RECAP

- Primality of random numbers (useful for RSA): check for base-2 pseudoprimality
  - deterministic test: ($2^{n-1} \equiv 1 \bmod n$)
  - probabilistic analysis based on Pomerance's Theorem (the density of base-2 pseudo-primes is vanishing)

- Miller-Rabin primality test: randomized search for a certificate of compositeness:

On input n (fixed):

Determine the existence of:

1. $a \in \mathbb{Z}_n^+$: $a^{n-1} \not\equiv 1 \bmod n$
   (n is not a base-a pseudoprime)
   ↳ not effective for Carmichael numbers ($\forall a \in \mathbb{Z}_n^*$: $a^{n-1} \equiv 1 \bmod n$)
2. $x \in \mathbb{Z}_n^+ - \{1, \underbrace{-1}_{\equiv n-1}\}$: $x^2 \equiv 1 \bmod n$
   (nontrivial square root of unity)

How does MR(n) check for nontrivial square roots of 1?

To check for certificate of type 1, MR(n) must compute

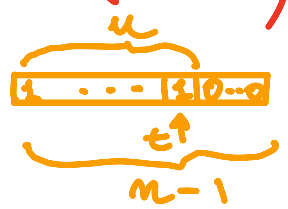
$$MOD\_EXP(a, n-1, n)$$

for random values of a. Recall that MOD_EXP is based on SQUARING.

During some iterations of modular exponentiation the algorithm checks if nontrivial roots of unity are spotted.

Specifically, let n odd (or otherwise $(n=2, \text{prime}) \vee (n=2k, k>1, \text{composite})$)

Write $(n-1) = u \cdot 2^t$, u odd



We compute

$$(a^{n-1}) = (a^u)^{2^t} \bmod n \text{ as } \left((a^u \bmod n)^{2^t}\right) \bmod n$$

by performing t squaring ops on $d_0 = a^u \bmod n$: $d_i \leftarrow d_{i-1} * d_{i-1} \bmod n$ $1 \leq i \leq t$

We check for type-2 certificates during those t squaring ops.

The search for both types of certificates is summarized by the following PSEUDOCODE

CERTIFICATE(a, n) $\{n \text{ odd}\}$

* Let $n-1 = 2^t \cdot u$, $t \geq 1$, u odd *

$\{ (n-1)_2 = (\underbrace{a_k, a_{k-1}, \ldots, a_t}_{(u)_2}, \underbrace{0, \ldots, 0}_{t}) \}$

1

$\{ a^{n-1} = a^{u \cdot 2^t} = (a^u)^{2^t} \}$ ← t squaring ops on a^u

$d \leftarrow$ MOD_EXP(a, u, n)

$\{ d_0 = a^u \bmod n \}$

for $i \leftarrow 1$ to t do

$\quad d' \leftarrow (d \cdot d) \bmod n$ $\quad \{ \underbrace{(a^u)^{2^{i-1}}}_{d_{i-1}} \rightarrow \underbrace{(a^u)^{2^i}}_{d_i (=d')} \}$

$\quad$ if $(d' = 1)$ $\quad$ 1

$\quad\quad$ then if $((d \neq 1) \wedge (d \neq n-1))$ $\quad$ type 2

$\quad\quad\quad$ then return COMPOSITE

$\quad\quad\quad$ else return NONWITNESS

$\quad d \leftarrow d'$

return COMPOSITE $\{ a^{n-1} \neq 1 \bmod n \}$ type 1

MR(n, s)

if $(n = 2)$ then return PRIME

if even(n) then return COMPOSITE

for $i \leftarrow 1$ to s do

$\quad a \leftarrow$ RANDOM$(\{1, 2, \ldots, n-1\})$

$\quad$ if CERTIFICATE(a, n) = COMPOSITE

$\quad\quad$ then return COMPOSITE

return PRIME

RUNNING TIME: Basically, $\leq s$ executions of MOD_EXP(a, n):

$$T_{MR}(|\langle n\rangle|, s) = O(s \cdot |\langle n\rangle|^3)$$

CORRECTNESS MR(n) may be incorrect only when it says that n is PRIME while n is in fact COMPOSITE (one-sided)

The analysis shows that this is unlikely because every $a \in \mathbb{Z}_n^+ = \{1, \dots, n-1\}$ is a nonprimality certificate with probability $\geq \frac{1}{2}$ (when n is composite).

We will only prove CORRECTNESS for non-Carmichael's numbers (see CLRS for full proof)

We need some FACTS in group theory

DEF Given a (multiplicative) finite group $(G, \cdot)$, a subgroup G' of G is a nonempty subset

$$G' \subseteq G \ : \ (G', \cdot) \text{ is a group}$$

FACT 1 $G' \subseteq G$ is a subgroup of G

$$\Leftrightarrow (G' \neq \emptyset) \wedge (\cdot \text{ is closed over } G')$$

PROOF ($\Leftarrow$): $x \in G' : x, x^2, \ldots, x^t \in G' :- \exists\, 1 \leq k < h : x^k = x^h \Rightarrow x^{h-k} = e \in G'$

$- \text{ if } x \neq e : x^{h-k-1} = x^{-1}$

FACT 2 (Lagrange's Theorem) (no proof)

Let $(G, \cdot)$ be a finite (multiplicative) group. Then for each subgroup G' of G it must be $|G'| \mid |G|$

The cardinality (order) of a subgroup of a finite group always divides the cardinality of the group!

COROLLARY Any proper subgroup $G' \subset G$ of a finite group G is such that

$$|G'| \leq \frac{|G|}{2}$$

PROOF The largest divisor of $|G|$ smaller than $|G|$ is $\frac{|G|}{2}$:

$$|G| = K|G'| \quad , K > 1 \quad (G' \subset G')$$

$$\Rightarrow |G'| = \frac{|G|}{K} \leq \frac{|G|}{2}$$

CORRECTNESS PROOF (non-Carmichael numbers only)

Assume that n is composite (for n prime, $MR(n)$ is always correct)

$\boxed{\text{Since } n \text{ is not Carmichael: } \exists\, b \in \mathbb{Z}_n^* : b^{n-1} \neq 1 \bmod n}$

Consider the set of NON-WITNESSES in $\mathbb{Z}_n^*$: (CERT.(a,n)=?)

$NW = \{a \in \mathbb{Z}_n^* : (a^{n-1} \equiv 1) \bmod n \wedge$ (no nontrivial root of 1 discovered in the exponentiation of a)$\}$

We have

$NW \subseteq \{a \in \mathbb{Z}_n^* : a^{n-1} \equiv 1 \bmod n\} \subset \mathbb{Z}_n^*$

We prove that $H = \{a \in \mathbb{Z}_n^* : a^{n-1} \equiv 1 \bmod n\}$ is a proper subgroup of $\mathbb{Z}_n^*$:

0. $1 \in H \Rightarrow H \neq \emptyset$

1. Closure: if $a, b \in H$: $\begin{cases} a^{n-1} \equiv 1 \bmod n \\ b^{n-1} \equiv 1 \bmod n \end{cases}$

therefore $(a^{n-1} b^{n-1}) = (ab)^{n-1} \equiv 1 \bmod n$

$\Rightarrow ab \in H$

.

Also: $H \subset \mathbb{Z}_n^*$ since $\exists\, b \in \mathbb{Z}_n^* : b^{n-1} \not\equiv 1 \mod n$

$$\Rightarrow \quad |NW| \leq |H| \leq |\mathbb{Z}_n^*|/2 \leq (n-1)/2$$

Therefore:

$$\Pr(a \in NW) = \frac{|NW|}{\underset{\substack{\uparrow \\ |\mathbb{Z}_n^+|}}{n-1}} \leq \frac{n-1}{2(n-1)} = \frac{1}{2}$$

We can prove the same result for Carmichael's numbers

$$\Pr(a \in NW) \leq \frac{1}{2}$$

(here we use nontrivial square roots)

In conclusion:

$$\Pr(MR(n) \text{ incorrect}) \leq \Pr(MR(n) \text{ returns PRIME when } n \text{ is composite})$$

$$= \Pr(s \text{ extractions from } NW) < \left(\frac{1}{2}\right)^s$$