $t_p | t_q$. Similarly, we must have $t_q | t_p$, and therefore $t_p = t_q$. But then $p = 2^{s_p} t_p + 1$ and $q = 2^{s_q} t_q + 1$ are equal, contradicting our assumption that p and q are distinct. □

Theorem 13.8 yields the following probabilistic primality test.

Algorithm 13.9 (Miller-Rabin)**.**
Given an odd integer N:

1. Pick a random integer $a \in [1, N-1]$.
2. Write $N = 2^2 t + 1$, 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 13.10. For $N = 561$, $a = 2$: $561 = 2^4 \cdot 35 + 1$. Thus, we compute:

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

This is not $\pm 1 \bmod 561$ so we continue:

$$236^2 \equiv 166 \bmod 561$$
$$166^2 \equiv 67 \bmod 561$$
$$67^2 \equiv 1 \bmod 561$$

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 a prime. Note the contrast with the Fermat test, which effectively just checks whether the last value computed above is 1 and does not detect that 561 is composite.

We should view the Miller-Rabin test as 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 $O(n\mathsf{M}(n))$, where $n = \log N$, the same as exponentiation in $\mathbb{Z}/N\mathbb{Z}$. 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. For any particular integer N, either N is prime or it isn't; it makes no sense to say that N is prime with some probability. If N is a random integer 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. However, 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 actually much more effective than Theorem 13.8 suggests.

Theorem 13.11 (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 Theorem 2 in [7]. □

Example 13.12. For large N, Theorem 13.11 gives excellent bounds on the probability that a random integer N is prime, given that it passes a single Miller-Rabin test:

If $k = 256$, then $1 - k^2 \cdot 4^{2-\sqrt{k}} \geq 1 - 2^{-12}$.
If $k = 1024$, then $1 - k^2 \cdot 4^{2-\sqrt{k}} \geq 1 - 2^{-40}$.

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

13.2 Elliptic Curve Primality Proving

We now consider a method to unqeuivocally *prove* whether a given integer N is prime or composite, using elliptic curves. Elliptic curve primality proving (ECPP) is based on a fundamental theorem of Goldwasser and Kilian [8]. To simplify the statement of the theorem, we make the following definitions.

Definition 13.13. Let $P = (x : y : z)$ be a projective point on an elliptic curve $E/\mathbb{Q}$, where $x, y, z \in \mathbb{Z}$, and let N be a nonzero integer. If $z \equiv 0 \bmod N$ then the point P is said to be *zero mod N*; otherwise, P is *nonzero mod N*. If $\gcd(z, N) = 1$ then the point P is said to be *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 being strongly nonzero and nonzero mod N coincide. We now state the theorem, using $\Delta(E)$ to denote the discriminant of E.

Theorem 13.14 (Goldwasser-Kilian)**.** *Let $E/\mathbb{Q}$ be an elliptic curve, and let M and N be positive integers with $M > (N^{1/4} + 1)^2$ and N prime to $\Delta(E)$. Suppose there is a point $P \in E(\mathbb{Q})$ such that MP is zero mod N and $(M/q)P$ is strongly nonzero mod N for every prime $q|M$. 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 $p \leq \sqrt{N}$, and E has good reduction at p since N is prime to $\Delta(E)$. 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 $(M/q)P$ is strongly nonzero mod N and therefore nonzero mod p, for every prime $q|M$. Thus P has order M on the reduction of E modulo p, and by the Hasse bound $M \leq (\sqrt{p}+1)^2$. But we also have $M > (N^{1/4} + 1)^2 \geq (p^{1/2} + 1)^2$, which is our desired contradiction. □

Note that in the theorem above, we need to know the prime factors q of M. In particular, we need to be sure that they 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 13.15. A *primality certificate* for p is a tuple of integers

$$(p, A, B, x_0, y_0, q),$$

where $P = (x_0 : y_0 : 1)$ is a point on the elliptic curve $E\colon y^2 = x^3 + Ax + B$ over $\mathbb{Q}$, the positive integer p is prime to $\Delta(E)$, and $q > (p^{1/4} + 1)^2$ is such that qP is zero mod p.

Note that $P = (x_0 : y_0 : 1)$ is always strongly nonzero mod p, since its z-coordinate is 1. Theorem 13.14 implies that if there exists a primality certificate $(p, \ldots, q)$ for p in which 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 it's primality via trial division.

This leads to the following recursive algorithm.

Algorithm 13.16 (Goldwasser-Kilian)**.** Given an 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 $q \leq (\sqrt{p} + 1)^2/2$, if p is prime, or return **composite** if 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 $\gcd(-16(4A^3 + 27B^2), p) = 1$.

2. Use Schoof's algorithm to compute $M = \#E(\mathbb{F}_p)$, assuming that p is prime.
   If anything goes wrong, or if $M \notin [(\sqrt{p} - 1)^2, (\sqrt{p} + 1)^2]$, then return **composite**.

3. Write $M = cq$, where $l \nmid c$ for primes $l > b$ and $l \nmid q$ for primes $l \leq b$.
   If $c = 1$ or $q \leq (p^{1/4} + 1)^2$, then go to step 1.

4. Perform a Miller-Rabin test on q. If it returns **false**, go to step 1.

5. Compute $P = (P_x : P_y : P_z) = c(x_0 : y_0 : 1)$ on E, working modulo p.
   If $\gcd(P_z, p) \neq 1$, go to step 1, else set $x_1 = P_x/P_z \bmod p$ and $y_1 = P_y/P_z \bmod p$.

6. Compute $Q = (Q_x : Q_y : Q_z) = q(x_1 : y_1 : 1)$ 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, B, x_1, y_1, q).

Note that step 5 is not strictly necessary, since 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 13.16 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.

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 [3]. 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 prime p' is obtained in a random way, making 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 use the original Goldwasser-Kilian algorithm, no matter what p is. But their result was theoretically significant, since it proved for the first time that primes could be recognized in polynomial time by a randomized algorithm.

Remark 13.17. 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, and is completely 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.[4] There is a generalization of Hasse's theorem due to Weil that implies that the cardinality of $J_C(\mathbb{F}_p)$ is approximately p^2 and lies within an interval whose width is about $8p^{3/2}$. The key point is that this interval is large enough relative to p^2 that we can actually prove that it contains many primes (roughly as many as implied by the prime number theorem). Adleman and Huang show that for a randomly chosen 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 be expected to certify in polynomial time. In order to make this all work, Adleman and Huang actually modify the Goldwasser-Kilian algorithm slightly to make the proportion of bad inputs even smaller, and they also have to prove that $\#J_C(\mathbb{F}_p)$ can be computed in polynomial time, via an analog of Schoof's algorithm.[5]

In fact, the original algorithm of Goldwasser-Kilian is no longer used; there is a faster version of this 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 the need to use Schoof's algorithm [2]. Like the Goldwasser-Kilian algorithm, this algorithm has not been proven to run in expected polynomial time, but in practice it is very fast. When combined with a further optimization due to Shallit [10], 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; it is substantially faster than even optimized versions of the deterministic polynomial-time algorithm of Agrawal, Kayal, and Saxena [1] that came later.

We will examine the Atkin-Morain algorithm more closely after we have studied the theory of complex multiplication.

[4] To learn more about Jacobians of genus 2 curves, take 18.782 in the fall.

[5] All of this is laid out in their monograph [3], which you can access online (via MIT library subscription) at http://link.springer.com/book/10.1007/BFb0090185/page/1.

References

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

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

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

[4] W. Alford, J. Grantham, S. Hayman, and A. Shallue, *Constructing Carmichael numbers through improved subset-product algorithms*, Mathematics of Computation, to appear, preprint http://arxiv.org/abs/1203.6664.

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

[6] R. Crandall and C. Pomerance,*Prime Numbers: A Computation Perspective*, 2nd edition, Springer, 2005.

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

[8] 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.

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

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