Primality Testing

- We move to factoring, or irreducibility testing, of integers.
- Motivation:
  - natural question (first raised by Gauss formally)
  - commercially, appears in RSA public-key cryptosystem; used in browsers, file transfer (SSH), smartcards, digital signature, etc.
- First question: Is input n (lg n-bits) a prime?

Historical attempts

1) Antiquity (Eratosthenes Sieve, 300 BC)

Divide n by $2, 3, 5, 7, 11, \dots \to \lfloor \sqrt{n} \rfloor$.

- Doable for small n, eg. $n = 127$.
- Infeasible for large n, eg $n = 2^{127} - 1$.

— Ideally, we want a $(\log n)^{O(1)}$-time algorithm.
$\to$ (poly-time)

2) Fermat test (1660s): Test, for several a, $a^n \equiv a \pmod{n}$

- It's fast for a single 'a' $\in (\mathbb{Z}/n)$.
- But, how many a's should we try to be sure?
- Is this a criterion for primality?

- Carmichael (1910) showed the existence of composite n's s.t. $\forall a \in (\mathbb{Z}/n)^*$, $a^n \equiv a \bmod n$.

  e.g. $n = 561 = 3 \times 11 \times 17$.

- Alford, Granville & Pomerance (1994) showed:

Carmichael numbers are infinite.

In fact, $\{1 \to n\}$ has $\geq n^{2/7}$ such numbers.

3) Solovay-Strassen (1974). The first "practical" primality test.

- Based on quadratic residuosity property in prime fields.

Lemma 1 (Legendre symbol): For prime p & $a \in \mathbb{Z}$,

$$\left(\frac{a}{p}\right) := \left(a^{\frac{p-1}{2}} \bmod p\right) \in \{-1, 0, +1\}.$$

'a' is square (or quadratic residue) in $\mathbb{F}_p^*$ iff $\left(\frac{a}{p}\right) = 1$.

Pf: (seen before). $\square$

Lemma 2 (Jacobi symbol): For numbers $a, n \in \mathbb{Z}$, define $\left(\frac{a}{n}\right) := \prod_{\text{prime } p \mid n} \left(\frac{a}{p}\right)$ (with repetition). Then,

(i) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$; $\forall a, b \in \mathbb{Z}$ [Multiplicative]

(ii) $\left(\frac{a}{n}\right) \cdot \left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}}$; $\forall$ odd, coprime $a, n \in \mathbb{Z}$.

[It's called Gauss quadratic reciprocity law (1796).]

(iii) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$ & $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$; $\forall$ odd $n \in \mathbb{N}$.

Pf. skipped: • (i) – (iii) have elementary proofs.

• (ii) has more than 200 proofs known! $\square$

– Lemma 2 gives a fast algorithm to compute $\left(\frac{a}{n}\right)$, in a way similar to Euclid's gcd algo.

Algo: Input – a & n in binary.

1) If $\gcd(a,n) \neq 1$ then OUTPUT 0.

2.1) Reduce a to $(a \bmod n) \in \left(-\frac{n}{2}, \frac{n}{2}\right]$.

2.2) If $a<0$ then use $\left(\frac{-a}{n}\right)=\left(\frac{-1}{n}\right)\cdot\left(\frac{a}{n}\right)=(-1)^{\frac{n-1}{2}}\cdot\left(\frac{a}{n}\right)$ to reduce 'a' to the <u>positive</u> case.

[Also, use $\left(\frac{-1}{2}\right)=1$ to handle even n case.]

2.3) If $2|a$ then make it <u>odd</u> by $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$.

2.4) If $a=1$ then OUTPUT 1.

3) OUTPUT $\left(\frac{n}{a}\right)\cdot(-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}}$.

▷ In each recursive call, n gets <u>halved</u>. Like euclid-gcd analysis, the time complexity is $\tilde{O}(\lg n)$.

▷ Odd n prime $\Rightarrow \left(\frac{a}{n}\right)\equiv a^{\frac{n-1}{2}} \bmod n$. <u>Qn</u>: It fails for composite n?

– Solovay-Strassen used this idea to design a test:

<u>Algo:</u> (Input- $n \in \mathbb{N}$ in binary)

1) If $2 \mid n$ or $n = a^b$ for $b \in \mathbb{N}_{>1}$, then OUTPUT <u>Composite</u>.
2) Pick random $a \in (\mathbb{Z}/n)^*$. Compute $\left(\frac{a}{n}\right)$.
3) If $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod n$ then OUTPUT <u>Prime</u>. else OUTPUT <u>Composite</u>.

▷ Time taken is $\tilde{O}(\lg^2 n)$.

<u>Claim 1:</u> n prime $\Rightarrow$ it outputs Prime.

<u>Pf:</u> $\left(\frac{a}{n}\right)$ is Legendre symbol; equals $a^{\frac{n-1}{2}} \pmod n$; $\square$

Claim 2: n composite $\Rightarrow \Pr_{a \in (\mathbb{Z}/n)^*}[\text{output } \underline{\text{Prime}}] \leq 1/2$.

Pf: • Consider the set $\underline{B} := \{a \in (\mathbb{Z}/n)^* \,/\, \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n\}$.

• B is a subgroup of $(\mathbb{Z}/n)^*$.

$\Rightarrow \quad |B| \mid \varphi(n)$.

• We'll show that $B \neq (\mathbb{Z}/n)^*$; thus, $|B| \leq \varphi(n)/2$.

• The idea is Chinese Remaindering: Assume $B = (\mathbb{Z}/n)^*$

• Suppose $\exists$ prime p_1 s.t. $p_1^2 \mid n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ s.t. $p_1, \ldots, p_k$ are distinct primes.

• $B = (\mathbb{Z}/n)^* \Rightarrow$ generator g of $(\mathbb{Z}/p_1^{e_1})^*$ is in B.

$\Rightarrow g^{n-1} \equiv 1 \bmod p_1^{e_1} \Rightarrow \varphi(p_1^{e_1}) = p_1^{e_1-1}(p_1-1) \mid (n-1) \Rightarrow p_1 \mid (n-1)$

$\Rightarrow$ contradiction as $p_1 | n$.

$\Rightarrow$ n is squarefree; say, $n = \prod_{i=1}^{k} p_i$.

- Suppose $\exists\, i \in [k]$ & $g \in (\mathbb{Z}/n)^*$ s.t.

$$g^{\frac{n-1}{2}} \not\equiv \left(\frac{g}{p_i}\right) \bmod p_i .$$

$\Rightarrow$ By CRT, find $a \equiv g \bmod p_i$ & $a \equiv 1 \bmod p_j$ for $j \neq i$.

$$\Rightarrow \quad a^{\frac{n-1}{2}} \equiv g^{\frac{n-1}{2}} \not\equiv \left(\frac{g}{p_i}\right) \equiv \left(\frac{a}{p_i}\right) \bmod p_i$$

$$= \left(\frac{a}{n}\right)$$

$\Rightarrow$ $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \bmod n$ $\Rightarrow$ $\lightning$ to $B = (\mathbb{Z}/n)^*$.

- Thus, assume $\forall g, \forall i, \ g^{\frac{n-1}{2}} \equiv \left(\frac{g}{p_i}\right) \mod p_i$.

- Again, pick an $a \in (\mathbb{Z}/n)^*$ s.t. $\left(\frac{a}{p_1}\right) = -1$, while $a \equiv 1 \mod p_i$, for $2 \leq i \leq k$.

$$\Rightarrow \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{p_1}\right) \equiv -1 \mod p_1 \quad ; \quad \text{while}$$

$$\equiv \left(\frac{a}{p_i}\right) = 1 \mod p_i, \text{ for } i > 1.$$

$$\Rightarrow \quad a^{\frac{n-1}{2}} \not\equiv \pm 1 \mod n \quad [\because k \geq 2]$$

$$\Rightarrow \quad a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \mod n \Rightarrow \lightning \text{ to } B = (\mathbb{Z}/n)^*$$

$$\Rightarrow \quad B \neq (\mathbb{Z}/n)^*$$

$$\Rightarrow \quad \Pr_a[\text{error}] \leq 1/2. \qquad \square$$

Derandomization of this by Riemann Hypothesis (RH)

- (Ankeny'50 & Bach'90) showed that:

  If $B \subsetneq (\mathbb{Z}/n)^*$ & GRH,

  then $\exists\, a \in \{1, 2, \ldots, \lceil 2\lg^2 n \rceil\}$, $a \notin B$.

  small-certificate exists!

  $\Rightarrow$ Solovay-Strassen derandomized under GRH.

- Next we study a slightly more practical primality test, by Miller ('75) & Rabin ('77).

- <u>Idea</u>: Continue beyond $1 \equiv a^{n-1}$, $a^{\frac{n-1}{2}} \pmod n$ to $a^{\frac{n-1}{4}}$, $a^{\frac{n-1}{8}}$, ...

Whp we will see a square-root of 1 other than $\pm 1 \bmod n$ $\Rightarrow$ proving n composite.

<u>Miller-Rabin test</u>: (<u>Input</u> - n in binary)

1) < Same as SS-test >.

2.1) Randomly pick $a \in (\mathbb{Z}/n)^*$. If $a^{n-1} \not\equiv 1 \bmod n$ then COMPOSITE.

2.2) Compute k, m s.t. $(n-1) = 2^k \cdot m$ & m odd.

3) $\forall i = 0$ to $k-1$: Compute $u_i := a^{m \cdot 2^i} \bmod n$.

4) If $\exists i$, $u_i = 1$ but $u_{i-1} \neq \pm 1$ then COMPOSITE
else PRIME.

▷ Time taken is $\tilde{O}(\lg^2 n)$.

Fact: n prime $\Rightarrow$ it outputs PRIME.

Pf: • For prime n, $\sqrt{1} \equiv \pm 1 \bmod n$
since $(\mathbb{Z}/n)$ is a field. $\square$

Theorem: If n is odd & has ≥ 2 distinct prime factors, the bad a's, i.e. $B := \{a \in (\mathbb{Z}/n)^* \mid a^m \equiv 1$ or $\exists i \in [0..k],\ a^{m2^i} \equiv -1\}$ are at most $\Phi(n)/4$ many.

Proof: • Again, we'll use CRT on n.

• Let 2^ℓ be the highest 2-power that divides $\gcd(p-1 \mid \text{prime } p \text{ factor of } n)$.

• Define $B' := \{a \in (\mathbb{Z}/n)^* \mid a^{m2^{\ell-1}} \equiv \pm 1 \bmod n\}$.

D $B \subseteq B'$ & B' is a subgroup of $(\mathbb{Z}/n)^*$.

Pf: • B' is clearly a subgroup.

• Let $a \in B$. $\Rightarrow a^m \equiv 1$ OR $\exists i$, $a^{m2^i} \equiv -1$.

• If $a^m \equiv 1$ then $a \in B'$; done.

• Assume $a^{m2^i} \equiv -1 \bmod n$.

$\Rightarrow \forall p^e | n$, $a^{m2^i} \equiv -1 \bmod p^e$ & $a^{\phi(p^e)} \equiv 1 \bmod p^e$ & $a^{m2^{i+1}} \equiv 1$.

$\Rightarrow 2^{i+1} \mid (p-1) \Rightarrow i+1 \leq \ell \Rightarrow i \leq \ell - 1 \Rightarrow a^{m2^{\ell-1}} \equiv \pm 1 \bmod n$

$\Rightarrow a \in B'$ as well. $\square$

– How large is $|B'|$?

$\triangleright$ $|B'| = 2 \cdot \prod_{p|n} \left[\underline{\gcd(m, p-1)} \cdot 2^{\ell-1} \right]$.

Pf: • First, estimate $\#\{a \mid a^{m2^{\ell-1}} = 1\}$.

$= \prod_{p|n} \#\{a \in (\mathbb{Z}/p^e)^* \mid a^{m2^{\ell-1}} \equiv 1 \bmod p^e\}$

$= \prod_{p|n} \gcd(m2^{\ell-1}, \varphi(p^e))$ [$\because (\mathbb{Z}/p^e)^*$ is cyclic]

$= \prod_{p|n} \gcd(m2^{\ell-1}, p^{e-1}(p-1)) = \prod_{p|n} \gcd(m2^{\ell-1}, p-1)$

$= \prod_{p|n} 2^{\ell-1} \cdot \gcd(m, p-1)$.

- Overall, we deduce $|B'| = 2 \cdot \prod_{p \mid n} 2^{\ell-1} \cdot \gcd(m, p-1)$. $\square$

$$\Rightarrow \frac{|B'|}{\varphi(n)} = 2 \cdot \prod_{p^e \| n} \frac{2^{\ell-1} \cdot \overbrace{(m, p-1)}^{\text{odd}}}{(p-1) \cdot p^{e-1}}$$

[$\because$ m is odd, $(m, p-1) \cdot 2^{\ell-1}$ divides $(p-1)/2$

$\Rightarrow$ numerator $\leq (p-1)/2$]

$$< 2 \cdot \prod_{p^e \| n} \frac{1/2}{p^{e-1}}$$

$\Rightarrow \begin{cases} \text{If } n \text{ has } \geq 3 \text{ prime factors then the above } \leq 2 \cdot \frac{1}{8} = \frac{1}{4} \\ \text{If } \exists p \mid n,\ p^2 \mid n \text{ then above } \leq 2 \cdot \frac{1/2}{2} \cdot 1/2 = 1/4. \end{cases}$

- Suppose $n = p \cdot q$ for <u>distinct</u> primes p, q.

$$\Rightarrow \frac{|B'|}{\varphi(n)} = \frac{1}{2} \cdot \frac{(p-1, m)}{(p-1)/2^{\ell}} \cdot \frac{(q-1, m)}{(q-1)/2^{\ell}}$$ numerator divides denominator

- RHS $> 1/4 \Rightarrow (p-1, m) = (p-1)/2^{\ell}$ & $(q-1, m) = (q-1)/2^{\ell}$.
- Let $(p-1, m) =: p'$ & $(q-1, m) =: q'$ [p', q' are odd]

$$\Rightarrow n = 2^k m + 1 = pq = (1 + 2^{\ell} p') \cdot (1 + 2^{\ell} q')$$

$$\Rightarrow 2^k m + 1 \equiv 1 + 2^{\ell} q' \pmod{p'}$$

$$\Rightarrow 0 \equiv m \equiv q' \pmod{p'} \Rightarrow p' \mid q'$$

- Similarly, $q' \mid p'$. $\Rightarrow p' = q' \Rightarrow p = q \Rightarrow \lightning$.

$$\Rightarrow |B'| \leq \varphi(n)/4 \Rightarrow |B| \leq \varphi(n)/4 < n/4. \qquad \square$$

Corollary 1: MR-test errs only when n is composite, & error probability $< 1/4$.

Corollary 2: MR-test derandomizes under GRH.

Pf:
- We know $B' \subsetneq (\mathbb{Z}/n)^*$.
- Thus, from "GRH connection" $\exists\, 1 \le a \le \lceil 2\lg^2 n \rceil$, $a \notin B'$. Thus, $a \notin B$.
- On composite n, this 'a' is a good certificate. $\square$

- Cryptography is a major consumer of number theory. (Eg. HTTPS, SSH, SFTP, digital signature, etc.)

RSA (Public-key cryptosystem)

- Primality & integer factoring appear in the cryptosystem by Rivest, Shamir & Adleman ('77).

- Preprocess: 1) Carefully choose primes $p \neq q$.

  2) $n := p \cdot q$ & $\varphi(n) := (p-1)\cdot(q-1)$.

  3) Choose $e \in [\varphi(n)]$ coprime to $\varphi(n)$ & n.

  4) $d := e^{-1} \bmod \varphi(n)$.

  Public-key: (e, n)

  Private-key: (d, p)

- Encryption: $m \mapsto (m^e \bmod n) =: c$
plaintext ← ciphertext

- Decryption: $c \mapsto (c^d \bmod n) \equiv m$ (Why?)

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

[Exercise: $m^{\varphi(n)} \equiv 1 \bmod n$]

- Adversary only knows (e, n, c).

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

finding $\varphi(n)$
▷ is equivalent to factoring n.

RSA-problem.

integer-factoring.

▷ Prime p is found by sampling & MR-test.

- Now we will focus on deterministic polynomial-time primality test.

  First such test was invented by Agrawal-Kayal-S (Aug 2002).

→ It's a major example of derandomization in complexity. (It's unpractical.)