Deterministic Primality Testing

Last time

Randomized test.

Based on the characterization

$(X+1)^n \equiv X^n + 1 \pmod n$ iff ($\hookrightarrow$ in $\mathbb{Z}[X]$)

n is prime.

Randomized test:

Test this identity mod random polynomials $E(X)$ of moderate degree. $d \approx \text{polylog } n$

Analysis: If the test passed for many E, then

working mod p for some $p \mid n$,

we get many many irreducibles

$\approx p^d \gg n$.

of degree d s.t. $E(x) \mid (x+1)^n - x^n - 1$ in $\mathbb{F}_p[x]$.

$\Rightarrow (x+1)^n - x^n - 1 = 0$ in $\mathbb{F}_p[x]$.

Claim If n is not a prime power, then $(x+1)^n - x^n - 1 \neq 0$ in $\mathbb{F}_p[x]$

Proof If $p^l \mid n$, divide it out.

$$(x+1)^{p^l \cdot a} = x^{p^l \cdot a} + 1^{p^l} \text{ in } \mathbb{F}_p[x]$$

$$\Rightarrow (x+1)^a \equiv x^a + 1 \text{ in } \mathbb{F}_p[x].$$

Then apply binomial thm.

If $p \nmid a$,

$$\binom{a}{1} \neq 0 \bmod p.$$

Agrawal – Kayal – Saxena Primality Test

Input n.

1. If n is a perfect power
   REJECT

2. $R =$ polylog (n) $(= O(\log^5 n))$
   $A =$ polylog (n) $(\in O(\log^6 n))$

2.5 If any $r \le R$ divides n, REJECT.

3. Test if

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

for all $a \in \{1, 2, \ldots, A\}$
$r \in \{1, 2, \ldots R\}$.

4 If not REJECT, else ACCEPT

Easy: If n is prime, alg ACCEPTs.

Suppose n is not a prime power.

and the algorithm ACCEPTS.

Want to get a contradiction.

We know that for all $a \in [A]$, $r \in [R]$

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

Fix a particular $r \leq R$, TBD.

Let p be a prime dividing n, (Which p is TBD) $p \nmid r$

Then we know that:

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

$$(X+a)^n \equiv X^n + a \text{ in } \mathbb{F}_p[X]/(X^r - 1)$$

For all ω, an n^{th} root of 1 in $\overline{\mathbb{F}}_p$,

$$(\omega+a)^n = \omega^n + a$$

In $\overline{\mathbb{F}}_p$, how do the n^{th} roots of 1 look?

In which extension of $\mathbb{F}_p$ do they lie?

$$(X^q-1) = \prod_{i=1}^{\ell} h_i(X)$$

What are degrees of the $h_i(X)$?

If $\alpha \in \overline{\mathbb{F}}_p$, then the smallest i s.t. $\alpha^{p^i} = \alpha$ is the

degree of the minimal poly of α over $\mathbb{F}_p$.

$= [\mathbb{F}_p(\alpha) : \mathbb{F}_p]$.

The n'th roots of 1 in $\overline{\mathbb{F}_p}$ are exactly n in number, and are a cyclic group.

Take a generator ω_0 of this cyclic group. $\{1, \omega_0, \omega_0^2, \dots, \omega_0^{n-1}\}$ is all the n^{th} roots of 1.

$\omega_0, \omega_0^p, \omega_0^{p^2}, \dots, \underbrace{\omega_0^{p^l}}_{\ell}, \dots$

Which is the smallest $l \geq 1$.

$\omega_0^{p^\ell} = \omega_0$?

Ans: smallest ℓ s.t. $p^\ell \equiv 1 \bmod r$.

= Order of p mod r.

If $u = \text{ord}(p) \bmod r$, then all r^{th} roots of 1 lie in $\mathbb{F}_{p^u}$.

Intuition: want u to be large so that the identity

$$(x+a)^n = x^n + a$$

is tested at substitutions of x that are in very high degree extensions over $\mathbb{F}_p$.

Pick $r \leq R$ s.t. $\text{ord}(n) \bmod r$ is $\geq \log^2 n$.

Claim There exists such an r.

Proof Want r s.t.

$$n \not\equiv 1 \bmod r$$
$$n^2 \not\equiv 1 \bmod r$$
$$n^3 \equiv 1 \bmod r$$
$$\vdots$$
$$n^{\log^2 n} \not\equiv 1 \bmod r.$$

Want r that is relatively prime to $(n-1)(n^2-1) \cdots (n^{\log^2 n}-1)$

$$\approx n^{\log^3 n} \times 2^{\log^4 n}.$$

Fun fact $\prod_{q} q \geq e^{\log^5 n}$

primes
$q \leq \log^5 n$

So there is an r.

Fix this r.

Let $H_r = \{ r^{th} \text{ roots of } 1 \text{ in } \overline{\mathbb{F}}_p \}$

Definition

Let $f(x) \in \mathbb{F}_p[x]$

$m \in \mathbb{N}$.

Then we say that f and m commute if for all $\omega \in H_r$

$$f(\omega)^m = f(\omega^m)$$

Fact 1

From hypothesis, $\forall a \leq A$,

$x+a$ and x^n commute.

Fun fact 2: Any $f(X) \in \mathbb{F}_p[X]$ and ρ commute.

Fact 3

If $f_1(X)$ and m commute

and $f_2(X)$ and m commute

then: $f_1 \cdot f_2(X)$ and m commute

Proof Fix any $\omega \in H_n$.

$$(f_1 \cdot f_2(\omega))^m = (f_1(\omega))^m \cdot (f_2(\omega))^m$$

$$= f_1(\omega^m) \cdot f_2(\omega^m)$$

$$(f_1 \cdot f_2)(\omega^m)$$

$= (\tau_1 \cdot \tau_2)(\omega)$

Fact 4

If $f(x)$ and m_1 commute and $f(x)$ and m_2 commute then $f(x)$ and $m_1 \cdot m_2$ commute.

Proof Fix any $\omega \in H_\pi$.

$$f(\omega^{m_1 m_2}) = f((\omega^{m_1})^{m_2})$$

$$= f(\omega^{m_1})^{m_2} \quad (\text{since } \omega^{m_1} \in H_\pi)$$

$$= (f(\omega))^{m_1 m_2}$$

We know: every $f(x)$ from:

$$\{ X + a : a \in [A] \}$$

and every m from

$\{n, p\}$

Commute.

$$S = \left\{ \prod_{i=1}^{R} (X + a_i) \ : \ \text{each } a_i \in [A] \right\}$$

$$T = \left\{ n^i p^j \ : \ i, j \geq 0 \right\}$$

Then by Facts 3, 4,

any $f(X)$ in S commutes with any m in T.

$\overline{T} = T \mod x.$

Let $t = |\overline{T}|.$

Claim: There are 2 numbers

$m_1, m_2 \leq \underbrace{n^{2\sqrt{t}}}_{\text{small}}$

s.t. $\forall\ f(x) \in S$ and all $\omega \in H_n$,

$$f(\omega)^{m_1} = f(\omega)^{m_2}.$$

Proof

$$\{ n^i p^j \ : 0 \leq i \leq \sqrt{t},\ 0 \leq j \leq \sqrt{t} \}$$

there are $\underbrace{> t \text{ elements}}$ in this.

THIS IS WHERE $n \neq p^l$ is used.

So some two m_1, m_2 are identical

mod n.

For m_1, m_2, $\omega^{m_1} = \omega^{m_2}$ for all $\omega \in H_n$.

So $\forall\ f(x) \in S$,

$$f(\omega)^{m_1} = f(\omega^{m_1}) = f(\omega^{m_2}) = (f(\omega))^{m_2}$$

So $\Omega = \{ f(\omega) : f(x) \in S, \omega \in H_n \}$

has all elements being $(m_1 - m_2)^{th}$ roots of 1.

Next time: $|\Omega| \gg n^{2\sqrt{t}}$.