Primality testing

An integer $N \in \mathbb{N}_{\geq 2}$ is prime if $N \mid ab \Rightarrow N \mid a$ or $N \mid b$ or, equivalently, if $ab = N \Rightarrow a \in \{1, -1\}$ or $b \in \{1, -1\}$ $\forall a, b \in \mathbb{Z}$.
All the other integers are said to be COMPOSITE.

Fundamental thm arithmetic: Every positive integer can be written as product of positive prime factors. This is unique up to order of the factors.

Here we want to test whether a given integer N is prime or not.
Can we do better than division by all integers up to $\sqrt{N}$? Eratosthenes

Recall some facts:

- $\mathbb{Z}_N^\times = \{a \bmod N \in \mathbb{Z}_N : \gcd(a, N) = 1\}$ is the multiplicative group of units in $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$.
- $|\mathbb{Z}_N|^\times = \varphi(N)$ where φ is the Euler's totient function
- If $N = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ then the Chinese Remainder Theorem says that $\mathbb{Z}_N \tilde{=} \mathbb{Z}_{p_1^{e_1}} \times \ldots \times \mathbb{Z}_{p_r^{e_r}}$ and $\mathbb{Z}_N^\times \tilde{=} \mathbb{Z}_{p_1^{e_1}}^\times \times \ldots \times \mathbb{Z}_{p_r^{e_r}}^\times$
  ↳ ring isomorphism ↳ group isomorphism
- Euler's theorem (generalization of Fermat's little theorem) states that if $\gcd(a, n) = 1$ then $a^{\varphi(n)} \equiv 1 \bmod n$

(Non-primality) Fermat's test

Assume $N \in \mathbb{N}_{\geq 3}$, N odd.

Theorem: If n is prime and $\gcd(a, n) = 1$ then $a^{n-1} \equiv 1 \bmod n$.

Corollary: Let $a \in [1, n-1]$. If $a^{n-1} \not\equiv 1 \bmod n$ then n is composite.

Fermat's test

Input: Odd integer ≥ 5

Output: "composite" or "possibly prime"

1. Choose a random in $\{2, \ldots, n-2\}$
2. Compute $b = a^{n-1}$ rem n with the repeated squaring
3. If $b \neq 1$ then return "composite" else return "possibly prime"

Remark: If a and n are not coprime then b and n are also not coprime and the algorithm correctly returns "composite". However, if it returns "possibly prime" it may be wrong.

Consider the following subgroup of $\mathbb{Z}_N^\times$

$$L_N = \{ u \in \mathbb{Z}_N^\times : u^{N-1} = 1 \}$$

L_N is a group and Fermat's little theorem says that $L_N = \mathbb{Z}_N^\times$ if N is prime. If $L_N \neq \mathbb{Z}_N^\times$ then $\# L_N \leq \frac{1}{2} \# \mathbb{Z}_N^\times$.

If the a chosen in step 1 is in $\mathbb{Z}_N^\times \setminus L_N$, then the test will answer composite. Such an a is called Fermat witness.

If $a \bmod N \in L_N$ then a is a Fermat liar for N

If we know any witness, we know that N is composite.

The test fails when N is composite and $L_N = \mathbb{Z}_N^\times$. An N for which this happens are called Carmichael numbers. These are composite numbers without Fermat witnesses.

The probability failure p_m of the Fermat test (i.e. the probability of selecting a s.t. $a^{n-1} \equiv 1 \bmod n$) is $p_N = \frac{|L_N|}{N-1}$

L_N is the Kernel of the group homomorphism $x \longmapsto x^{N-1}$

Therefore L_N is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ and so $|L_N| \mid \varphi(N)$

If $L_N \neq (\mathbb{Z}/N\mathbb{Z})^*$ then $|L_N| \leq \frac{\varphi(N)}{2}$ and hence

$$p_N = \frac{|L_N|}{N-1} \leq \frac{|L_N|}{\varphi(N)} \leq \frac{1}{2}$$

If the test is repeated 10 times, the probability of failing to detect that n is composit is less than $\frac{1}{2^{10}} \approx 0.00098$.

The test fails for Carmichael numbers.

It is based on the following theorem

Theorem (Miller-Rabin). Let n be an odd prime number. Write $n-1 = 2^v m$ where m is an odd integer. $\forall$ integer a coprime to n either $a^m \equiv 1 \bmod n$ or there exists $i \in [0, v-1]$ s.t. $a^{2^i m} \equiv -1 \bmod n$.

Proof: Assume $a^m \not\equiv 1 \bmod n$. We will show that $\exists\, i \in [0, v-1]$ s.t. $a^{2^i m} \equiv -1 \bmod n$. Since n is odd, the integer $v \geq 1$. If n is prime then $\mathbb{Z}/n\mathbb{Z}$ is a field. $\forall\, a \in (\mathbb{Z}/n\mathbb{Z})^*$ we have

$$a^{2^v \cdot m} = a^{n-1} = 1$$

Let $\mathcal{I} = \{i \in [0, v] : a^{2^i m} \equiv 1 \bmod n\}$. This set is nonempty and $0 \notin \mathcal{I}$. Let $i_0 = \min \mathcal{I}$. Then $i_0 \geq 1$.

Since $a^{2^{i_0} m}$ satisfies

$$\left(a^{2^{i_0-1} m}\right)^2 = a^{2^{i_0} m} = 1 \mod n$$

$$\Rightarrow a^{2^{i_0-1} m} \in \{\pm 1\}$$

Since i_0 is minimal $\Rightarrow a^{2^{i_0-1} m} = -1 \bmod n$. ∎

Algorithm (Miller-Rabin)

Input: n odd integer, v, m s.t. $n-1 = 2^v m$, $a \in [1, n-1]$

Output: "n composite" or "n probably prime".

$d = \gcd(a, n)$

if $d \neq 1$ then

    return "n is composite and d is a factor"

end if

$b = \text{rem}(a^m, n)$

if $b \equiv 1 \bmod n$ or $\exists\, i \in [0, v-1]$ s.t. $b^{2^i m} \equiv -1 \bmod n$ then

    return "n probably prime"

else

    return "n is composite"

end if.

The complexity is the same as the Fermat test. We apply it to randomly chosen $a \in [1, n-1]$. Suppose that n is composite and let's study the probability p_n of selecting a liar i.e. an integer a that does not allow to detect if n is composite. We denote by M_n the set of Miller-Rabin liares.

$$M_n = \left\{ x \in (\mathbb{Z}/n\mathbb{Z})^\times : x^m = 1 \text{ or } \exists\, i \in [0, v-1] \text{ s.t. } x^{2^i m} = -1 \right\}$$

strong liars

Theorem: Suppose that n is an odd composite number. Then

$$|M_n| \leq \frac{n-1}{4}$$

Therefore $p_n < \frac{1}{4}$.

We will skip the proof.

Complexities:

- Fermat $O(K \log^2 n)$ where K is the number of tests
- Miller-Rabin $O(K \log^3 n)$ where K is the number of tests
- Solovay-Strassen $O(K \log^3 n)$ where K is the number of tests

$\Rightarrow$ The prob failure of solovay-Strassen is $\leq \frac{1}{2^K}$ (The one of Miller-Rabin is $\leq \frac{1}{4^K}$.

Brief Recap Polynomials

Algorithms	Complexity	
- Multiplication of polynomials		
• Karatsuba	$O(n^{\log_2 3})$	
• FFT	$O(n \log n)$	
- Division of polynomials		
• Euclidean algorithm	$O(m(n-m))$	$n = \deg F$, $m = \deg G$
• Fast Euclidean division using modular inverse	$O(M(n))$ ↳ complexity of multiplication of two polyn of deg $\leq n$.	
• Modular rivers with Newton iteration $g^{-1} \bmod x^e$	$O(M(e))$	
• Euclidean algorithm to find $\gcd(f,g)$	$O(\deg f \cdot \deg g)$	
• Extended Euclidean algorithm to find u, v, g s.t. $g = uf + vg$		

Algorithms	Complexity
• Multipoint evaluation of P s.t. $\deg P \leq n-1$ in $a_0, \dots, a_{n-1}$	$O(M(n) \log n)$
• Interpolation Lagrange Given $a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1}$ find the unique polynomials f of $\deg f < n$ s.t. $f(a_i) = b_i$	$O(n^2)$
• Sum of fractions	$O(M(n) \log n)$
• Fast interpolation	$O(M(n) \log n)$
• Factorization of Polynomials BERLEKAMP	$O(n^\omega + (q+n) M(n) \log n)$ where ω is the exponent of matrix multiplication
• Repeated squaring (square and multiply) From TD9 g^t	$O(\log t)$ where t is exponent

Primality tests	Probability failures
- Fermat	$\leq 1/2$
- Miller-Rabin	$\leq 1/4$
- Solovay-Strassen	$\leq 1/2$

Theory of Resultant:

- Checking if a polynomial has multiple root
- Intersection of two curves
- Implicitation
- Finding minimal polynomial
- Finding gcd of two polynomials