Primality testing is in P

Bogdan Grechuk • 10 Jul 2026

This post continues my series on favorite theorems of the twenty-first century. For an overview of the categories and my earlier selections, see this post.

My choice for 2003 in *Algorithms and Complexity* is the theorem of Agrawal, Kayal, and Saxena establishing the existence of a deterministic polynomial-time algorithm for deciding whether a given integer is prime or composite. Their work was published in 2004 (Agrawal et al. 2004).

One of the fundamental algorithmic problems in number theory is *primality testing*: given an integer $k > 1$, determine whether k is prime or composite. The most direct approach is to test every possible divisor between 2 and $\sqrt{k}$. This requires on the order of $\sqrt{k}$ divisions and is therefore exponential in the number of digits of k. The natural question is whether primality can be decided much more efficiently.

Primality testing is a *decision problem*: a yes-or-no question defined on an infinite collection of finite inputs. A decision problem belongs to the complexity class P if there is an algorithm that always returns the correct answer and whose running time is bounded by a polynomial in the length of the input. Since an integer k can be represented using $O(\log k)$ bits, a polynomial-time primality test must run in

$$O\big((\log k)^m\big)$$

bit operations for some constant m.

In 1976, Miller (Miller 1976) gave a polynomial-time primality test whose correctness depends on the Extended Riemann Hypothesis. In 1980, Rabin (Rabin 1980) converted Miller's method into an unconditional randomized algorithm. The resulting Miller–Rabin test runs in polynomial time and can make its probability of error arbitrarily small. It is extremely effective in practice, but it does not by itself show that primality testing belongs to P, since an algorithm in P must be deterministic and always correct.

A major deterministic advance came in 1983, when Adleman, Pomerance, and Rumely (Adleman et al. 1983) constructed a primality test with running time

$$(\log k)^{O(\log\log\log k)}.$$

This is only slightly worse than polynomial time, but it is not polynomial. Agrawal, Kayal, and Saxena finally closed the gap by constructing a deterministic algorithm with running time polynomial in $\log k$.

Theorem 1 *There exists a deterministic polynomial-time algorithm for primality testing.*

The starting point of the proof is an elementary consequence of the binomial theorem. If k is prime, then every intermediate binomial coefficient

$$\binom{k}{j}, \qquad 0 < j < k,$$

is divisible by k. Consequently, for every integer a,

$$(x+a)^k \equiv x^k + a \pmod{k}.$$

Equivalently,

$$(x+a)^k - (x^k + a) \in k\mathbb{Z}[x].$$

This polynomial identity can be made computationally useful by also reducing modulo $x^r - 1$. Thus, if k is prime, then for every pair of positive integers a and r,

$$(x+a)^k \equiv x^k + a \pmod{x^r - 1,\ k}. \tag{1}$$

In explicit divisibility form, condition (1) says that there exist polynomials $f, g \in \mathbb{Z}[x]$ such that

$$(x+a)^k - (x^k + a) = (x^r - 1)g(x) + kf(x).$$

Testing the corresponding identity without reducing modulo $x^r - 1$ would be impractical, since the polynomial $(x+a)^k$ has degree k. Reduction modulo $x^r - 1$ replaces it by a polynomial of degree less than r. The central achievement of Agrawal, Kayal, and Saxena was to show that r can be chosen deterministically and bounded by a polynomial in $\log k$. They also showed that it is enough to test the congruence for only polynomially many values of a.

With suitable elementary preliminary checks, these congruences have a powerful converse: if the required identities hold, then k must be a prime power. Since perfect powers can themselves be recognized deterministically in polynomial time, one can distinguish primes from composite prime powers without sacrificing the polynomial running-time bound. Every step of the resulting algorithm is deterministic, and the total number of bit operations is bounded by a polynomial in $\log k$. This proves Theorem 1 and establishes that primality testing belongs to P.

References

Adleman, Leonard M., Carl Pomerance, and Robert S. Rumely. 1983. “On Distinguishing Prime Numbers from Composite Numbers.” *Ann. of Math.* 117: 173–206.

Agrawal, Manindra, Neeraj Kayal, and Nitin Saxena. 2004. “PRIMES Is in P.” *Ann. of Math.* 160 (2): 781–93.

Miller, Gary L. 1976. “Riemann’s Hypothesis and Tests for Primality.” *J. Comput. System Sci.* 13 (3): 300–317.

Rabin, Michael O. 1980. “Probabilistic Algorithm for Testing Primality.” *J. Number Theory* 12 (1): 128–38.