- We will later show that $B \neq (\mathbb{Z}/n\mathbb{Z})^*$.
- Thus, $|B| \leq \frac{1}{2} \cdot |(\mathbb{Z}/n\mathbb{Z})^*| = \frac{\varphi(n)}{2}$.

$\Rightarrow \Pr_{a \in (\mathbb{Z}/n\mathbb{Z})^*}[a \in B] \leq 1/2.$ □

Connection with Riemann hypothesis (RH)

- RH is a longstanding open question about the zeros of (the analytic extension of)

$$\zeta(s) := \sum_{n \geq 1} n^{-s}$$ (Riemann zeta fn.)

- RH has deep connections to the distribution of prime numbers.

- (Ankeny 1950 & Bach 1990) showed that:

If $B \lneq (\mathbb{Z}/n\mathbb{Z})^*$ & GRH holds, then $\exists\, a \in \{1, \ldots, \lceil 2\lg^2 n \rceil\}$ s.t. $a \notin B$.

⇒ Solovay-Strassen's primality test can be derandomized, under GRH, to a deterministic poly-time test.

- Miller (1975) gave another such test, which was later made practical by Rabin (1977).

  Miller-Rabin test is the simplest & practically the most popular primality test.

  - Idea: Continue beyond $a^{\frac{n-1}{2}} \pmod n$ to $a^{\frac{n-1}{4}}$, $a^{\frac{n-1}{8}}, \dots \pmod n$. Whp we'll get a $\sqrt{1}$ other than $\pm 1 \bmod n$.

Miller-Rabin test: (Input: $n \in \mathbb{N}$ in binary.)

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

2.1) Randomly choosed $a \in [n-1]$.

2.2) If $(a,n) \neq 1$ or $a^{n-1} \not\equiv 1 \pmod n$
then OUTPUT composite.

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

4) For $i = 0$ to $(k-1)$
Compute $u_i = a^{m \cdot 2^i} \bmod n$.

5) If $\exists i$, $u_i = 1$ & $u_{i-1} \neq \pm 1$
then OUTPUT composite else OUTPUT prime.

- Its time complexity is clearly $\tilde{O}(\lg^2 n)$.

Fact: If n is prime then it outputs "prime".

Pf:

- For prime n, $\sqrt{1}$ can only be $\pm 1 \bmod n$, since $\mathbb{Z}/n\mathbb{Z}$ is a field. □

Theorem: If n is odd & has ≥ 2 distinct prime factors then the bad a's of Miller-Rabin, i.e.

$$B := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^m = 1 \text{ or } \exists 0 \leq i \leq k, a^{m2^i} = -1\}$$

are at most $\varphi(n)/4$ many.

Proof:

- We will prove this by studying the congruences mod n via Chinese remaindering.

- Let 2^ℓ be the highest 2-power that divides $\gcd(p-1 \mid \text{prime } p \text{ dividing } n)$.
- Define $B' := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{m \cdot 2^{\ell-1}} = \pm 1\}$.

▷ $B \subseteq B'$.

Pf: • Let $a \in B$.

• If $a^m = 1$ then clearly $a \in B'$.

• If $a^{m \cdot 2^i} = -1$ then $\forall p \mid n$, $a^{m 2^i} = -1 \pmod p$.

$\Rightarrow 2^{i+1} \mid (p-1)$

$\Rightarrow i \leq (\ell - 1) \Rightarrow a^{m \cdot 2^{\ell-1}} = \pm 1 \pmod n$.

$\Rightarrow a \in B'$. □

▷ $\#B' = 2 \cdot \prod_{p \mid n} (\gcd(m, p-1) \cdot 2^{\ell-1})$ ← distinct primes $p \mid n$

Pf:

- Let us compute $\#\{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{m 2^{\ell-1}} = 1\}$.

$$\bullet = \prod_{p|n} \#\{a \in (\mathbb{Z}/p^{e_p}\cdot\mathbb{Z})^* \mid a^{m\cdot 2^{l-1}} = 1\}$$

[where, $n = \prod_{p|n} p^{e_p}$ for distinct primes.]

$$= \prod_{p|n} \gcd(m2^{l-1}, \phi(p^{e_p}))$$

[$\because (\mathbb{Z}/p^{e_p}\mathbb{Z})^*$ is a cyclic group of order $\phi(p^{e_p})$.]

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

[$\because \phi(p^{e_p}) = p^{e_p-1}(p-1)$; p is coprime to $2m$ & m is odd.]

• By the above count we deduce that

$$\#B' = 2\cdot \prod_{p|n} (m, p-1)\cdot 2^{l-1} \quad . \qquad \square$$

$$\Rightarrow \frac{\#B'}{\varphi(n)} = 2\cdot \prod_{p|n} \frac{(m, p-1)\cdot 2^{l-1}}{(p-1)\cdot p^{e_p-1}}$$

$$< 2\cdot \prod_{p|n} \frac{1/2}{p^{e_p-1}}$$ [$\because$ the numerator divides $(p-1)/2$]

$\Rightarrow$ We are done { if n has ≥ 3 prime factors, or
if $\exists p|n$, $e_p \geq 2$.

• Thus, we assume $n = p \cdot q$ for distinct primes.

$$\Rightarrow \frac{\#B'}{\varphi(n)} = 2 \cdot \frac{(p-1, m) \cdot 2^{l-1}}{p-1} \cdot \frac{(q-1, m) \cdot 2^{l-1}}{q-1}$$

$$= \frac{1}{2} \cdot \frac{(p-1, m)}{(p-1)/2^l} \cdot \frac{(q-1, m)}{(q-1)/2^l}$$

← numerators divide their denominator

• RHS is $\geq 1/4$ only if

$$(p-1, m) = (p-1)2^{-l} \quad \& \quad (q-1, m) = (q-1)2^{-l}.$$

$\Rightarrow \exists\, p', q'$ dividing m s.t.

$$p-1 = 2^l \cdot p' \quad \& \quad q-1 = 2^l \cdot q'.$$

$$\Rightarrow n = 2^k \cdot m + 1 = (1 + 2^l \cdot p') \cdot (1 + 2^l \cdot q')$$

$$\Rightarrow p' | q' \;\&\; q' | p'$$

$$\Rightarrow p' = q' \Rightarrow p = q, \text{ a } \lightning$$

• Thus, $\frac{\#B}{\varphi(n)} \leq \frac{\#B'}{\varphi(n)} < \frac{1}{4}$. □

Corollary 1: Miller-Rabin test could err when n is composite, with probability $< 1/4$.

Corollary 2: Miller-Rabin could be derandomized,

under GRH, to a det. poly-time test.

Pf:

- We have shown that if n is composite then B' is a proper subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$.

- Thus, from the "GRH connection" $\exists\, 1 \le a \le 2\lg^2 n$, $a \notin B'$.

$\Rightarrow a \notin B$, and hence Miller-Rabin works correctly with this a. $\square$

Proving Solovay-Strassen

- We now give the missing proof of the Solovay-Strassen test.

The idea is to study congruences mod n via CRT.

Theorem: If n is composite, odd & having ≥ 2 prime factors then $B := \{a \in (\mathbb{Z}/n\mathbb{Z})^* \mid a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right)\}$ is

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

Proof:

- Suppose $\exists$ prime p_1, $p_1^2 \mid n$. Let $n = p_1^{e_1} \cdots p_k^{e_k}$ for distinct primes p_i.
- Since $(\mathbb{Z}/p_1^{e_1}\mathbb{Z})^*$ is a cyclic group of order $\phi(p_1^{e_1}) = p_1^{e_1-1} \cdot (p_1 - 1)$, we could pick its <u>generator</u> g.
- If $g \in B$ then $\phi(p_1^{e_1}) \mid (n-1)$
  $\Rightarrow p_1 \mid (n-1)$, a $\lightning$.

$\Rightarrow g \notin B$ and we are done.

- Thus, we assume $n = p_1 \cdots p_k$.
- If $\exists i \in [k]$ & g s.t. $g^{\frac{n-1}{2}} \not\equiv \left(\frac{g}{p_i}\right) \pmod{p_i}$,

then we can find, by CRT, $a \equiv g \pmod{p_i}$ & $\forall j \in [k] \setminus \{i\}$, $a \equiv 1 \pmod{p_j}$.

$\Rightarrow a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) = \left(\frac{a}{p_i}\right) \pmod{p_i}$

$\Rightarrow a \notin B$ and we'll be done.

• Thus, the bad case is : $\forall g, \forall i, g^{\frac{n-1}{2}} \equiv_{p_i} \left(\frac{g}{p_i}\right)$.

• Now, since $k \geq 2$, we could pick an a s.t.
$\left(\frac{a}{p_1}\right) = 1$, $\left(\frac{a}{p_2}\right) = -1$ & $a \equiv_{p_i} 1$, $\forall i \in [3 \ldots k]$.

$\Rightarrow a^{\frac{n-1}{2}} \equiv_{p_1} 1$, $\equiv_{p_2} -1$ & $\equiv_{p_i} 1$, $\forall i \in [3 \ldots k]$.

$\Rightarrow a^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$

$\Rightarrow a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$.

$\Rightarrow$ $\alpha \notin B$. □