1 Primality Testing

The Fermat primality test is a probabilistic test to determine if a number is a probable prime. The test is based on the Fermat little theorem which states that if p is prime, then for any integer a co-prime to p it holds that

$$a^{p-1} \equiv 1 \pmod{p} \ . \tag{1}$$

I.e., if $p = 7$ and $a = 2$, then $2^6 = 64 \equiv 1 \pmod{7}$. If we want to test that p is prime, we can pick random a-s not divisible by p and see if the equality holds. If the equality does not hold for some value a, then p is composite. This congruence is unlikely to hold for a random a if p is comsposite. Therefore, if the equality holds for sufficiently large number of a-s, then we say that p is a probable prime to base a.

For $a = 1$ and $a \equiv -1 \pmod{p}$ the congruence trivially holds. For this reason, a is selected in the range $1 < a < p - 1$. Any integer for which (1) holds is known as a Fermat liar, and such p is called Fermat pseudoprime to base a – a compsite number that passes the Fermat primality test. If we manage to find an a for which (1) does not hold, then a is a Fermat witness for the compositeness of n.

In example, suppose we want to check if 221 is prime. We randomly pick a in the range $1 < a < 221$, say, 38. Then we check if (1) holds.

$$38^{220} \equiv 1 \pmod{221} \ .$$

Then we have two possibilities – 221 is prime, or 38 is a Fermat liar. So we take another a, say 24 and see that

$$24^{220} \not\equiv 1 \pmod{221} \ ,$$

and hence 24 is a Fermat witness for the compositeness of 221. It follows that 38 is a Fermat liar, and 221 is composite. Indeed, $221 = 13 \cdot 17$.

The first problem with this approach is that there are infinitely many Fermat pseudoprimes. A more serious problem is that there are integers p for which all values of a with $\gcd(a, p) = 1$ are Fermat liars. Such integers p are called Carmichael numbers. They are quite rare, but there is an infinite amount of Carmichael numbers. Due to these problems Fermat primality test is not used in this form as described above. More powerful and reliable extensions to the Fermat test exist, such as the Miller–Rabin test.

Theorem 1. If p is a composite number and not a Carmichael number, then at least half of all $a \in \mathbb{Z}/p\mathbb{Z}^\times$ are Fermat witnesses.

Proof. Let a be a Fermat witness, and $a_1, a_2, \ldots, a_s$ be Fermat liars. Then for all $i = 1, 2, \ldots, s$, it holds that

$$(a \cdot a_i)^{p-1} \equiv a^{p-1} \cdot a_i^{p-1} = a^{p-1} \cdot 1 \equiv a^{p-1} \not\equiv 1 \pmod{p} \ .$$

If a is a Fermat witness, then any product of a with a Fermat liar is a Fermat witness. Hence, at least half of a-s are Fermat witnesses. □

Consider the set $L = \{a \in \mathbb{Z}/p\mathbb{Z}^\times : a^{p-1} \bmod p = 1\}$. It can be shown that L is a subgroup of $\mathbb{Z}/p\mathbb{Z}^\times$ under multiplication. First, the identity 1 trivially satisfies the Fermat little theorem, hence $1 \in L$. If $a \in L$, then also $a^{-1} \in L$, since

$$1 = (a \cdot a^{-1})^{p-1} \bmod p = a^{p-1} \cdot (a^{-1})^{p-1} \bmod p = (a^{-1})^{p-1} \bmod p \ ,$$

therefore, $(a^{-1})^{p-1} \bmod p = 1$, and hence $a^{-1} \in L$. Finally, if $a, b \in L$, then $ab \in L$.

$$\begin{cases} a^{p-1} \bmod p = 1 \\ b^{p-1} \bmod p = 1 \end{cases} \implies a^{p-1} \cdot b^{p-1} \bmod p = (ab)^{p-1} \bmod p = 1 \ .$$

Hence, L is a subgroup of $\mathbb{Z}/p\mathbb{Z}^{\times}$, and by Lagrange theorem $|L|$ must divide $|\mathbb{Z}/p\mathbb{Z}^{\times}|$. This means that

$$\frac{|L|}{|\mathbb{Z}/p\mathbb{Z}^{\times}|} \leqslant \frac{1}{2} \ .$$

By selecting a randomly from $\mathbb{Z}/p\mathbb{Z}^{\times}$ the probability to select a Fermat liar is at most $\frac{1}{2}$. The probability to select a Fermat witness is at least $\frac{1}{2}$.

If we run Fermat test 10 times, and all the times the result is that n is a probable prime, then the probability that all 10 times we have been selecting Fermat liars is at most 2^{-10}. The probability that n is a probable prime is then $1 - 2^{-10}$.

A good introduction to group theory and the proof of Fermat little theorem can be seen in `http://www.math.uchicago.edu/~may/VIGRE/VIGRE2011/REUPapers/Momkus.pdf`

2 Exercises

Exercise 1. How would you test if an integer n is prime, using the brute-force approach?

Exercise 2. Apply Fermat primality test to verify the primality of $351, 511$, and 717.

Exercise 3. Solve for x: $x^2 \bmod 63 = 1$, where 63 is the product of two primes 7 and 9.

Exercise 4. Adversary Carol has intercepted two RSA cryptograms, $y_1 = 537$ sent by Alice to Bob, and $y_2 = 285$ sent by Alice to Eve. The public key of Bob is $(e_1 = 18, n_1 = 943)$, and the public key of Eve is $(e_2 = 19, n_2 = 943)$. What is the message m sent by Alice to Bob and Eve?

Exercise 5. Suppose that adversary Carol has intercepted three cryptograms y_1, y_2, y_3 sent to three different users whose public keys are $(e, n_1), (e, n_2), (e, n_3)$. Notice that all public keys use the same public exponent, and different moduli. What does Carol needs to do to reconstruct the message m?