Proving primality

D. J. Bernstein
University of Illinois at Chicago

Thm (Agrawal, Kayal, Saxena 2002):
"PRIMES $\in$ P."

i.e. there is a deterministic polynomial-time algorithm A such that $A(s) = 1$ iff s is the decimal expansion of a prime number.

Proving compositeness

e.g. 3141592653589793238
is not prime.

e.g. 314159265358979323
is not prime:
it is $317213509 \cdot 990371647$.

Thm: Assume that

$a > 1$, $b > 1$, and $ab = n$.

Then n is not prime.

For every non-prime n:

can find suitable a, b

by trying all a's in

$\left\{2, 3, \ldots, \left\lfloor\sqrt{n}\right\rfloor\right\}$.

Verifying compositeness proof:
log time $\asymp \log d$
where d is length of input.
"PRIMES $\in$ coNP."

Finding compositeness proof:
log time $\asymp d$.

One way to prove primality:
Fail to prove compositeness;
log time $\asymp d$.

Faster factoring

Many ways to find a
more quickly than trial division.

Number field sieve: conjectured
log time $\asymp d^{1/3}(\log d)^{2/3}$.

Compositeness without factoring

Thm (Fermat):
Assume that $a^n \neq a$ in $\mathbf{Z}/n$.
Then n is not prime.

e.g. $n = 314159265358979323$
is not prime:
$2^n = 198079119221837432 \neq 2$
in $\mathbf{Z}/n$.

Represent $\mathbf{Z}/n$ as $\{0, 1, 2, \ldots, n-1\}$.

Computing powers in $\mathbf{Z}/n$ takes log time $\asymp \log d$.

e.g. in $\mathbf{Z}/35621$: $2^{12900} = 509$ so $2^{25800} = 509^2 = 259081 = 9734$.

Quickly proves compositeness of *most* non-primes n.

But some non-primes n have $2^n = 2$ in $\mathbf{Z}/n$.
Some non-primes n ("Carmichael numbers") have $a^n = a$ in $\mathbf{Z}/n$ for all a.

e.g. $2821 = 7 \cdot 13 \cdot 31$;
but $2^{2821} = 2$ in $\mathbf{Z}/2821$.

Thm (Artjuhov 1966, et al.):
Assume that $n \in 5 + 8\mathbf{Z}$ and that a, $a^{(n-1)/2} + 1$, $a^{(n-1)/4} + 1$, $a^{(n-1)/4} - 1$ are nonzero in $\mathbf{Z}/n$.
Then n is not prime.

e.g. in $\mathbf{Z}/2821$: $2^{1410} + 1 = 1521$; $2^{705} + 1 = 2606$; $2^{705} - 1 = 2604$.

Cover all n using similar tests for $n \in 3 + 4\mathbf{Z}$, $n \in 9 + 16\mathbf{Z}$, etc.

For every non-prime n:
if generalized Riemann hypothesis is true, can find $a \leq 70(\log n)^2$.
(Miller 1976; Oesterlé 1979)

Trying all these a's takes log time $\asymp \log d$.

“GRH implies PRIMES $\in$ P.”

For every non-prime n:
most a's work.
(Rabin 1976; Monier 1980;
Atkin, Larson 1982; similar:
Solovay, Strassen 1977)

Try $100d$ uniform random a's;
negligible chance of failure;
log time $\asymp \log d$.
"PRIMES $\in$ coRP."

Can eliminate randomness by generating "pseudorandom" sequence of a's for n.

If generator is cryptographically strong then algorithm never fails.

"If there is a strong PRNG then BPP = coRP = RP = P." (basic idea: Yao 1982)

Proving primality

Thm (Lucas 1876): Assume that
$n > 1$; $a^{n-1} = 1$ in $\mathbf{Z}/n$;
and $a^{(n-1)/q} \neq 1$ in $\mathbf{Z}/n$
for every prime q dividing $n - 1$.
Then n is prime.

e.g. $n = 1000003$ is prime:
$n - 1 = 2 \cdot 3 \cdot 166667$;
$2, 3, 166667$ are prime;
in $\mathbf{Z}/n$: $2^{n-1} = 1$, $2^{(n-1)/2} \neq 1$,
$2^{(n-1)/3} \neq 1$, $2^{(n-1)/166667} \neq 1$.

If n is prime
then can find a and q's.

Verifying primality proof:
log time $\asymp \log d$.
"PRIMES $\in$ NP."

Finding primality proof is slow.
Much faster if $n - 1$ factors nicely.

Partial factorization of $n-1$
is sufficient. (Pocklington 1914)

Or n^2-1. (Morrison 1975;
Brillhart, Lehmer, Selfridge 1975)

Proving primality with Jacobi sums
using n^6-1, $n^{24}-1$, etc.:
log time $\asymp \log d \log\log d$.
(Adleman, Pomerance, Rumely
1979)

Replace unit group with random elliptic-curve group. Conjecturally negligible chance of failure; log time $\asymp \log d$.

"If primes are well distributed then PRIMES $\in$ RP."

(Goldwasser, Kilian 1986; relying on Schoof 1985)

Replace elliptic-curve group with group of points on Jacobian of genus-2 hyperelliptic curve. Negligible chance of failure; log time $\asymp \log d$.

"PRIMES $\in$ RP."

(Adleman, Huang 1992)

Thm (Agrawal, Kayal, Saxena 2002):

Assume that q and r are prime,

q divides $r-1$,

$n^{(r-1)/q} \bmod r \notin \{0,1\}$,

and $\binom{q+s-1}{s} \geq n^{2\lfloor\sqrt{r}\rfloor}$.

If n has no prime divisors $< s$,

and $(x+b)^n = x^n + b$

in the ring $(\mathbf{Z}/n)[x]/(x^r-1)$

for all $b \in \{0,1,\ldots,s-1\}$,

then n is a power of a prime.

Find q, r, s with $rs \in (\log n)^{10+o(1)}$.
Check remaining conditions.
Proves that n is prime,
or proves that n is composite.

Bottleneck in computation:
$s \log_2 n$ multiplications of
huge integers, each $\approx 2r \log_2 n$ bits.
Time $r^{1+o(1)} s (\log n)^{2+o(1)}$;
$\log \text{time} \asymp \log d$.

Life after “PRIMES $\in$ P”

Simplified proof. (Lenstra)

Polynomial time does *not* mean fast.
In practice, use coRP tests.
For proofs, use Jacobi sums.

Trying to make AKS competitive:
$\approx 450\times$ speedup (Bernstein);
$\approx 1000\times$ additional speedup
(Lenstra, Poonen, Voloch); more?