PRIMES is in P

Theorem (Manindra Agrawal, Neeraj Kayal, Nitin Saxena, August 6, 2002). There is a deterministic polynomial-time algorithm for determining whether a number is prime or composite.


Part II (Sept. 26). Details of the new algorithm. The paper is available at

http://www.cse.iitk.ac.in/primality.pdf

See also an exposition by Daniel Bernstein at

http://cr.yp.to/papers.html#aks
Computational Complexities

*input size:* Number of bits $L$ needed to represent input. For an input of number $n$, $L = \lfloor \log_2 n \rfloor + 1$.

*polynomial time:* The number of “bit operations” is $O(L^A)$ for some constant $A$. Complexity class $P$.

<table>
<thead>
<tr>
<th>Operation</th>
<th>run. time</th>
<th>notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>add/sub</td>
<td>$O(L)$</td>
<td></td>
</tr>
<tr>
<td>mult/div</td>
<td>$O(L^2)$</td>
<td>grade school algorithm</td>
</tr>
<tr>
<td></td>
<td>$O(L^{1+\varepsilon})$</td>
<td>Schönhage-Strassen</td>
</tr>
<tr>
<td>gcd$(a,b)$</td>
<td>$O(L^{2+\varepsilon})$</td>
<td>Euclid</td>
</tr>
<tr>
<td>$a^b \mod c$</td>
<td>$O(L^{2+\varepsilon})$</td>
<td>repeated squaring</td>
</tr>
</tbody>
</table>

Here $a, b, c$ have size $\leq L$.

**Primality algorithm:** Input a positive integer $n$, outputs “prime” or “composite”.

**Factoring is much harder.** Fastest algorithm, Number Field Sieve, has (heuristically) a running time of $O(2^{c \sqrt[3]{L}})$.

**First algorithm** (ancient Greece, Euclid and/or Eratosthenes). Divide $n$ by primes (or all numbers) $p \leq \sqrt{n}$. Running time about $\sqrt{n} \approx 2^{L/2}$; “exponential time” algorithm.
Fermat’s (little) Theorem (1640). If $n$ prime and $n \nmid a$, then
\[ a^{n-1} \equiv 1 \pmod{n}. \]

Example:
\[ n = 10^{64} + 1, \ 2^{n-1} \not\equiv 1 \pmod{n} \implies n \text{ is composite}. \]

Is the converse of FT true? No: $2^{340} \equiv 1 \pmod{341}$.

Call $n$ a base $a$ pseudoprime if $a^{n-1} \equiv 1 \pmod{n}$.

Carmichael numbers. These are composite $n$ with $a^{n-1} \equiv 1 \pmod{n}$ for all $a$ with $\gcd(a, n) = 1$. Smallest $n = 561 = 3 \cdot 11 \cdot 17$, discovered by R. D. Carmichael in 1910.

How many Carmichael numbers?

(i) There are 246,683 of them $< 10^{16}$ (R. Pinch).

(ii) There are infinitely many (Alford, Granville, Pomerance 1994).

(iii) Conjecture (Erdős, Pomerance): there are $\gg_{\varepsilon} x^{1-\varepsilon}$ of them up to $x$. 
Lucas tests

Based on properties of *Lucas sequences*, two term recurrence sequences such as the Fibonacci sequence \( f_n \).

Fix \( P, Q \), put \( D = P^2 - 4Q \) and define

\[
u_0 = 0, u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \quad (n \geq 1).
\]

**Theorem (Lucas 1876).** Let \( n > 1 \) be an odd prime, \( n \nmid PQ \), and suppose \( D^{(n-1)/2} \equiv -1 \pmod{n} \). Then \( p|u_{p+1} \).

Example: \( P = 1, Q = -1 \), so \( u_n = f_n \) and \( D = 5 \).

**Fact:** \( 5^{(n-1)/2} \equiv -1 \pmod{n} \) for prime \( n \equiv 2, 3 \pmod{5} \).

Thus, if \( n \equiv 2, 3 \pmod{5} \) and \( n \) is prime, then \( n|f_{n+1} \).

The converse is false: \( 323|f_{324}, \quad 323 = 17 \cdot 19 \).
The $n - 1$ and $n + 1$ primality tests (Lucas, 1876)

The $n - 1$ test: Suppose $\gcd(a, n) = 1$. Then $n$ is prime if both

\[
a^{n - 1} \equiv 1 \pmod{n},
\]

\[
a^{(n - 1)/q} \not\equiv 1 \pmod{n} \text{ for all prime } q | (n - 1).
\]

If particular, $a$ has multiplicative order $n - 1$ modulo $n$.

The $n + 1$ tests: Sample theorem: Suppose $n \equiv 2, 3 \pmod{5}$. Then $n$ is prime if both

\[
n | f_{n + 1},
\]

\[
\gcd(f_{(n+1)/q}, n) = 1 \text{ for all prime } q | (n + 1).
\]

Disadvantages: Requires factorization of $n - 1$ or $n + 1$.

Advantages: Works great for numbers $n$ of special forms such as Fermat numbers $2^{2^k} + 1$ or Mersenne numbers $2^p - 1$.

Lucas (1876): $2^{127} - 1$ is prime (computation by hand).

Largest known prime: $2^{13466917} - 1$ (computation not by hand).
Partial Factorizations

**Idea:** $n \pm 1 = FU$, $F$ is factored part, $U$ is unfactored part.

**Pocklington (1914).** Tests requiring only $F > \sqrt{n}$.

**Brillhart, Lehmer, Morrison, Selfridge (1970s).** Tests requiring only (i) $F > n^{1/3}$ or (ii) $n^2 - 1 = (n-1)(n+1) = FU$ with $F > 4(\sqrt{n} + 1)$.

**H. Williams (1978).** Tests based on partial factorization of $n^6 - 1$ and $n^k - 1$ for a few other $k$.

**Adleman, Pomerance, Rumely (1983)** Test based on properties of Gauss and Jacobi sums, requires $n^I - 1 = FU$ with $F > n$, but $I$ is arbitrary. Complexity increases with $I$.

**H. W. Lenstra (1985)** Test based on arithmetic of finite fields, also requires $n^I - 1 = FU$ with $F > n$. Complexity increases with $I$.

Note: By Fermat, if $p$ is prime and $(p - 1)|I$ then $p|(n^I - 1)$.

**Theorem (APR 1983).** For large $n$ and a constant $c > 0$,

$$\prod_{(p-1)|I} p > n$$

for some $I \approx (\log n)^{c \log \log \log n}$.

**Corollary** There is a primality test with a running time of $O(L^{c \log \log L})$ for some $c > 0$. (Fastest provable running time before AKS).
The Strong Pseudoprime Test

M. Artjuhov (1966); popularized by J. Selfridge in early 1970s. Based on Fermat plus \( x^2 \equiv 1 \pmod{p} \implies x \equiv \pm 1 \pmod{p} \).

The test: Take \( a \) with \( \gcd(a, n) = 1 \), write \( n - 1 = 2^s d \), \( d \) odd. If \( a^d \equiv 1 \) or \( a^{d2^r} \equiv -1 \pmod{n} \) for some \( 0 \leq r \leq s - 1 \), call \( n \) a strong pseudoprime to base \( a \). If not, \( n \) is composite (call \( a \) a witness to the compositeness of \( n \)).

Fact: There are no “strong Carmichael numbers”.

Theorem (Rabin, Monier, 1980). If \( n \) is composite, \( n \) is a strong pseudoprime to at most \( \frac{1}{4} \phi(n) \) of the bases \( a \) with \( 1 \leq a \leq n, \gcd(a, n) = 1 \). Consequently, if \( n \) passes \( k \) such tests (\( k \) different \( a \)), the “probability” that \( n \) is composite is \( (1/4)^k \).

For composite \( n \), let \( w(n) \) be the least witness for \( n \).

Theorem (R. Burthe, 1995) \( w(n) = O(n^{1/(6\sqrt{e}) + \varepsilon}) \); \( w(n) = 2 \) for almost all composite \( n \).

Theorem (G. Miller, 1976) If ERH is true, then \( w(n) = O(\log^2 n) \). Consequently, if ERH is true, then the strong pseudoprime test (trying all \( a \leq c \log^2 n \)) is a polynomial time algorithm for primality.

Fact: the smallest composite number which is a strong pseudoprime to bases 2, 3, 5, 7, 11, 13 and 17 is 341, 550, 071, 728, 321.
Other tests


Fastest deterministic algorithm in practice.

Assuming some conjectures about Elliptic curves, it also has a polynomial running time.

Frobenius tests (J. Grantham, 1998). Same general principle as the strong pseudoprime test, but a composite \( n \) is a Frobenius pseudoprime for at most \( 1/7700 \) of the possible bases.

A curiosity. There is no known composite \( n \cong 3, 7 \pmod{10} \) which is both a strong pseudoprime to base 2 and satisfies \( n \mid f_{n+1} \).
The Agrawal-Kayal-Saxena algorithm

**Input:** A large positive odd integer \( n \).

**Output:** PRIME or COMPOSITE.

1. Put \( L = \lfloor \log_2 n \rfloor + 1 \). Test if \( n = m^k \) for some integers \( m \) and \( k \geq 2 \). If so, output COMPOSITE and stop.

2. Let \( s \) run through the primes: 2, 3, 5, \ldots until one of two conditions is met:
   - (2a) \( \gcd(n, s) > 1 \). Output COMPOSITE and stop.
   - (2b) The largest prime factor \( q \) of \( s - 1 \) satisfies \( q \geq 6\sqrt{sL} \) and \( n^{(s-1)/q} \not\equiv 1 \pmod{s} \). Put \( r = s \) and go to step 3.

3. For integers \( b, 1 \leq b \leq B := \lfloor 3\sqrt{rL} \rfloor \), check that

\[
(1) \quad (x + b)^n \equiv x^n + b \pmod{n, x^r - 1},
\]

that is, check that \((x + b)^n = x^n + b\) in the polynomial ring \((\mathbb{Z}/n\mathbb{Z})[x]/(x^r - 1)\). If (1) is satisfied for all such \( b \), output PRIME. Otherwise, output COMPOSITE.
Running time of the algorithm

Step 1. Computing \( \lfloor \sqrt{n} \rfloor \) takes \( O(L^{1+\varepsilon}) \) time, using Newton’s method. There are \( O(L) \) possible values of \( k \) to check, total time \( O(L^{2+\varepsilon}). \)

\( O(L^{1+\varepsilon}) \) algorithm: D. J. Bernstein, Detecting perfect powers in essentially linear time, Mathematics of Computation 67 (1998), 1253-1283.

Step 2. Suppose one stops at the prime \( r \):

(i) Time to create list of primes \( s \leq r \) together with largest prime factors of \( s-1 \): \( O(r^{1+\varepsilon}) \) by sieve of Eratosthenes.

(ii) Time to compute each \( n^{(s-1)/q} \mod s \): \( O(L^{1+\varepsilon}) \) to compute \( n \mod s \), then \( O((\log r)^{2+\varepsilon}) \) to compute \( n^{(s-1)/q} \mod s \).

Time for step 2: \( O(r^{1+\varepsilon}L^{1+\varepsilon}). \)

Step 3. First, \( x^n \equiv x^n \mod r \mod (x^r - 1) \). Computing \( n \mod r \) takes \( O(L^{1+\varepsilon}) \) time. For each \( b \), there are \( O(L) \) multiplications needed in \( (\mathbb{Z}/n\mathbb{Z})[x]/(x^r - 1) \). FFT can be used to multiply the polynomials, involving \( O(r^{1+\varepsilon}) \) integer multiplications, each taking \( O(L^{1+\varepsilon}) \) time. Time for step 3: \( O(r^{3/2+\varepsilon}L^{3+\varepsilon}) \).

Total time for all steps: \( O(r^{3/2+\varepsilon}L^{3+\varepsilon}) \).
Goldfeld’s Theorem

**Theorem** (M. Goldfeld, 1969). $N(x, y) :=$ number of primes $p \in (x, 2x]$ with $p - 1$ having a prime factor $> y$. For some $\theta > 1/2$, $c > 0$ and $x \geq x_0$,

$$N(x, x^\theta) \geq c \frac{x}{\ln x}.$$

**Brun-Titchmarsh Theorem.** The number, $\pi_{q,a}(x)$, of primes $p \leq x$, $p \equiv a \pmod{q}$ is $\leq K\frac{x}{\varphi(q)\ln(x/q)}$.

$K = 2 + \varepsilon$ (Selberg, 1946); $K = 2$ (Montgomery & Vaughan, 1973)

**Bombieri-Vinogradov Theorem** (1965). $\forall A > 0$, $\exists B > 0$:

$$\sum_{q \leq \frac{x}{\ln b} \atop q \leq B} \max_{y \leq x} \left| \pi_{q,b}(y) - \frac{\text{li}(y)}{\varphi(q)} \right| = O(x(\log x)^{-A}).$$

Goldfeld’s Theorem with $\theta = 0.61$: Let $M = \prod_{x < p \leq 2x} (p - 1)$. By Prime Number Theorem, $M = e^{(1+o(1))x}$. By the Bombieri-Vinogradov and Brun-Titchmarsh theorems, the prime factors of $M$ that are $< x^\theta$ contribute to $M$ at most $e^{(\mu+o(1))x}$, $\mu = 1/2 + K \ln \frac{1}{2-2\theta}$. If $\theta \leq 0.61$, there must be many prime factors of $M$ that are $> x^\theta$.

Improvements: $\theta = 2/3$ (Fouvry, 1985); $\theta = 0.677$ (Baker and Harman, 1998).
Bounding $r$

**Lemma.** $r = O(L^\alpha)$, $\alpha = \frac{1}{\theta-1/2}$.

**Proof.** In fact, (2b) must be satisfied for some $s = O(L^\alpha)$. For some $c_1, c_2, n_0$ : if $n \geq n_0$, there is a set $S$ of at least $c_1 L^\alpha / \ln L$ primes $s \in (c_2 L^\alpha, 2c_2 L^\alpha]$ with $s - 1$ divisible by a prime $q \geq (c_2 L^\alpha)^\theta \geq 6\sqrt{sL}$. For each $s \in S$, $\frac{s-1}{q} \leq H = c_4 L^{\alpha/2-1}$. But

$$\prod_{i=1}^{H} (n^i - 1) \leq n^{H^2} \leq 2^{c_5 L^\alpha-1},$$

so the left side is divisible by at most $c_5 L^\alpha-1 = o(L^\alpha / \ln L)$ primes. Thus, at least one $s \in S$ does not divide the left side, i.e. $n^{(s-1)/q} \not\equiv 1 \pmod{s}$.

**Total running time:** $O(L^{3+3\alpha/2+\varepsilon}) = O(L^{12+\varepsilon})$ with $\theta = \frac{2}{3}$.

**Conjecture:** $r = O(L^2)$; namely for some $s \in (c_6 L^2, 2c_6 L^2]$, $\frac{s-1}{2} = q$ is prime (a so-called Sophie Germain prime): this would yield a running time of $O(L^{6+\varepsilon})$. 
Correctness of the algorithm

I. If the algorithm outputs COMPOSITE, $n$ is composite.
True for Step 1. True for Step 2a, since for large $n$, $r < n$. Step 3 is based on

**Lemma** Let $(b,n) = 1$. $n$ is prime iff the polynomial congruence

\[(x + b)^n \equiv x^n + b \pmod{n}\]

holds.

**Proof** $\implies$: Fermat plus binomial theorem. $\Leftarrow$: if $q^k \mid n$, $q^k \nmid \binom{n}{q}$.

Since $b < r$ and $(s,n) = 1$ for prime $s \leq r$ (Step 2), if $n$ is prime then $(x + b)^n \equiv x^n + b \pmod{n}$ for all such $b$.

II. If the algorithm outputs PRIME, $n$ is prime.

Basically, (2) takes time at least $O(n)$ to check, so the polynomials are reduced modulo $x^r - 1$ for (1). Checking (1) is much faster, but cannot determine if $n$ is prime. However, by verifying (1) for many different $b$’s, one can conclude that $n$ is prime. This is an analog of using different bases $b$ in the strong pseudoprime test, but the result is unconditional.
Proof that output=PRIME $\implies n$ is prime

A. Take $r$ and $q$ from step 2b. $\exists p | n$ with $p^{(r-1)/q} \neq 0, 1 \pmod{r}$ and therefore the order of $p$ modulo $r$ is $\geq q \geq 6\sqrt{r}L$.

B. For $1 \leq b \leq B$ and $i, j \geq 0$,

$$(x + b)^{n^i p^j} \equiv x^{n^i p^j} + b \pmod{p, x^r - 1}.$$  

Proof: By (1) with $x \rightarrow x^{n^i}$,

$$(x^{n^i} + b)^n \equiv x^{n^{i+1}} + b \pmod{p, x^{rn^i} - 1}.$$  

Since $(x^r - 1)|(x^{rn^i} - 1)$, the congruence holds $(\pmod{p, x^r - 1})$ as well. By induction, $(x + b)^{n^i} \equiv x^{n^i} + b \pmod{p, x^r - 1}$ for all $i \geq 0$. By Fermat’s Theorem and binomial theorem,

$$(x + b)^{n^i p^j} \equiv (x^{n^i} + b)^{p^j} \equiv x^{n^i p^j} + b \pmod{p, x^r - 1}.$$  

C. There are $> r$ products $n^i p^j$ with $0 \leq i, j \leq \lfloor \sqrt{r} \rfloor$. For two distinct pairs $(i, j)$, $(k, \ell)$, $n^i p^j \equiv n^k p^\ell \pmod{r}$. Put $t = n^i p^j$, $u = n^k p^\ell$, so that for $1 \leq b \leq B$ we have

$$(3) (x + b)^t \equiv x^t + b \equiv x^u + b \equiv (x + b)^u \pmod{p, x^r - 1}.$$
D. Let \( h(x) \) be an irreducible polynomial in \( \mathbb{F}_p[x] \) dividing \( \frac{x^r-1}{x-1} \). Since \( \mathbb{F}_p[x]/h \) is a finite field of size \( p^v \), \( v = \deg h \), we find that \( v \) is the order of \( p \) modulo \( r \), which is \( \geq q \).

E. By (3), \( (x+b)^t = (x+b)^u \) in \( \mathbb{F}_p[x]/h \); the monomials \( x+b \) are distinct elements of \( (\mathbb{F}_p[x]/h)^* \), since \( v \geq 2 \) and \( \gcd(n, b_1 - b_2) = 1 \) for \( 1 \leq b_1 < b_2 \leq B \). Let \( G \) be subgroup of \( (\mathbb{F}_p[x]/h)^* \) generated by the monomials \( x+b \) for \( 1 \leq b \leq B \). \( G \) is cyclic and \( |G| \geq (q+B-1)_B^B \): namely \( G \) contains all products \( \prod_{b=1}^B (x+b)^{\nu_b} \) where \( \sum \nu_b \leq q-1 \) and each \( \nu_b \geq 0 \).

F. Since \( q \geq 2B \),

\[
\left( \frac{q+B-1}{B} \right) \geq \left( \frac{3B-1}{B} \right) \geq \frac{(2B)^B}{B^B} \geq \frac{1}{2} n^{2\sqrt{r}} > n^{2\sqrt{r}}.
\]

On the other hand,

\[
|t-u| \leq n^{\sqrt{r}} p^{\sqrt{r}} \leq n^{2\sqrt{r}} < |G|.
\]

But \( g^t = g^u \forall g \in G \), so \( |G| \) divides \( |t-u| \). Therefore, \( t = u \), i.e. \( n^i p^j = n^k p^\ell \). Since \( i \neq k \), \( n \) is a power of \( p \). By Step 1, \( n = p \).