AKS primality test

- First, generalize the Fermat little theorem to polynomials:

▷ n is prime iff $(x+a)^n \equiv (x^n+a) \mod n$

$a \in (\mathbb{Z}/n)^*$

formal var. in $(\mathbb{Z}/n)[x]$.

Pf: ($\Rightarrow$): $(x+a)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot a^i \cdot x^{n-i} \equiv x^n + a^n$

$\equiv x^n + a \pmod n$.

($\Leftarrow$): Suppose n is composite & prime $p|n$.

$\Rightarrow \binom{n}{p} \not\equiv 0 \mod n \Rightarrow (x+a)^n \not\equiv x^n + a \pmod n$.

$\square$

- Computation of $(x+a)^n \bmod n$ is infeasible, as it involves $n+1 > 2^{(\lg n)}$ - terms.

- Idea: Instead compute $(x+a)^n \bmod \langle n, Q(x)\rangle$ for low-degree $Q(x)$.
[By repeated-squaring mod $\langle n, Q\rangle$, it takes time $(\lg n) \times \tilde{O}(\deg Q \cdot \lg n) = \tilde{O}(\deg Q \cdot \lg^2 n)$.]

- This idea gives (Agrawal-Biswas '99)'s randomized test: $(x+1)^n \equiv (x^n+1) \bmod \langle n, Q(x)\rangle$, for a random $Q \in (\mathbb{Z}/n)[x]$ of $\deg \approx \lg n$.

- AKS ('02) derandomized it by studying
$(x+a)^n - (x^n + a) \bmod \langle n, x^r - 1 \rangle$.

AKS test: (*Input* – $n \in \mathbb{Z}_{\geq 2}$ in binary.)

1) If $\exists\, a, b > 1$, $n = a^b$ then OUTPUT Composite.
2) Compute the smallest $r \in \mathbb{N}$: $\mathrm{ord}_r(n) > 4\lg^2 n$.
3) If $\exists\, a \in [r]$, $1 < \gcd(a,n) < n$ then
   OUTPUT Composite.
4) For $1 \leq a \leq \lceil 2\sqrt{r} \cdot \lg n \rceil =: \ell$,
   if $(x+a)^n \not\equiv (x^n + a) \bmod \langle n, x^r - 1 \rangle$ then
   OUTPUT Composite.

5) else OUTPUT Prime.

- How big is r?
- Say, $\forall r \le R$, $\mathrm{ord}_r(n) \le 4\lg^2 n$.
  $\Rightarrow \forall r \le R$, $r \mid (n-1)(n^2-1)\cdots(n^{\lfloor 4\lg^2 n \rfloor}-1) =: \Pi$.
  $\Rightarrow \mathrm{lcm}\{r \mid r \in [R]\} \mid \Pi$.

▷ $\mathrm{lcm}\{r \mid r \le R\} \geq 2^R$ [$\because$ prime estimates]

▷ $\Pi < n^{16\lg^4 n}$

$\Rightarrow 2^R < n^{16\lg^4 n} \Rightarrow R < 16\lg^5 n$.

$\Rightarrow \exists r < 16\lg^5 n$, in Step 2.

▷ AKS-test takes time $\ell \cdot \tilde{O}(r\lg^2 n) \le \tilde{O}(r^{1.5} \cdot \lg^3 n)$
$\le \tilde{O}(\lg^{10.5} n)$.

Lemma 1: n prime $\Rightarrow$ AKS outputs "Prime".

Pf: $\because$ $(x+a)^n \equiv x^n + a \mod \langle n, x^r - 1 \rangle$. $\square$

Lemma 2: n composite $\Rightarrow$ AKS outputs "Composite".

Proof: • Ideas: CRT on $(\mathbb{Z}/n)$ & $(\mathbb{Z}/p)[x]/\langle x^r - 1 \rangle$.

Interplay of two groups $\mathcal{I}$ & $\mathcal{J}$.

(integers) (field elements)

• Suppose for a composite n, all congruences in Step 4 passed. Let prime $p \mid n$.

(i) $\mathcal{I} := \langle n, p \mod r \rangle = \langle (n^i p^j) \mod r \ (i, j \geq 0) \rangle$

$\triangleright$ $t := |\mathcal{I}| \geq \mathrm{ord}_r(n) > 4 \lg^2 n$.

- Note that Step-4 $\Big\} \Longrightarrow (x+a)^{n^i p^j} \equiv (x^{n^i p^j}+a)$ mod $\langle p, x^r-1\rangle$.
& $(x+a)^p \equiv x^p + a \pmod p$)

↳ This motivates I !

(ii) Let $h \,|\, (x^r-1)/(x-1)$ be an irreducible factor over $\mathbb{F}_p$. Define $\underline{J} := \langle (x+1), (x+2), \ldots, (x+\ell) \bmod (p,h) \rangle$.

$\mathbb{F}_p[x]/\langle h\rangle$ is a field.

- Note: Step-4 $\Rightarrow \forall f \in J,\ f(x)^n \equiv f(x^n) \bmod \langle p, h\rangle$.

↳ This motivates J !

$\triangleright$ $|J| \geq 2^{\min(\ell, t)} > \underline{n^{2\sqrt{t}}}$.

Pf: • Consider two elements $f, g \in J$ that are products of only $\leq t$-many $(x+a)$'s.

• Suppose $f \equiv g \mod \langle p, h\rangle$. Then, by Step 4,

$\Longrightarrow$ $\forall m \in I$, $f(x^m) \equiv g(x^m) \mod \langle p, h\rangle$

$\Longrightarrow$ $f(Y) - g(Y)$ has $|H| = t$-many $\underline{\text{distinct}}$ roots in the field $\mathbb{F}_p[x]/\langle h(x)\rangle$; though it has $\deg < t$. $\Longrightarrow$ $f(Y) - g(Y) = 0$.

$\Longrightarrow$ $|J| \geq \#(\deg \leq t \text{ products of } (x+a)\text{'s}) \geq 2^{\min(\ell, t)}$.

• Note: $\min(\ell, t) \geq \min(2\sqrt{r}\lg n, t) \geq \min(2\sqrt{t}\lg n, t) = 2\sqrt{t}\lg n$. $\Longrightarrow$ $\underline{|J| > n^{2\sqrt{t}}}$. $\square$

▷ J is a cyclic subgroup of $(\mathbb{F}_p[x]/\langle h\rangle)^*$.

— $\because |\mathcal{G}| = t$, $\exists (i,j) \neq (i',j')$, $0 \leq i, j, i', j' \leq \sqrt{t}$

s.t. $n^i p^j \equiv n^{i'} p^{j'} \mod \langle r \rangle$.

— Let f be a generator of J.

$$\Rightarrow \quad f(x^{n^i p^j}) \equiv f(x^{n^{i'} p^{j'}}) \mod \langle p, h \rangle$$

(by step 4) $\Rightarrow \quad f^{n^i p^j} \equiv f^{n^{i'} p^{j'}}$ "

$$\Rightarrow \quad n^i p^j - n^{i'} p^{j'} \equiv 0 \mod |J|.$$

$\Rightarrow$ ($\because$ $n^i p^j$ & $n^{i'} p^{j'} \leq n^{2\sqrt{t}} < |J|$) $n^i p^j = n^{i'} p^{j'}$

$\Rightarrow$ $n =$ p-power $\Rightarrow$ ↯. $\Rightarrow$ n is prime. □