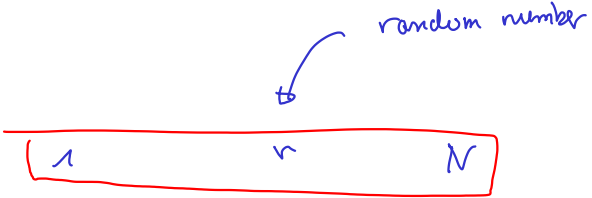
Plan for today

- Recal: Weak fermat test and Carmichael numbers
- The Miller-Rabin test
- Intro to density of primes



$$P(r \in \mathbb{P}) = \frac{\pi(N)}{N} \qquad \pi(N) = |\mathbb{P} \cap \{1, \dots, N\}|.$$

$$\approx \frac{1}{\log(N)}$$

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*

IF N is composite and not Carmichael then Pr of asserting probably prime $\leq 1/2$.

in this case, the algorithm does not err.

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 $1/2^i$.

proof: $H = \{a \in \mathbb{Z}_N^* : a^{N-1} \equiv 1 \pmod N\}$ is a subgroup of $\mathbb{Z}_N^*$.

Since N not Carmichael and composite $H \subsetneq \mathbb{Z}_N^*$. $\Rightarrow |H| \le \frac{1}{2} \cdot |\mathbb{Z}_N^*|$

$\le \frac{1}{2} |\{1, \dots, N-1\}|$

∎

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 $i = 1, \ldots, k$.

proof: $N = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ ✓ Checking. Factorization of N into distinct primes

Assume $\alpha_1 \geq 2$. Consider $a = (p_1 + 1, 1, 1, \ldots, 1) \in \mathbb{Z}_N^*$, Chinese remainder thm.

In other words $a \equiv p_1 + 1 \bmod p_1^2$, $a \equiv 1 \bmod p_2^{\alpha_2}$, $\ldots$, $a \equiv 1 \bmod p_k^{\alpha_k}$.

Remember that $\operatorname{order}(a) \mid N - 1$ (since $a^{N-1} \equiv 1 \bmod N$).

$$(p_1 + 1)^k = \sum_{j=0}^{k} \binom{k}{j} p_1^{k-j} \cdot 1^j = \sum_{j=0}^{k} \binom{k}{j} p_1^{k-j} \quad (\bmod p_1^2) \qquad (k \geq 2)$$

$$= k \cdot p_1 + 1 \Rightarrow \operatorname{order}(p_1 + 1 \bmod (p_1^2)) = p_1$$

but $(p_1 + 1)^{N-1} \equiv 1 \bmod p_1^2$

$\Rightarrow p_1 \mid N - 1$ ↯

Proof

The group of strong liars

$N-1 = (\underbrace{x\cdots *1}_{q}\overbrace{0000}^{\ell}) = q\cdot 2^{\ell}$

- N odd Carmichael number
- $N-1 = q\cdot 2^{\ell}$ with q odd integer
- Let $k \in \mathbb{N}_0$ be minimal such that $\forall a \in \mathbb{Z}_N^* : a^{q\cdot 2^k} = 1$. $k \geq 0$ since $(-1)^{q\cdot 2^0} \neq 1$
- $k \geq 1$
- Define $L = \{a \in \mathbb{Z}_N^* : a^{q\cdot 2^{k-1}} = \pm 1\}$

Lemma

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

proof: $a, b \in L$ to show $a\cdot b^{-1} \in L$.

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

∎

Strong liars are proper subgroup

Theorem

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

Proof: Suppose N is Carmichael and $k \in \mathbb{N}_0$ s.t. $\forall a \in \mathbb{Z}_N^*$ one has $a^{q \cdot 2^k} = 1$, (k minimal). N is of the form $N = p_1 \cdot p_2 \cdots p_j$.

Let $b \in \mathbb{Z}_N^*$ with $b^{q \cdot 2^{k-1}} \neq 1$. Without loss of generality, we can assume that $b^{q \cdot 2^{k-1}} \not\equiv 1 \pmod{p_1}$. Write $Q = \prod_{i=2}^{j} p_i$. $\not\equiv \bmod p_1$, $\equiv \bmod Q$.

Via the Chinese remainder thm $\exists\, c \in \mathbb{Z}_N^*$ with $c \xrightarrow{\phi} (b, 1)$

$c^{q \cdot 2^{k-1}} = (b^{q \cdot 2^{k-1}}, 1) = (\neq 1, 1) \neq \begin{matrix}(-1,-1) \cong -1 \\ (1,1) \cong 1\end{matrix}$ $\quad c^{q \cdot 2^{k-1}} \neq \pm 1 \bmod N$

$\Rightarrow c \in \mathbb{Z}_N^* \setminus L$. ∎

The Miller-Rabin test

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

$N-1 = q \cdot 2^\ell$

$A_1 = a^q$ → fast exponentiation.

$a^{q \cdot 2^1}, a^{q \cdot 2^2}, \ldots a^{q \cdot 2^\ell} = a^{N-1}$

$\neq \pm 1 \quad \sim +1$

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*

If F is a field, then
$p(x) \in F[x]$, $p(x) = x^2 - 1$
has only two roots ± 1

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 $\log N$, Bitlength of N.

proof: Let N be composite. If N is not Carmichael, then

$$\Pr(a^{N-1} \equiv 1 \pmod N) \leq 1/2 \Rightarrow \Pr(\text{Alg. returns composite}) \geq 1/2.$$

Let N be Carmichael. $Z = \{a \in \mathbb{Z}_N^* : a^{q \cdot 2^{k-1}} = \pm 1\} \subsetneq \mathbb{Z}_N^*$.

$\Pr(a \notin Z) \geq 1/2$. Since $a^{q \cdot 2^k} = 1$, we have a witness for N being composite.

∎

Input: odd N

if N composite ("Probably prime" with $Pr \leq 1/2$)

if N prime (surely Alg returns prime).

Repeat Alg 1000 times. $Pr(\text{Alg never asserts composite} \mid N \text{ is composite}) \leq (1/2)^{1000}$ → very small.

Plan for today

- Chebyshev's theorem on the density of prime numbers.

Notation

- $\mathbb{P} := \{p \in \mathbb{N} : p \text{ is prime}\}$.
- For $x \in \mathbb{R}_+$, $\pi(x) := |\{p \in \mathbb{P} : p \leq x\}|$.

The prime number theorem

Conjectured by Gauß.

Theorem (Prime Number Theorem (Hadamard, de la Vallée Poussin 1896))

$\pi(x) \sim \frac{x}{\ln x}$

Jacques Hadamard

∗ 8. December 1865 in Versailles

† 17. October 1963 in Paris

Charles-Jean de La Vallée Poussin

∗ 14. August 1866 in Löwen

† 2. MÃďrz 1962 in Brussels

A weaker theorem

Theorem (Chebyshev's Theorem)

$\pi(x) = \theta\left(\frac{x}{\ln x}\right)$

Use of that Theorem:

There are constants $c_1, c_2 \in \mathbb{R}_{>0}$ s.t.

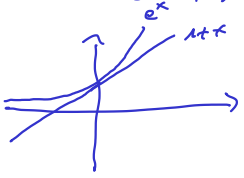
$$c_1 \cdot \frac{x}{\ln(x)} \leq \pi(x) \leq c_2 \cdot \frac{x}{\ln(x)}.$$

$x \in \{1, \dots, N\}$ uniformly at random.

$$\Pr(x \in \mathbb{P}) = \frac{\pi(N)}{N} \geq c_1 \cdot \frac{N}{\ln(N) \cdot N} = \Theta\left(\frac{1}{\text{size}(N)}\right)$$

$\Pr(i \text{ times no prime}) \approx \left(1 - \frac{1}{\text{size}(N)}\right)^i$

$\leq e^{-i/\text{size}(N)} \leq \frac{1}{1000}$



$e^x \geq 1+x$

$-i/\text{size}(N) \leq -\ln(1000)$

$i \geq \text{size}(N) \cdot \ln(1000)$

$\Pr(\text{hit a prime in 1000 trials}) \geq 1 - \frac{1}{1000}$

Long enough.

A basic fact on binomial coefficients

Fact

For each $m \in \mathbb{N}$, one has $\frac{2^{2m}}{2m} \leq \binom{2m}{m} \leq \binom{2m+1}{m} \leq 2^{2m}$.

1. $2^{2n} = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i}$

$= 1+1 + \sum_{i=1}^{2n-1} \binom{2n}{i}$

$\leq 1+1+(2n-1)\binom{2n}{n}$

$= 2+(2n-1)\binom{2n}{n} \leq 2n\binom{2n}{n}$

$\Rightarrow \frac{2^{2n}}{2n} \leq \binom{2n}{n}$

2. $2^{2n+1} \geq \sum_{i=0}^{2n+1} \binom{2n+1}{i}$

$\geq \binom{2n+1}{n} + \binom{2n+1}{n+1}$

$= 2 \cdot \binom{2n+1}{n}$

The p-adic order of an integer

Definition

Given $p \in \mathbb{P}$ and $n \in \mathbb{N}$, we let $\mathrm{ord}_p(n)$ to be the biggest k such that $p^k \mid n$.

Fact

For $p \in \mathbb{P}$ and $n \in \mathbb{N}$, one has $\mathrm{ord}_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.

$\pi(x) = \Omega(\frac{x}{\ln x})$

Fact

For each $n \in \mathbb{N}$, one has $\pi(n) \geq (\frac{1}{2} \ln 2) \cdot \frac{n}{\ln n}$.

More basics

Fact

For all $x \in \mathbb{R}_+$, one has

$$\prod_{p \leq x,\, p \in \mathbb{P}} p < 4^x.$$

$\pi(x) = O(\frac{x}{\ln x})$