Lecture Notes for International Mathematical Olympiad

FERMAT'S LITTLE THEOREM

1. Statement and proof

Theorem 1 (Fermat's little theorem)**.** *Let p be a prime with $a \in \mathbb{Z}$. Then $a^p \equiv a \bmod p$. Or equivalently, if $(a,p)=1$, then $a^{p-1} \equiv 1 \bmod p$.*

It suffices to suppose $(a,p)=1$ and prove $a^{p-1} \equiv 1 \bmod p$. We introduce a lemma.

Lemma 2. *Let p be a prime, $a \in \mathbb{Z}$, and $(a,p)=1$. Then*

$$\{a \bmod p, 2a \bmod p, \ldots, (p-1)a \bmod p\} = \{0, 1, \ldots, p-1\}.$$

Proof. Assume $ia \equiv ja \bmod p$ for $1 \leqslant i < j \leqslant p-1$. Then $p \mid a(j-i)$. Since $(a,p)=1$, we see $p \mid (j-i)$. On the other hand, $0 < j-i < p-1 < p$, which contradiction to $p \mid (j-i)$. □

Proof of Theorem 1. Granting the lemma, we see

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \bmod p$$

and hence

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

Note that $p \nmid (p-1)!$, so we have $a^{p-1} \equiv 1 \bmod p$. □

Remark 3. The converse of Fermat's little theorem is not valid, i.e. if we suppose $a^p \equiv a \bmod p$, then p is not necessarily a prime. For a counter example, we seek for n such that $2^n \equiv 2 \bmod n$. But it turns out that $341 = 31 \cdot 11$ works. It suffices to check that $2^{341} \equiv 2 \bmod 341$. In fact,

$$2^{341} \equiv (2^{31})^{11} \equiv 2^{31} \equiv (2^{11})^2 \cdot 2^9 \equiv 2^2 \cdot 2^9 \equiv 2^{11} \equiv 2 \bmod 11,$$

and

$$2^{341} \equiv (2^{11})^{31} \equiv 2^{11} \equiv 2048 \equiv 2 \bmod 31.$$

2. Primary applications

2.1. Find the remainder of a large number.

Problem 4. *Compute* $145^{89} + 3^{2002} \bmod 13$.

Solution. We have

$$145 \equiv 2 \bmod 13 \implies 145^{89} \equiv 2^{89} \bmod 13.$$

By Fermat's little theorem with $a=2$ and $p=13$, $2^{12} \equiv 1 \bmod 13$. So

$$2^{89} \equiv (2^{12})^7 \cdot 2^5 \equiv 2^5 \equiv 6 \bmod 13.$$

Similarly we get $3^{12} \equiv 1 \bmod 13$. Therefore,

$$3^{2002} \equiv (3^{12})^{166} \cdot 3^{10} \equiv (3^3)^3 \cdot 3 \equiv 3 \bmod 13.$$

So $145^{89} + 3^{2002} \equiv 6 + 3 \equiv 9 \bmod 13$. □

Date: August 30, 2022.

2.2. **Carmichael numbers.**

Problem 5. *Prove that there the set*

$$Q = \{n \in \mathbb{N} : 2^n \equiv 2 \bmod n\}$$

has infinitely many elements.

Solution. The idea is to construct a function $\mathbb{N} \to \mathbb{N}$ such that, once some $n \in Q$ is given, then $f(n) \in Q$ with $f(n) > n$. If so, we get infinitely many elements

$$n < f(n) < f(f(n)) < \cdots$$

in Q. We use the fact that if $2^n - 1$ is a prime then so also is n itself. Let $a_n \in Q$ and denote $a_{n+1} = 2^{a_n} - 1$. It follows that a_{n+1} is not a prime. We have

$$2^{a_n} \equiv 2 \bmod a_n \implies a_n \mid 2^{a_n} - 2 = a_{n+1} - 1.$$

Write $a_{n+1} - 1 = ka_n$ for some $k \in \mathbb{Z}$. Then

$$(2^{a_n} - 1) \mid (2^{a_{n+1}-1} - 1) = (2^{a_n})^k - 1.$$

So $2^{a_{n+1}-1} \equiv 1 \bmod a_{n+1}$. It follows that $2^{a_{n+1}} \equiv 2 \bmod a_{n+1}$ and $a_{n+1} \in Q$. This completes the proof. □

Exercise 6. Show that there are infinitely many $n \in \mathbb{N}$ such that

$$n \mid (2^n + 2), \quad (n-1) \mid (2^n + 1).$$

Remark 7. In Problem 5, elements in set Q are called *quasi-prime integers*. Furthermore, if some non-prime n such that $a^n \equiv a \bmod n$ for all $a \in \mathbb{Z}$ uniformly, then n is called a *Carmichael number*.

Proposition 8. *Let n be a square-free composite integer satisfying $(p-1) \mid (n-1)$ for each prime divisor p of n. Then n is a Carmichael number.*

Proof. By assumption we write $n = p_1 \cdots p_k$ the product of distinct primes. Then n is Carmichael if and only if n is composite, and $a^n \equiv a \bmod n$ for all $a \in \mathbb{Z}$. So it suffices to prove that $a^n \equiv a \bmod p_i$ for $i = 1, \ldots, k$.

Suppose p is any prime divisor of n. If $p \mid a$ then there is nothing to prove. Assuming $p \nmid a$, then by Fermat's little theorem, we have $a^{p-1} \equiv 1 \bmod p$. Also, the condition $(p-1) \mid (n-1)$ dictates that $n - 1 = k(p-1)$ for some $k \in \mathbb{Z}$. Then

$$a^{n-1} \equiv (a^{p-1})^k \equiv 1 \bmod p \implies a^n \equiv a \bmod p.$$

This completes the proof. □

Remark 9. The converse of Proposition 8 is also valid. Namely, if n is Carmichael, then it must be square-free and $(p-1) \mid (n-1)$ for each prime divisor $p \mid n$. For example, $561 = 3 \cdot 11 \cdot 17$ is Carmichael whereas $341 = 31 \cdot 11$ is not.

2.3. **Division problems.**

Problem 10. *Given a prime $p = 6k + 1 \geqslant 13$ with $k \in \mathbb{N}$. Denote $m = 2^p - 1$. Prove that*

$$127m \mid (2^{m-1} - 1).$$

Before proving this, recall that for $a, b, m, n \in \mathbb{Z}_{>0}$ with $ab \neq 1$ and $(a, b) = 1$, we have

(1) $(a^m - b^m) \mid (a^n - b^n)$ if and only if $m \mid n$;
(2) $(a^m + b^m) \mid (a^n + b^n)$ if and only if $m \mid n$ and $2 \nmid \frac{n}{m}$;
(3) $(a^m - b^m, a^n - b^n) = a^{(m,n)} - b^{(m,n)}$.

Proof. By (3), we have

$$(127, m) = (2^7 - 1, 2^p - 1) = 2^{(7,p)} - 1 = 2^1 - 1 = 1.$$

On the one hand,

$$\begin{aligned} 127 \mid (2^{m-1} - 1) &\iff (2^7 - 1) \mid (2^{m-1} - 1) &&\iff 7 \mid (m-1) = (2^p - 2) \\ &\iff 2^p \equiv 2 \bmod 7 &&\iff 2^{6k} \equiv 1 \bmod 7 \end{aligned}$$

but this is implied by Fermat's little theorem, as $2^6 \equiv 1 \bmod 7$. On the other hand, by a similar argument,

$$m \mid (2^{m-1} - 1) \iff 2^p \equiv 2 \bmod p,$$

which is again a consequence of Fermat's little theorem. □

3. More advanced problems

Problem 11. *Let $a_1, \ldots, a_n, b_1, \ldots, b_k \in \mathbb{Z}$ satisfies $a_1, \ldots, a_n > 1$. Show that there are infinitely many positive integers d's such that for any $1 \leqslant i \leqslant k$,*

$$S_i = S_i(d) := a_1^d + \cdots + a_n^d + b_i$$

is a composite number.

Proof. We run a similar argument as in the solution to Problem 5. Choose any $d \in \mathbb{N}$ to begin with. For convenience we may assume $(a_1, \ldots, a_n, b_i) = 1$ for each i. Also choose p_i to be a prime divisor of S_i for each i. Construct

$$d_j = d + j(p_1 - 1) \cdots (p_k - 1), \quad j \in \mathbb{Z}_{>0}.$$

Then by Fermat's little theorem, $a_i^{d_j} \equiv a_i^d \bmod p_i$ for each i as $a_r^{p_i - 1} \equiv a_r \bmod p_i$ for some $1 \leqslant r \leqslant n$. It follows that

$$S_i(d_j) = a_1^{d_j} + \cdots + a_n^{d_j} + b_i \equiv S_i = a_1^d + \cdots + a_n^d + b_i \equiv 0 \bmod p_i.$$

On the other hand, $S_i(d_j) > S_i \geqslant p_i$. So each $S_i(d_j)$ for $j \in \mathbb{Z}_{>0}$ is a composite number. This gives us infinitely many such d. □

Problem 12 (IMO, 2005)**.** *Determine all positive integers relatively prime to all the terms of the infinite sequence*

$$a_n = 2^n + 3^n + 6^n - 1, \quad n \geqslant 1.$$

Solution. Equivalently, we are to show that for each prime p there exists some n such that $p \mid a_n$. Namely, the prime divisors for $\{a_n\}$ runs through all prime integers. Since $2 \mid a_2$ and $3 \mid a_2$, we assume $p \geqslant 5$ at work. By Fermat's little theorem,

$$2^{p-1} \equiv 2 \bmod p, \quad 3^{p-1} \equiv 3 \bmod p, \quad 6^{p-1} \equiv 6 \bmod p.$$

Then

$$6a_{p-2} = 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \equiv 3 + 2 + 1 - 6 \equiv 0 \bmod p$$

and hence $p \mid a_{p-2}$ for $(6, p) = 1$. This completes the proof. □

School of Mathematical Sciences, Peking University, 100871, Beijing, China
Email address: daiwenhan@pku.edu.cn