Det. poly-time primality

- The previous primality tests solve the problem practically.
  They can also be derandomized assuming GRH.

- An unconditional derandomization was given by Agrawal-Kayal-S (2002).

- First, generalize the Fermat identity to polynomials: $(\forall a \in (\mathbb{Z}/n\mathbb{Z})^*)$

▷ n is prime iff $(x+a)^n \equiv x^n + a \pmod{n}$.
formal variable

Pf:

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

- $\Leftarrow$: Suppose n is composite & prime $p \mid n$.
- Then $\binom{n}{p} \not\equiv 0 \pmod{n}$. $\Rightarrow (x+a)^n \not\equiv_n x^n + a$. □
(Exercise)

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

- But, we could compute $(x+a)^n \bmod \langle n, Q(x)\rangle$ for low-degree polynomials $Q(x)$.

[By $f(x) \bmod \langle n, Q(x)\rangle$ we mean to denote the residue of f in the ring $(\mathbb{Z}/n\mathbb{Z})[x]/\langle Q(x)\rangle$.
Note that the elements here require only $(\deg Q)\cdot(\lg n)$ bits to represent. Hence, the arithmetic operations have $\underline{\tilde{O}(\deg Q \cdot \lg n)}$ time complexity.]

- This idea was employed by (Agrawal & Biswas, 1999) to devise a randomized test:

$$\text{Test } (x+1)^n \equiv x^n + 1 \bmod \langle n, Q(x)\rangle$$

for a random $Q(x) \in (\mathbb{Z}/n\mathbb{Z})[x]$ of degree $\sim \lg n$.

If n passes the test, OUTPUT prime.

- AKS (2002) derandomized it by studying
$$(x+a)^n - (x^n + a) \mod \langle n, x^r - 1\rangle.$$

<u>AKS test</u>: (Input: $n \in \mathbb{Z}_{>2}$ in binary.)

1) If $\exists a, b > 1$, $n = a^b$ then OUTPUT composite.

2) Compute the smallest $r \in \mathbb{N}$, $\mathrm{ord}_r(n) > 4 \cdot \lg^2 n$.

3) If $\exists a \in [r]$, $1 < (a,n) < n$ then OUTPUT composite.

4) For $1 \leq a \leq \lceil 2 \cdot \sqrt{r} \cdot \lg n \rceil =: \ell$,
   if $(x+a)^n \not\equiv x^n + a \mod \langle n, x^r - 1\rangle$
   then OUTPUT composite.

5) Else OUTPUT prime.

- Firstly, how big is r?
- Say, $\forall r \leq R$, $\mathrm{ord}_r(n) \leq 4 \cdot \lg^2 n$. Then,
  $\forall r \leq R$, $r \mid \Pi := (n-1)(n^2-1) \cdots (n^{\lfloor 4 \lg^2 n \rfloor} - 1)$.

$\Rightarrow \mathrm{lcm}\{r \mid r \in [R]\} \mid \Pi$.

- We know that $\begin{cases} \Pi \leq n^{16 \lg^4 n}, \& \\ \mathrm{lcm}\{r \mid r \leq R\} \geq 2^R. \end{cases}$

(Eg., see prime number estimates.)

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

$\Rightarrow r \leq R \leq 16 \cdot \lg^5 n$.

▷ AKS test has time complexity $\ell \cdot \lg n \cdot \tilde{O}(r \lg n)$
$= \tilde{O}(\lg^3 n \cdot r^{3/2}) = \tilde{O}(\lg^{10.5} n)$.

<u>Lemma 1</u>: n is prime $\Rightarrow$ AKS outputs "prime".

<u>Pf</u>: $\because (x+a)^n \equiv x^n + a \mod \langle n, x^r - 1 \rangle$. □

<u>Lemma 2</u>: n is composite $\Rightarrow$ AKS outputs "composite".

<u>Proof</u>:

- <u>Ideas</u>: Chinese remaindering on $\mathbb{Z}/n\mathbb{Z}$ & $(\mathbb{Z}/p\mathbb{Z})[x]/\langle x^r - 1 \rangle$. Interplay of two groups I & J.

- Suppose for a composite n all the congruences in Step 4 hold.

Let prime $p \mid n$.

- We will consider the size of the two associated groups (multiplicative):

(i) $\mathcal{I} := \langle n, p \pmod r \rangle$.

Note that $(x+a)^n \equiv x^n + a \bmod \langle p, x^r - 1 \rangle$

$\Rightarrow (x+a)^{n^i \cdot p^j} \equiv x^{n^i \cdot p^j} + a \bmod \langle p, x^r - 1 \rangle$

for all $i, j \in \mathbb{N}$.

$\Rightarrow \mathcal{I}$ is motivated by the <u>exponents</u> in Step 4.

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

<u>Pf</u>: Simply, because $\mathcal{I}$ has $\{n, n^2, \ldots\} \pmod r$. $\square$

(ii) Let $h \mid \frac{x^r - 1}{x - 1}$ be an irreducible factor over $\mathbb{F}_p$.

Define another group

$$J := \langle x+1, x+2, \ldots, x+\ell \bmod (p, h) \rangle.$$

Note that $(x+a)^n \equiv x^n + a \bmod \langle p, h(x) \rangle$, $a \in [\ell]$, implies that also for $f(x) := \prod_{a\in[\ell]} (x+a)^{i_a}$

$$f(x)^n \equiv f(x^n) \bmod \langle p, h\rangle.$$

$\Rightarrow J$ is motivated by the <u>base</u> in Step 4.

$\triangleright$ $\#J \geqslant 2^{\min(\ell,t)} > n^{2\sqrt{t}}$.

Pf: • Let f, g be product of $\le t$ many $(x+a)$'s.

• If $f \equiv g \bmod \langle p,h\rangle$ then by Step 4:

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

$\Rightarrow$ $f(Y) - g(Y)$ has $\#I = t$ <u>distinct</u> roots in the field $\mathbb{F}_p[x]/\langle h(x)\rangle$, though its deg $< t$.

$\Rightarrow$ $f - g = 0$.

$\Rightarrow$ $\#J \geqslant \#$(deg $\le t$ polynomials formed by multiplying $x+a$'s) $\geqslant 2^{\min(\ell,t)}$.

• Note that $\min(\ell,t) \geqslant \min(2\sqrt{r}\cdot \lg n, t)$

$\geqslant \min(2\sqrt{t}\cdot \lg n, t) > 2\sqrt{t}\cdot \lg n$.

$\Rightarrow$ $\#J > n^{2\sqrt{t}}$. $\square$

▷ J is a cyclic group.

- $\because \# \mathcal{I} = t$, $\exists (i,j) \neq (i',j')$, $0 \leq i, j, i', j' \leq \sqrt{t}$
  s.t. $n^i p^j \equiv n^{i'} p^{j'} \pmod{r}$.

$\Rightarrow \forall f \in J$, $f(x^{n^i p^j}) \equiv f(x^{n^{i'} p^{j'}}) \bmod \langle p, h \rangle$
$\Rightarrow$ (Step 4) $f^{n^i p^j} \equiv f^{n^{i'} p^{j'}} \bmod \langle p, h \rangle$

$\Rightarrow \quad n^i p^j \equiv n^{i'} p^{j'} \pmod{\# J}$

- As $|n^i p^j|, |n^{i'} p^{j'}| \leq n^{2\sqrt{t}} < \# J$,
  we deduce $n^i p^j = n^{i'} p^{j'}$
  $\Rightarrow$ n is a power of p, a $\lightning$.

- The contradiction means that n is prime at Step 5.

$\square$