Fermat's Little Theorem

Your name

2020년 5월 23일

그림 1: Fermat (1607 1655)

Fermat's Little Theorem

Fermat's Little Theorem:

If p is prime, then for every a s.t. $a \nmid p$ (i.e. a cannot divide p), $a^{p-1} \equiv 1 \ (mod\ p)$.

Proof. Let S be the nonzero integers modulo p: that is, $S = \{1, 2, 3, \ldots, p-1\}$. We'll first prove that the effect of multiplying these numbers by $a \pmod p$ generates the permutation of S.

The numbers $a^i \bmod p$ and $a^j \bmod p$ are distinct because if $a \cdot i \equiv a \cdot j \pmod p$, then dividing both sides by a(multiplying by a^{-1}) gives $i \equiv j \pmod p$. They are nonzero as $a \cdot 1 \equiv 0$ similarly implies $i \equiv 0$ due to nonzero a. Therefore, the resulting numbers of multiplying S by $a \pmod p$ are all distinct and nonzero. And since they lie in the range $[1, p-1]$, they must be a permutation of S.

Now we can write S as:

$$S = \{1, 2, \cdots, p-1\} = \{a \cdot 1 \bmod p, a \cdot 2 \bmod p, \cdots, a \cdot (p-1) \bmod p\}$$

and multiplying all elements in each representations will give

$$(p-1)! \equiv a^{p-1} \cdot (p-1)!.(\mod p)$$

As p is prime, it is coprime with $(p-1)!$, so we can divide both hands by $(p-1)!$, which gives the theorem. □

Consequently, we can think of the algorithm that picks a positive integer $a < N$ at random and returns YES if $a^{N-1} \equiv 1 \pmod{N}$ (otherwise, return NO). Unfortunately, FERMAT'S LITTLE THEOREM is not an iff statement; therefore, we cannot guarantee the result when the input is not a prime(i.e., the input is composite). It is certain that if input generates "NO," it is composite. But if the result is "YES," we don't know whether the input is prime or not.

Carmichael number

Before improving our algorithm, let's first learn about *Carmichael numbers*, which pass Fermat's test for all a relatively prime to N. Our algorithm will almost certainly fail if these number comes as input. Nevertheless, in a Carmichael-free universe, any non-Carmichael composite number N will fail the test for *at least half the possible values of* a!! Following lemma proves this.

LEMMA:

If $a^{N-1} \not\equiv 1$ *mod* N *for some* a *relatively prime to* N*, then it must hold for at least half the choices of* $a < N$*.*

Proof. Fix any value a for which $a^{N-1} \not\equiv 1 \bmod N$. Then for every $b < N$ that passes Fermat's test with respect to N, there exists it's twin $a \cdot b$, that fails the test:

$$(a \cdot b)^{N-1} \equiv a^{N-1} \cdot b^{N-1} \equiv a^{N-1} \bmod N.$$

Moreover, all these elements $a \cdot b$ are distinct(reference the proof of FERMAT'S LITTLE THEOREM.). This 1-to-1 function $b \mapsto a \cdot b$ shows that at least as many elements fail the test as pass it. □