Plan for today

- Recal: Weak fermat test and Carmichael numbers
- The Miller-Rabin test

Motivation for primality test

$N = p \cdot q$ (log-size primes)

Factorization

- How dense are primes?
- How to recognize primes.

The weak Fermat test

- Input: $N \in \mathbb{N}$ odd
- Assert: *Composite* or *probably prime*
- Choose $a \in \{1, \ldots, N-1\}$ uniformly at random
- If $a^{N-1} \pmod N = 1$ assert *probably prime*
- else assert *composite*

Fast exponentiation.

Fermat's little thm:

if $N \in \mathbb{P}$, then $\forall a \in \{1, \ldots, N-1\}$

$a^{N-1} \equiv 1 \mod (N)$

subgroup.

$H = \{a \in \mathbb{Z}_n^* : a^{N-1} \equiv 1 \mod N\} \leq \mathbb{Z}_N^*$

N is not Carmichael and composite $\Rightarrow |H| \mid |\mathbb{Z}_N^*| \Rightarrow 2 \cdot |H| \leq |\mathbb{Z}_N^*| \leq |\{1, \ldots, N-1\}|$

proper

$\Rightarrow$ probability of Alg asserting probably prime $\leq 1/2$

$\leq \left(\frac{1}{2}\right)^{10000}$

Q: N not Carmichael and composite. Run Alg 10000 times. Prob[each round assert probprime]

Carmichael numbers

An odd composite number $N \in \mathbb{N}$ is called *Carmichael number* if

$$\forall a \in \mathbb{Z}_N^* : a^{N-1} = 1.$$

If N is not Carmichael

Theorem

Let N be an odd composite number that is not Carmichael, then the weak Fermat test asserts probably prime with probability at most $1/2$.

If the weak Fermat test is repeated i times, then the probability that it asserts probably prime in all i rounds is at most $1/2^i$.

How do Carmichael numbers look like

Theorem

Every Carmichael number N is of the form

$$N = p_1 \cdots p_k,$$

where the p_i are distinct primes and $(p_i - 1) \mid (N - 1)$ for $i = 1, \ldots, k$. , $k \geq 3$.

proof: Let $N = p_1^{e_1} \cdots p_k^{e_k}$ be a Carmichael number.

First show $e_i = 1$, $i = 1, \ldots, k$: CRT: $\mathbb{Z}_N^* \simeq \left(\mathbb{Z}_{p_1^{e_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{e_k}}^*\right)$

cyclic group.

$\Rightarrow$ $\exists$ element in $\mathbb{Z}_N^*$ of order $(p_1 - 1) \cdot p_1^{e_1 - 1}$

But $x^{N-1} = 1 \Rightarrow (p_1 - 1) \cdot p_1^{e_1 - 1} \mid N - 1$ $\Rightarrow e_1 - 1 = 0$ $\Rightarrow e_1 = 1$

$\Rightarrow \exists g \in \mathbb{Z}_{p_1^{e_1}}^*$ s.k. $\langle g \rangle = \mathbb{Z}_{p_1^{e_1}}^*$, $\operatorname{ord}(g) = (p_1 - 1) \cdot p_1^{e_1 - 1}$

order $(g, 1, \ldots, 1) = (p_1 - 1) \cdot p_1^{e_1 - 1}$

We have also shown $(p_i - 1) \mid N - 1$, $i = 1, \ldots, k$.

How do Carmichael numbers look like

Theorem

Every Carmichael number N is of the form

$$N = p_1 \cdots p_k,$$

where the p_i are distinct primes and $(p_i - 1) \mid (N - 1)$ for $i = 1, \ldots, k$.

Remains to be shown.

$k \geq 3$

assume $k = 2$. $N = p_1 \cdot p_2$

$N - 1 = p_1 \cdot p_2 - 1$

$= (p_1 - 1)(p_2 + 1) - p_1 + p_2$

$\exists$ element of order $(p_1 - 1)$ in $\mathbb{Z}_N^*$

$\exists$ " " $(p_2 - 1)$

$\Rightarrow (p_1 - 1) \mid N - 1$

$\Rightarrow (p_1 - 1) \mid (-p_1 + p_2)$

$= (-p_1 + 1) + (p_2 - 1)$

$\Rightarrow (p_1 - 1) \mid (p_2 - 1)$

(symmetric argument) $\Rightarrow (p_2 - 1) \mid (p_1 - 1)$

$\Rightarrow p_1 = p_2$ ↯

Proof

The group of strong liars

- N odd Carmichael number
- $N-1 = q \cdot 2^\ell$ with q odd integer
- Let $k \in \mathbb{N}_0$ be minimal such that $\forall a \in \mathbb{Z}_N^* : a^{q \cdot 2^k} = 1$.
- $k \geq 1$
- Define $L = \{a \in \mathbb{Z}_N^* : a^{q \cdot 2^{k-1}} = \pm 1\}$
- $a \in \mathbb{Z}_N^*$ strong liar if no jump from $\neq \pm 1$ to 1.

Lemma

$L \trianglelefteq \mathbb{Z}_N^*$

proof:

Subgroup test.

$\forall a, b \in L : a \cdot b^{-1} \in L$

$(a \cdot b^{-1})^{q \cdot 2^{k-1}} = a^{q \cdot 2^{k-1}} \cdot (b^{-1})^{q \cdot 2^{k-1}}$

$= \pm 1 \cdot (\pm 1)^{-1} = \pm 1$ ∎

$N-1 = 1101011000$ $\quad \ell = 3$

N Carm. (random) $a \in \mathbb{Z}_N^*$: $a^q, a^{q \cdot 2}, a^{q \cdot 2^2}, \ldots, a^{q \cdot 2^\ell}$

squaring squaring 11

$\neq \pm 1$ 1 1 1 → remain 1.

strong liars $\subseteq L$

N prime: How many roots?

$0 = X^2 - 1 \pmod N$

Strong liars are proper subgroup

$$L = \{ a \in \mathbb{Z}_N^* : a^{q \cdot 2^{k-1}} = \pm 1 \}$$

Theorem

Let N be a Carmichael number. Then L is a proper subgroup of $\mathbb{Z}_N^*$.

Proof: Remember: $k \geq 1$ is minimal with $\forall a \in \mathbb{Z}_N^* : a^{q \cdot 2^k} = 1$

thus $\exists b \in \mathbb{Z}_N^*$ s.t. $b^{q \cdot 2^{k-1}} \neq 1 \mod N$

Write N as $N = P \cdot Q$ with $\gcd(P, Q) = 1$

CRT $\mathbb{Z}_N^* \cong \mathbb{Z}_P^* \times \mathbb{Z}_q^*$. W.l.o.g. we can assume that $b^{q \cdot 2^{k-1}} \neq 1 \mod P$

$\exists a \in \mathbb{Z}_N^*$ with. $a \overset{CRT}{\longmapsto} (b, 1)$

$$a^{q \cdot 2^{k-1}} = (\underbrace{b^{q \cdot 2^{k-1}}}_{\neq 1}, 1)$$

not $(-1,-1)$ nor $(1,1)$ $\Rightarrow a^{q \cdot 2^{k-1}} \neq \pm 1 \mod N$

The Miller-Rabin test

N is composite ⇒ Prob(assert probably prime) ≤ 1/2

Input: $N \in \mathbb{N}$, $N \geq 3$ odd
Assert: *Composite* or *probably prime*

Compute $q \in \mathbb{N}$ and $\ell \in \mathbb{N}$ with $N = q \cdot 2^\ell + 1$ and q odd
Choose $a \in \{1, \ldots, N-1\}$ uniformly at random

$A_1 = a^q$

$a^q, a^{q \cdot 2}, a^{q \cdot 2^2}, a^{q \cdot 2^3}, \ldots, a^{q \cdot 2^\ell}$
A_1 A_2

for $i = 0 \ldots \ell - 1$
  $A_2 = A_1^2$
  if $A_2 = 1$ and $A_1 \neq \pm 1$ return *composite*
  $A_1 = A_2$

if $A_1 = 1$ return *probably prime*
else return *composite*

Analysis

Theorem

Let $N \in \mathbb{N}_{\geq 3}$ be an odd number. If N is prime, then the M-R algorithm returns probably prime. If N is composite, then the M-R algorithm returns probably prime with probability $\leq 1/2$. The M-R algorithm runs in polynomial time in $\log N$.

proof: N is composite and Not Carmichael, then by previous discussion $Pr(\text{probably prime}) \leq 1/2$.

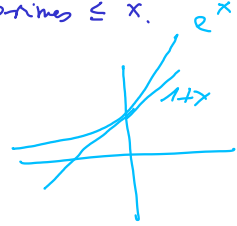
If N is Carmichael, then $Pr(a \text{ being a strong liar}) \leq 1/2$.

$\Rightarrow Pr(\text{probably prime}) \leq 1/2$.

Remark: There is meanwhile a polynomial and deterministic primality test. (Agrawal et al. 2002). But M-R test is still used in practice.

The density of primes.

Defi: $\pi(x) = \left| \{ p : p \in \mathbb{P}, p \le x \} \right|$ counts number of primes $\le x$.



Not going to prove this.

Prime number theorem: $\pi(x) \overset{\text{asymptotically}}{\approx} \frac{x}{\ln(x)}$

x random n-bit number, $\in \{0, \dots, 2^n - 1\}$

$$\Pr(x \in \mathbb{P}) = \frac{\pi(2^n - 1)}{2^n} \approx \frac{2^n}{\ln(2^n) \cdot 2^n} \approx \frac{1}{n}$$

Fish i-times, probability that only non-primes are caught:

$$\le \left(1 - \frac{1}{n}\right)^i \le e^{-i/n} = \frac{1}{e^{i/n}}.$$

$n = i$: $\frac{1}{e}$

We will prove instead:

$\exists$ constants c_1, c_2 s.th. $c_2 \cdot \frac{x}{\log(x)} \leq \pi(x) \leq c_1 \cdot \frac{x}{\log(x)}$

---

generate all primes until N Sieve of Eratosthenes.

~~1~~, 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ... N