HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2023

20/11/2023. Lecture 10.

1 The Miller–Rabin primality test

For an integer number n we can verify whether it is prime by trying all potential divisors among the candidates $1, 2, \ldots, \lfloor\sqrt{n}\rfloor$. However, this procedure is very slow. If the binary representation of n consists of k digits (i.e., $2^{k-1} \leq n < 2^k$), then the number of candidates $\sqrt{n} \sim \sqrt{2^k} = 2^{k/2}$ is exponential in k. In what follows we discuss an efficient (poly-time) test of primality.

We know that for all prime numbers p and for all $a \in \{1, 2 \ldots, p-1\}$

$$a^{p-1} = 1 \mod p$$

(Fermat's little theorem). This observation motivates the following naive test of primality:

Fermat test `of primality for an integer number` n **:**

1. take a random number $a \in \{1, 2 \ldots, n-1\}$
2. compute $b \leftarrow (a^{n-1} \mod n)$
3. if $b = 1 \mod n - 1$, return "prime" ; otherwise return "not prime".

Fermat's little theorem implies that for all prime numbers the Fermat test always sais *prime*. Is it true that for every composite number the test say *not prime* with a non-negligible probability? Unfortunately, this is not always the case. There exist composite integer numbers (cf. *Carmichael numbers*) for which this test fails for all $a \in \{1, 2 \ldots, n-1\}$.

Fortunately, there is a test that will most likely reveal non-primality for each composite number.

Miller–Rabin test `of primality for an integer number` n **:**

1. denote $n - 1 = m \cdot 2^r$, where m is an odd number (the maximal odd divisor of $n-1$)
2. take a random number $a \in \{1, 2 \ldots, n-1\}$
3. compute the series of numbers
   - $b_0 := a^m \mod n$
   - $b_1 := (b_0^2) = a^{m \cdot 2} \mod n$
   - $b_2 := (b_1^2) = a^{m \cdot 4} \mod n$
   - $\vdots$
   - $b_r := (b_{r-1}^2) = a^{m \cdot 2^r} = a^{n-1} \mod n$

   (we assume that each b_i belongs to $\{0, 1, 2, \ldots, n-1\}$)
4. if $b_0 = 1$, return "prime"

5. if there exists an $i \in \{0, 1, \ldots, r-1\}$ such that $b_i = p - 1$ (equivalently, $b_i = -1 \mod n$), return "prime"

6. in all other cases return "not prime"

In the class we proved the following sattements:

- if n is prime, the Miller–Rabin test says "prime" with probability 1
- if n has at least at least two different prime factors, then the Miller–Rabin test says not "prime" with probability $\geq 1/2$.

We did not proved the fact that the probability of failure is small for n that are powers of prime numbers (such a number is not prime but it has only one prime factor). However, the property "n is a power of an integer number" can be tested deterministically in polynomial time.

Theorem 1. *If n is a prime number, then the Miller–Rabin test returns "prime" with probability* 1.

Sketch of the proof. First of all, from Fermat's little theorem it follows that for every a

$$a^{n-1} = a^{m \cdot 2^r} = 1 \mod n.$$

Thus, $b_r = 1 \mod n$, and the list of the values $(b_0, b_1, \ldots, b_r)$ can look like

$$(1, 1, 1, \ldots, 1)$$

or

$$(*, * \ldots, *, -1, 1, \ldots, 1)$$

or

$$(*, * \ldots, *, 1, 1, \ldots, 1)$$

where $*$ denotes any number that is not equal to $\pm 1 \mod n$. In the first and the second case, the test returns the answer "prime". It remains to show that the third case is impossible.

The third case above means that for some i we have $b_i \neq \pm 1 \mod n$, and $b_{i+1} = 1 \mod n$. Combining this with the fact $b_{i+1} = b_i^2 \mod n$, we see that the equation

$$x^2 = 1 \mod n$$

has at least three different roots: 1, -1, and b_i. However, modulo a prime number n, every polynomial of degree 2 cannot have more than 2 roots. We have arrived to a contradiction, which completes the proof.

Theorem 2. *If n has at least two different prime factors, then the Miller–Rabin test returns "not prime" with a probability $\geq 1/2$.*

Sketch of the proof. If n has at least two different prime factors, than it can be represented as a product $n = n' \cdot n''$ where n' and n'' are co-prime integer numbers strictly greater than 1.

Let i_0 denote the maximal integer number such that there exists at least one $a \in \{1, \ldots, n-1\}$ such that

$$a^{m \cdot 2^{i_0}} = -1 \mod n.$$

(Observe that such an i_0 exists: we know for sure that $(p-1)^m = (-1)^m \mod n = -1 \mod n$ since m is odd.) Further, let

$$H = \{a \in \{1, 2, \ldots, n-1\} \text{ such that } a^{m \cdot 2^{i_0}} = \pm 1 \mod n\}$$

Observe that the Miller–Rabin test can return the (false) answer "prime" for the input n *only* if the randomly chosen a belongs to H. Therefore, to show that the probability of an error is $\leq 1/2$, we need to prove that $|H| < (n-1)/2$.

It is not hard to see that H is a subgroup in the group $(\mathbb{Z}/n\mathbb{Z})^\times$ (with the operation of multiplication modulo n). Hence, to prove that $|H| < |\mathbb{Z}/n\mathbb{Z}|/2$, it is enough to prove that $H \neq \mathbb{Z}/n\mathbb{Z}$. It remains to find $\hat{a} \in \mathbb{Z}/n\mathbb{Z}$ such that $\hat{a} \notin H$.

Let us fix an a such that $a^{m \cdot 2^{i_0}} = -1 \mod n$. Observe that $a^{m \cdot 2^{i_0}} = -1 \mod n'$. Now we inspect the list of numbers

$$a,\ a+n',\ a+2n',\ a+3n',\ \ldots, a+(n''-1)n'$$

We do two simple observations.

Fact 1. For each number b in this list we have $b^{m \cdot 2^{i_0}} = -1 \mod n'$ (since all these numbers are equal to each other modulo n').

Fact 2. All these numbers are pairwise distinct modulo n'' (since the difference between every two numbers $a + in'$ and $a + jn'$ is equal to $(i-j)n'$, which is not divisible by n'').

From Fact 2 it follows that the list contains every possible reminder modulo n'' exactly once, so there must be an element $a + jn'$ that is equal to 1 modulo n''. We take this number as $\hat{a}$. Buy the construction, we have

$$\hat{a} = -1 \mod n' \quad \text{and} \quad \hat{a} = 1 \mod n''.$$

It is clear that $\hat{a} \neq \pm 1 \mod n$. Thus, H does not cover the whole $\mathbb{Z}/n\mathbb{Z}$, and $|H| \leq |\mathbb{Z}/n\mathbb{Z}|/2$. This concludes the proof.

Exercise 1. Construct a polynomial time deterministic algorithm that takes as input a binary representation of a number n and tests whether $n = m^k$ for some integer numbers m and $k > 1$.

Remark 1. The Miller–Rabin test uses randomness. Can we test primality of integer numbers deterministically? The answer to this question is yes. The algorithm invented by Agrawal, Kayal, and Saxena is deterministic, and it verifies primality of a given integer number in polynomial time. But in practice the algorithm by Agrawal–Kayal–Saxena is slower than the Miller–Rabin test.

2 The RSA scheme of electronic signature

We briefly discussed an application of the asymmetric encryption (using RSA as the standard example) in a protocol of *electronic signature* and the network of *Certificate authorities*, which certify the ownership of a public key for Internet users.