Fermat's Little Theorem

sjLin

August 6, 2021

The great French mathematician Pierre de Fermat made many important discoveries in number theory. One of the most useful of these states that p divides $a^{p-1} - 1$ whenever p is prime and a is an integer not divisible by p. Fermat announced this result in a letter to one of his correspondents. However, he did not include a proof in the letter, stating that he feared the proof would be too long. Although Fermat never published a proof of this fact, there is little doubt (無庸置疑的) that he knew how to prove it, unlike the result known as Fermat's last theorem. The first published proof is credited to Leonhard Euler. We now state this theorem in terms of congruences.

Theorem 3, Fermat's Little Theorem

If p is prime and a is an integer not divisible by p, then

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

Furthermore, for every integer a we have

$$a^p \equiv a \pmod{p}.$$

Remark:
Fermat's little theorem tells us that if $a \in Z_p$,then $a^{p-1} = 1$ in Z_p.

Fermat's little theorem is extremely useful in computing the remainders modulo p of large powers of integers.

Example 9
Fine $7^{222} \pmod{11}$.

Solution:
We can use Fermat's little theorem to evaluate $7^{222} \pmod{11}$ rather than using the fast modular exponentiation algorithm. By Fermat's little theorem we know that $7^{10} \equiv 1 \pmod{11}$, so $(7^{10})^k \equiv 1 \pmod{11}$for every positive integer k. To take advantage of this last congruence, we divide the exponent 222 by 10, finding that $222 = 22 \cdot 10 + 2$. We now see that

$$7^{222} = 7^{22 \cdot 10 + 2} = (7^{10})^{22} 7^2 \equiv (1)^{22} \cdot 49 \equiv 5 \pmod{11}.$$

It follows that $7^{222} \pmod{11} = 5$.

#

Example 9 illustrated how we can use Fermat's little theorem to compute $a^n \pmod{p}$, where p is prime and $p \nmid a$. First, we use the divisin algorithm to find the quotient q and remainder r when n is divided by $p-1$, so that $n = q(p-1)+r$ where $0 \leq r < p-1$. It follows that $a^n = a^{q(p-1)+r} = (a^{p-1})^q a^r \equiv 1^q a^r \equiv a^r \pmod{p}$. Hence, to find $a^n \pmod{p}$, we only need to compute $a^r \pmod{p}$, We will take advantage of (利用) this simplification many times in our study of number theory.