Certifying Primality + Randomized algorithms for primality.

Thm There is an algorithm $A(n, w)$ s.t. for any t-bit integer n;

$A(n, w)$ runs in time $\text{poly}(t)$ and:

(1) If n is prime, $\exists\, w \in \{0,1\}^{\text{poly}(t)}$ s.t. $A(n, w)$ ACCEPTS

(2) If n is not prime, then for all $w \in \{0,1\}^{\text{poly}(t)}$, $A(n, w)$ REJECTS.

Pratt '70s.

Proof

Let $\mathbb{Z}_n^* = \{ a : 1 \le a < n \text{ s.t. } GCD(a, n) = 1 \}$

operation = multiplication mod n

n is prime iff $|\mathbb{Z}_n^*| = n-1$.

and $\exists\, g \in \mathbb{Z}_n^*$

$\mathbb{Z}_n^* = \{1, g, g^2, \ldots, g^{n-2}\}$

Proposal Give g as certificate of primality.

Need to verify that g has order = n-1.

Claim (*) Let H be a group. Let $h \in H$. Then order (h) equals m iff:

$$h^m = 1$$

and for all primes $q \mid m$,

$h^{m/q} \neq 1$.

Intended Certificate for n (when n is prime):

g – a generator of $\mathbb{Z}_n^*$

a prime factorization $\prod q_i^{e_i}$ of $n-1$

Recursively, Certificates of primality for all $q_i \geq 10$.

Verification algorithm

- Check that $g^{n-1} \equiv 1 \pmod n$
- Check that $g^{\frac{n-1}{q_i}} \neq 1 \pmod n$
- Check that $\prod q_i^{e_i} = n-1$. for all i.
- Check that all q_i are prime using their certificates.

If any check fails, REJECT, else ACCEPT.

Correctness

If n is prime, clearly this accepts with the

intended certificate

If n is not prime, then if
prime
the factorization of $n-1$ is correct,
Claim ⊛ $\Rightarrow$ order of g in $\mathbb{Z}_n^*$

is $n-1$, contradiction to
nonprimality.

If factorization is wrong, then

Some q_i is not prime.

and the recursive check
for that q_i's primality
will catch it.

Runtime / Certificate size.

$C(n)$ = certificate size for input
n.

$$C(n) \leq \log n + O(\log n) + \sum_{i=1}^{\ell} C(q_i)$$

$q_1, q_1, \ldots q_1$ .. e_1 times

$q_2 q_2 \ldots$ e_2 times

$\vdots$

$$\sum (\log(q_i) + 1) \leq O(\log n)$$

$$C(n) \leq O(\log n) + \sum_i C(q_i)$$

$C(n) \leq O(\log^2 n)$. (using $\sum \log(q_i) \leq \log n$)

Runtime = $\text{poly}(C(n)) = \text{polylog}(n)$.

Randomized algorithms for primality

Thm There is an algorithm $A(n, r)$ s.t. when n is a t-bit integer, $A(n, r)$ runs in

poly(t) time s.t.

1. If $r \in \{0,1\}^{poly(t)}$ is prime, then for all r $A(n, r)$ ACCEPTS.

2. If n is not prime, then

$$P_{r \in \{0,1\}^{poly(t)}}\left[A(n, r) \text{ REJECTS}\right] \geq 0.99$$

If $A(n, r)$ REJECTS then

n is not prime.

Proposal

Fermat's little theorem.

- Pick random $a \in \{0, 1, \ldots, n-1\}$

= Check that $a^{n-1} \equiv 1 \pmod{n}$.

{ Carmichael Numbers
105?

n s.t. $a^{n-1} \equiv 1 \mod n$ for all $a \in \mathbb{Z}_n^*$ }

There are ∞'ly many Carmichael #s, so the proposal doesn't work.

If p is prime, then

$$a^p \equiv a \pmod{p}$$

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Thm n is prime iff

$$(X+1)^n \equiv X^n + 1 \pmod{n}$$

as an identity in $\mathbb{Z}[X]/(n \cdot \mathbb{Z}[X])$

Proof

Compare coeffs on either side.

Coeff of X^{n-i} is $\binom{n}{i}$ on LHS, 0 on RHS.

Claim: If n is not prime, $\exists\, i \in [1, n-1]$ s.t. $n \nmid \binom{n}{i}$

If p is a prime s.t. $p \mid n$

$$\binom{n}{p} = \left(\frac{n}{p}\right)\left[\frac{(n-1)\cdots(n-p+1)}{(p-1)\cdots(1)}\right]$$

$\frac{n}{p}$: n/p ; denominator: Rel. prime to p.

So highest power of p dividing $\binom{n}{p}$ is one less than that of

(ϕ) ... n.

Idea Agrawal-Biswas Primality Test.

Check that

$$(X+1)^n \equiv X^n + 1 \pmod{n}$$

by substituting random values for X.

What about Carmichael #s?

Don't just substitute integer values for X!

Substitute algebraic #s too,

eg. $\sqrt{2}$. How? By reducing mod $X^2 - 2$.

Algorithm

1. Set $d = O(\log n)$
2. ~~Repeat $k = \text{poly} \log n$ times.~~

Pick $U(x) \in \mathbb{Z}_n[x]$ uniformly random monic of degree d.

Compute $(x+1)^n - x^n - 1 \pmod{n, U(x)}$

If nonzero, (REJECT & halt)

3. ACCEPT.

Analysis

Suppose n is not prime, and rejection Prob $< \frac{1}{2^d}$. We will get a contradiction

Let p be some prime factor of n.

Claim $(x+1)^n - x^n - 1 \not\equiv 0 \pmod{p}$.

Proof $p \nmid \binom{n}{p^e}$ where $p^e \mid n$ and $p^{e+1} \nmid n$.

If $(x+1)^n - x^n - 1 \equiv 0 \pmod{n, U(x)}$

then $(x+1)^n - x^n - 1 \equiv 0 \pmod{p, U(x)}$

then $(X+1)^n - X^n - 1 \equiv 0 \pmod{p, U(X)}$

$$\Rightarrow \quad U(X) \mid (X+1)^n - X^n - 1$$

as polynomials in $\mathbb{F}_p[X]$.

Fact 1

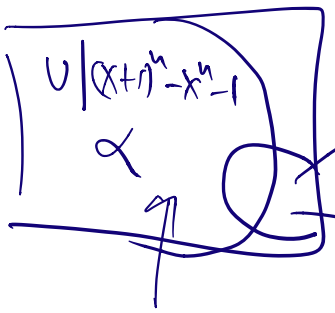
$$\Pr_{U(X)}\left[U(X) \text{ is irreducible in } \mathbb{F}_p[X] \right] = \frac{1}{d}.$$

~~If α-fraction of all~~ By assumption

If $\Pr_{U(X)}\left[U(X) \mid (X+1)^n - X^n - 1 \text{ in } \mathbb{F}_p[X] \right] > 1 - \frac{1}{2d}$!

Then $\Pr_{U}\left[U \text{ is irreducible} \wedge U(X) \mid (X+1)^n - X^n - 1 \right] \geq \frac{1}{2d}$.

$< d$



V is irreducible.

$\Rightarrow \quad \frac{1}{2d} \cdot \left(\#\text{ irreducible degree } d \text{ monic polys in } \mathbb{F}_p[X] \right)$

many irreducible polys divide $(X+1)^n - X^n - 1$.

$\Rightarrow \geq \left(\frac{1}{2d}\right) \cdot \frac{p^d}{d} (1 - o(1))$ many distinct, irred polys of degree d divide $(X+1)^n - X^n - 1$.

$\Rightarrow \quad d \cdot \left(\frac{1}{2d}\right) \cdot \frac{p^d}{d} \cdot (1 - o(1)) \leq n.$

Contradiction if $d = \Omega(\log n)$.

So rejection prob $\geq \frac{1}{2d} = \Omega\left(\frac{1}{\log n}\right)$

Repeating $\Theta\left(\frac{1}{\log n}\right)$ times makes rejection prob 0.99.