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 (Aug 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:

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

• ⇐: Suppose n is composite & prime $p | n$.

• Then $\binom{n}{p} \not\equiv 0 \pmod{n}$. $\Rightarrow (x+a)^n \not\equiv_n x^n + a$. □

(Exercise)

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

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

[By $f(x)$ mod $\langle n, Q(x)\rangle$ 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 $\tilde{O}(\deg Q \cdot \lg n)$ time complexity.]

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

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

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
  $(x+a)^n - (x^n+a) \bmod \langle n, x^r-1\rangle$.

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

5) Else OUTPUT prime.

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

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

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

(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 $\ell \cdot \lg n \cdot \tilde{O}(r \lg n)$
$= \tilde{O}(\lg^3 n \cdot r^{3/2}) = \tilde{O}(\lg^{10.5} n)$.

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

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

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

Proof:

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

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

  Let prime $p | n$.

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

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

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

$\Rightarrow I$ is motivated by the exponents in Step 4.

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

Pf: Simply because I has $\{n, n^2, \ldots\} \pmod r$. □

(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 $f(x) := \prod_{a \in [\ell]} (x+a)^{i_a}$

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

$\Rightarrow$ J is motivated by the base in Step 4.

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

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

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

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

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

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

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

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

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

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

▷ 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. $n^i p^j \equiv n^{i'} p^{j'} \pmod{r}$.

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

$\Rightarrow$ ($\underline{\text{Step 4}}$) $\quad f^{n^i p^j} \equiv f^{n^{i'} p^{j'}} \bmod \langle p, h\rangle$

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

- 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 ↯.

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

$\square$

RSA (Public-key cryptosystem)

- Cryptology is a major consumer of number theory.

- Primality & integer factoring appear in a cryptosystem by Rivest, Shamir & Adleman (1977).

Preprocessing:

1) Carefully choose prime $p \neq q$.
2) $n := p \cdot q$ & $\phi(n) := (p-1)\cdot(q-1)$.
3) Choose $1 < e < \phi(n)$ coprime to $\phi(n)$ & n.

   (n,e) is the public key.
4) $d := e^{-1} \bmod \phi(n)$ is the private key.

Encryption: $m \mapsto m^e \bmod n$.

Decryption: $c \mapsto c^d \bmod n$.

▷ $m \mapsto m^e \mapsto (m^e)^d \equiv m^{1+k\cdot\varphi(n)} \equiv m \pmod{n}$.

OPEN: Given (n,e), is There an efficient way to compute $e^{-1} \bmod \varphi(n)$ (or $c^{1/e} \bmod n$)?

Exercise: $\Phi(n)$ & factoring n are equivalent up to randomized poly-time.

▷ Integer factoring cracks RSA.

(RSA problem) ▷ e-th root finding (i.e. $c^{1/e} \bmod n$) also cracks RSA.

OPEN: Is RSA problem equivalent to integer factoring up to randomized poly-time?