PRIMES is in P

Manindra Agrawal
NUS Singapore / IIT Kanpur

The Problem

Given number n, test if it is prime efficiently.

Efficiently = in time a polynomial in number of digits

= $(\log n)^c$ for some constant c

The Trial Division Method

Try dividing by all numbers up to $n^{1/2}$.

- takes exponential time: $\Omega(n^{1/2})$.
- Also produces a factor of n when it is composite.

A Possible Approach

Find a characterization of prime numbers that is efficiently verifiable

- Many characterizations of primes have been obtained over centuries.
- But none were provably efficient until recently.

Wilson's Characterization (18th century)

n is prime

iff

$(n-1)! = -1 \pmod{n}$

- Requires O(n) operations

Fermat's Little Theorem (17th century)

n is prime

implies

for any a:

$a^n = a \pmod n$.

It is easy to check:

Compute a^2, square it to a^4, square it to a^8, …

Needs only $O(\log n)$ multiplications.

An Efficient but Wrong Characterization

n is prime

iff

for $0 < a < 4 \log^2 n$: $a^n = a \pmod n$

- Requires only $O(\log^3 n)$ multiplications and divisions.
- Fails on Carmichael numbers, e.g., 561 = 3 * 11 * 17.

Lucas' Characterization (1891)

n is prime

iff

for every prime divisor q of n-1:

there is an $1 < a < n$ such that

$a^{n-1} = 1 \pmod{n}$ and $\gcd(a^{(n-1)/q} - 1, n) = 1$

- Based on FLT
- It is inefficient: requires factorization of n-1

An NP ∩ coNP Algorithm

- A trivial algorithm shows that the set is in coNP: given a factor of n it is easy to verify that n is composite.

- [Pratt, 1974] Lucas' characterization yields an NP algorithm: guess a prime factorization of n-1; recursively verify its correctness; and guess an a with required properties.

Miller's (unproven) Characterization (1975)

$n = 1 + 2^t * s$ is odd prime

iff

for $0 < a < 4 \log^2 n$:

either $a^s = 1 \pmod n$

or $a^{2^k * s} = -1 \pmod n$ for some $0 \leq k < t$

Yields an Efficient Algorithm

- Based on FLT
- Yields an efficient algorithm: $O(\log^4 n)$ steps
- It is correct assuming Generalized Riemann Hypothesis

coRP Algorithms

- [1974] Solovay-Strassen gave the first unconditional but randomized polynomial time algorithm.
  - This algorithm might give a wrong answer with a small probability when n is composite.
- [1975] Rabin modified Miller's characterization to obtain another algorithm with similar properties.

An Almost Efficient Characterization

- [1983] Adleman, Pomerance, and Rumely gave a (rather complicated) characterization that yields a deterministic algorithm running in time $(\log n)^{c \log\log\log n}$.

An Efficient Chracterization

[2002] A., Kayal, Saxena gave the first deterministically verifiable efficient characterization.

Starting Point: A Polynomial based Characterization

n is prime

iff

$(X + 1)^n = X^n + 1 \pmod n$

Proof: $(X+1)^n - X^n - 1 = \sum_{j=1}^{n-1} \binom{n}{j} X^j$

If n is prime then all coefficients are divisible by n.

If n is composite then at least one is not.

- A generalization of FLT to polynomials.
- Simple and elegant.
- Inefficient: although requires only $O(\log n)$ polynomial multiplications, intermediate polynomials are of large degree.

A Way to Reduce Space

- Test the equation modulo $X^r - 1$ for a small r.
- Or, more generally, test if

$$(X + a)^n = X^n + a \pmod{n, X^r - 1}$$

For a few a's and a few small r's.

It Almost Works

n is prime

iff

for any r such that $O_r(n) > 4 \log^2 n$:

n has no divisor smaller than min(n,r) and

for every a, $1 \le a \le 2 \sqrt{r} \log n$:

$(X + a)^n = X^n + a \pmod{n, X^r - 1}$

$O_r(n)$ = smallest k with $n^k = 1 \pmod{r}$.

The Algorithm

Input n.

1. Find the smallest number r such that $O_r(n) > 4 (\log n)^2$.
2. If any number $< r$ divides n, output PRIME/COMPOSITE appropriately.
3. For every $a \leq 2\sqrt{r} \log n$:
   - If $(X+a)^n \neq X^n + a \pmod{n, X^r - 1}$ then output COMPOSITE.
4. Output PRIME.

Correctness: Non-trivial Part

Assume:

- r is given such that $O_r(n) > 4(\log n)^2$.
- Smallest prime dividing n is at least min(n,r).
- $(X+a)^n = X^n + a \pmod{n, X^r-1}$ for $0 < a \leq 2\sqrt{r} \log n$.

- Fix a prime p dividing n with $p \geq r$ and $O_r(p) > 1$.
- Clearly, $(X+a)^n = X^n + a \pmod{p, X^r-1}$ too for $0 < a \leq 2\sqrt{r} \log n$.
- And of course, $(X+a)^p = X^p + a \pmod{p, X^r-1}$ (according to previous prime characterization)

Introspective Numbers

- We call any number m such that $g(X)^m = g(X^m) \pmod{p, X^r-1}$ an introspective number for $g(X)$.

- So, p and n are introspective numbers for $X+a$ for $0 < a \leq 2\sqrt{r} \log n$.

Introspective Numbers Are Closed Under *

Lemma: If s and t are introspective for g(X), so is s * t.

Proof:

$$g(X)^{st} = g(X^s)^t \pmod{p, X^r - 1}, \text{ and}$$

$$g(X^s)^t = g(X^{st}) \pmod{p, X^{sr} - 1}$$

$$= g(X^{st}) \pmod{p, X^r - 1}.$$

So There Are Lots of Them

- Let $I = \{ n^i * p^j \mid i, j \geq 0 \}$.

- Every m in I is introspective for X+a for $0 < a \leq 2\sqrt{r} \log n$.

Introspective Numbers Are Also For Products

Lemma: If m is introspective for both g(X) and h(X), then it is also for g(X) * h(X).

Proof:

$$(g(X) * h(X))^m = g(X)^m * h(X)^m$$
$$= g(X^m) * h(X^m) \pmod{p, X^r-1}$$

So Introspective Numbers Are For Lots of Polynomials

- Let $Q = \{ \prod_{a=1,\, 2\sqrt{r}\log n} (X + a)^{e_a} \mid e_a \geq 0 \}$.

- Every m in I is introspective for every g(X) in Q.

Finite Fields Facts

- Let $h(X)$ be an irreducible divisor of r^{th} cyclotomic polynomial $C_r(X)$ in the ring $F_p[X]$:
  - $C_r(X)$ divides X^r-1.
  - Polynomials modulo p and $h(X)$ form a field, say F.
  - $X^i \neq X^j$ in F for $0 \leq i \neq j < r$.

Moving to Field F

- Since h(X) divides X^r-1, equations for introspective numbers continue to hold in F.

- We now argue over F.

Two Sets in Field F

- Let $G = \{ X^m \mid m \in I \}$.
  - Every element of G is an rth root of unity.
  - $t = |G| \geq O_r(n) > 4 \log^2 n$.

- Let $H = \{ g(X) \pmod{p, h(X)} \mid g(X) \in Q \}$.
  - H is a multiplicative group in F.

H is large …

- Let Q_t be set of all polynomials in Q of degree < t.

Lemma: There are > $n^{2\sqrt{t}}$ distinct polynomials in Q_t:

- Consider all products of X+a's of degee < t.
- There are $\binom{t+2\sqrt{r}\log n-1}{2\sqrt{r}\log n-1}$ > $\binom{4\sqrt{t}\log n}{2\sqrt{t}\log n}$ > $n^{2\sqrt{t}}$ of these (since r > t and $\sqrt{t}$ > 2 log n).

… because Q_t injects into F

- Let $f(X)$, $g(X)$ in Q_t with $f(X) \neq g(X)$.
- Suppose $f(X) = g(X)$ in F. Then:
  - For every X^m in G, $f(X^m) = f(X)^m = g(X)^m = g(X^m)$ in F.
  - So polynomial $P(z) = f(z) - g(z)$ has $|G| = t$ roots in F.
  - Contradiction, since $P(z) \neq 0$ and degree of $P(z)$ is $< t$.

… implies that I has few small numbers

- Let $m_1, m_2, \ldots, m_k$ be numbers in $I \leq n^{2\sqrt{t}}$.
- Suppose $k > t$.
- Then, there exist m_i and m_j, $m_i > m_j$, such that

$$X^{m_i} = X^{m_j} \text{ (in } F)$$

I: set of introspective numbers	$F = F_p[X]/(h(X)),\ h(X) \mid X^r-1$
Q: set of introspective polynomials	$G = X^I$ $\quad H = Q \pmod{h(X)}$

- Let $g(X)$ be any element of H.
- Then:

$$g(X)^{m_i} = g(X^{m_i}) = g(X^{m_j}) = g(X)^{m_j} \text{ (in } F)$$

- Therefore, $g(X)$ is a root of the polynomial $P(z) = z^{m_i} - z^{m_j}$ in the field F.

I: set of introspective numbers	$F = F_p[X]/(h(X)),\ h(X) \mid X^r-1$
Q: set of introspective polynomials	$G = X^I$ $\quad H = Q \pmod{h(X)}$

- Since H has more than $n^{2\sqrt{t}}$ elements in F, P(Y) has more than $n^{2\sqrt{t}}$ roots in F.

- Contradiction, since $P(z) \neq 0$ and degree of $P(z) = m_i \leq n^{2\sqrt{t}}$.

I: set of introspective numbers	$F = F_p[X]/(h(X)),\ h(X) \mid X^r-1$
Q: set of introspective polynomials	$G = X^I$ $\quad H = Q \pmod{h(X)}$

… so n must be a prime power!

- Consider numbers $n^a * p^b$ with $0 \le a, b \le \sqrt{t}$.
- Each such number is $\le n^{2\sqrt{t}}$ ("small").
- So there are $\le t$ ("few") such numbers.
- This gives a, b, c, d with

  $(a,b) \neq (c,d)$ and $n^a * p^b = n^c * p^d$
- Therefore, $n = p^e$ for some $e > 0$.

I: set of introspective numbers

Q: set of introspective polynomials

$F = F_p[X]/(h(X)),\ h(X) \mid X^r-1$

$G = X^I$

$H = Q \pmod{h(X)}$

This forces n to be prime

Lemma [Hendrik Lenstra Jr.,1983]: If $a^n = a \pmod n$ for $1 \le a \le 4 \log^2 n$ then n is square-free.

Since

$(X+a)^n = X^n + a \pmod{n, X^r-1}$ for $0 < a \le 2\sqrt{r} \log n$,

we have

$$a^n = a \pmod n \text{ for } 0 < a \le 4 \log^2 n,$$

(as $r > 4 \log^2 n$). So n must be square-free.

The Choice of r

- We need r such that $O_r(n) > 4 (\log n)^2$.
- Any r such that $O_r(n) \leq 4 (\log n)^2$ must divide

$$\Pi_{k=1,\, 4 \log^2 n} (n^k - 1) < n^{16 \log^4 n} = 2^{16 \log^5 n}.$$

- By Chebyshev's prime density estimates the lcm of first m numbers is at least 2^m (for $m > 7$).
- Therefore, there must exist an r that we desire $\leq 16 (\log n)^5 + 1$.

Time Complexity

- Step 3 dominates running time.
  - It needs to verify $O(\sqrt{r} \log n)$ equations.
  - Each equation needs $O^{\sim}(r \log^2 n)$ time to verify.
- So time complexity is $O^{\sim}(r^{1.5} \log^3 n) = O^{\sim}(\log^{10.5} n)$.

- Using a result of Fouvry, one can show that $r = O(\log^3 n)$ is enough.
  - The result shows that primes r such that $r-1$ has a large prime divisor have high density.
- This brings time complexity down to $O^{\sim}(\log^{7.5} n)$.

A Cleaner Characterization

- The characterization is a bit messy.
- Three different conditions need to hold:
  - r needs to be such that $O_r(n) > 4 (\log n)^2$
  - No prime divisor of n is smaller than $\min(n,r)$
  - For every a, $1 \le a \le \sqrt{r} \log n$:

$$(X + a)^n = X^n + a \pmod{n, X^r - 1}$$

- Can these be combined into a single equation?

Yes!

Use the equation

$$(X + 1)^n = X^n + 1 \pmod{n, Q(X)}$$

for appropriate small dgree $Q(X)$.

Eliminating Condition on r

Try for all $r \leq 16 \log^5 n$!

Eliminating Small Divisors

Lemma: If $(X + 1)^n = X^n + 1 \pmod{n, X^r}$ then n has no divisor less then min(n,r).

Proof: If prime $p < \min(n,r)$ divides n, then $(X + 1)^n = 1 + n/p\, X^p + \ldots \pmod{n, X^r} \neq 1 \pmod{n, X^r}$.

Eliminating Multiple Equations

Lemma: $(X + 1)^n = X^n + 1 \pmod{n, Q(X-a)}$ for $0 < a \leq B$ iff

$(X + a)^n = X^n + a \pmod{n, Q(X)}$ for $1 < a \leq B+1$.

Proof: Assume for $B-1$. Then:

$(X + 1)^n = X^n + 1 \pmod{n, Q(X-B)}$ iff

$(X+B+1)^n = (X+B)^n + 1 \pmod{n, Q(X)}$ iff

$(X+B+1)^n = X^n + B + 1 \pmod{n, Q(X)}$

Putting These Together …

n is prime

iff

$(X + 1)^n = X^n + 1 \pmod{n, Q(X)}$

where

$$Q(X) = X^{16\log^5 n} * \prod_{r=1}^{16\log^5 n} \prod_{a=1}^{2\sqrt{r}\log n} ((X-a)^r - 1)$$

- Degree of Q(X) is $O(\log^{27/2} n)$.

Further work

- [Lenstra-Pomerance,2003]: $r = O(\log^2 n)$ is enough with a different polynomial of degree r than X^r-1.
  - This improves time complexity to $O\tilde{}(\log^6 n)$.
- [Berrizbeitia-Bernstein,2003]: Randomized primality proving algorithm with time complexity $O\tilde{}(\log^4 n)$.

Further Improvement?

- Conjecture:

n is prime

iff

n is not a prime power,

$n \neq 1 \pmod{r}$ for some prime $r > \log n$,

and $(X-1)^n = X^n - 1 \pmod{n, X^r - 1}$

- Yields a $O^{\sim}(\log^3 n)$ time algorithm.