FERMAT'S THEOREM AND ITS CONSEQUENCES

Nirjhar Nath
nirjhar@cmi.ac.in

1 Introduction

In a letter to Bernhard Frénicle de Bessy (1605-1675) dated October 18, 1640, Fermat stated: If p is a prime and a is any integer not divisible by p, then p divides $a^{p-1} - 1$, along with the comment, "I would send you the demonstration, if I did not fear its being too long." This theorem had since been known as "Fermat's Little Theorem" or just "Fermat's Theorem", to distinguish it from Fermat's "Great" or "Last Theorem". Euler published the first proof of this theorem in 1736. However, Leibniz also left an identical argument in an unpublished manuscript sometime before 1683.

2 Preliminaries

The theorems and proofs to be discussed require some preliminaries, which are explained below.

2.1 Congruences and classes of residues

If $a, b \in \mathbb{Z}$ and $b = ak$ for some $k \in \mathbb{Z}$, then we say "a is a divisor of b" or "a divides b", and write $a \mid b$. If $m \mid x - a$, we say "x is congruent to a modulo m", and write $x \equiv a \pmod{m}$.

If $x \equiv a \pmod{m}$, then a is called *residue* of x modulo m. If $0 \leq a \leq m-1$, then a is the *least residue* (non-negative) of x. Thus, two integers a and b congruent modulo m have the same residues modulo m. A *class of residues* modulo m is the class of all the integers congruent to a given residue modulo m, and every member of the class is called a *representative* of the class. In this case, there are a total of m classes, represented by $0, 1, \ldots, m-1$. These m numbers, or any other set of m numbers which belongs to each of the m

classes, form a *complete set* (or *system*) *of incongruent residues modulo* m, or simply *complete set* (or *system*) *of residues modulo* m.

Assuming the knowledge of the basic properties of congruences, we prove some theorems.

THEOREM 1. If $(k, m) = d$, then

$$ka \equiv ka' \,(\mathrm{mod}\, m) \implies a \equiv a' \left(\mathrm{mod}\, \frac{m}{d}\right)$$

PROOF. Since $(k, m) = d$, so $k = dk_1$ and $m = dm_1$ for some k_1, m_1 with $(k_1, m_1) = 1$. Then

$$\frac{ka - ka'}{m} = \frac{k_1(a - a')}{m_1}$$

and since $m \mid ka - ka'$ and $(k_1, m_1) = 1$, so

$$m_1 \mid a - a' \text{ or, } a \equiv a' \,(\mathrm{mod}\, m_1)$$

□

A particular case of this theorem is the following.

COROLLARY 1.1. If $(k, m) = 1$, then

$$ka \equiv ka' \,(\mathrm{mod}\, m) \implies a \equiv a' \,(\mathrm{mod}\, m)$$

THEOREM 2. If $a_1, a_2, \ldots, a_m$ is a complete set of incongruent residues (mod m) and $(k, m) = 1$, then $ka_1, ka_2, \ldots, ka_m$ is also such a set.

PROOF. Using COROLLARY 1.1 we have,

$$ka_i \equiv ka_j \,(\mathrm{mod}\, m) \implies a_i \equiv a_j \,(\mathrm{mod}\, m)$$

which is impossible unless $i = j$, by hypothesis. □

THEOREM 3. If $(m, m') = 1$, a runs through a complete set of residues (mod m) and a' runs through a complete set of residues (mod m'). Then $a'm + am'$ runs through a complete set of residues (mod mm').

PROOF. Firstly, there are mm' integers $a'm + am'$. Suppose

$$a_1'm + a_1m' \equiv a_2'm + a_2m' \,(\mathrm{mod}\, mm')$$

Then,

$$a_1'm + a_1m' \equiv a_2'm + a_2m' \,(\mathrm{mod}\, m)$$

i.e.,

$$a_1m' \equiv a_2m' \,(\mathrm{mod}\, m)$$

Now, $(m, m') = 1$ gives

$$a_1 \equiv a_2 \,(\mathrm{mod}\, m)$$

and similarly,

$$a_1' \equiv a_2' \,(\mathrm{mod}\, m')$$

which are impossible by hypothesis. □

We present below some lemmas that will be necessary to prove some theorems in the following sections.

LEMMA 1: The product of any n successive positive integers is divisible by $n!$.

PROOF: Let

$$P_{n,m} = m(m+1)\cdots(m+n-1)$$

be the product of n successive positive integers starting from m.

LEMMA 2: If p is a prime, then $\binom{p}{k} \equiv 0 \pmod{p}$ for $1 \leq k \leq p-1$.

PROOF: Since

$$k!\binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0(\mathrm{mod}\, p)$$

we are done. □

3 Fermat's theorem

We begin with proving Fermat's theorem.

THEOREM 4 (Fermat's theorem). If p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$$

PROOF. Consider the set S of the first $p-1$ positive integer multiples of a, i.e.,

$$S = \{a, 2a, \ldots, (p-1)a\}$$

Since $\{1, 2, \ldots, p-1\}$ is a complete set of incongruent residues (mod p), so by THEOREM 2, S is also such a set. Therefore, the elements of S must be congruent modulo p to $1, 2, \ldots, (p-1)$ taken in some order. Thus, we have

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \,(\mathrm{mod}\, p)$$

i.e.,

$$a^{p-1}(p-1)! = (p-1)! \,(\mathrm{mod}\, p)$$

Since p doesn't divide any of $1, 2, \ldots, (p-1)$, so $p \nmid (p-1)!$ and hence

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$$

□

More generally, we can drop the condition $p \nmid a$ to arrive at the following corollary.

COROLLARY 4.1. If p is a prime, then $a^p \equiv a \,(\mathrm{mod}\, p)$.

PROOF. This is trivial when $p \mid a$, since then $a^p \equiv 0 \equiv a \,(\mathrm{mod}\, p)$. If $p \nmid a$, the result of THEOREM 1 can be multiplied by a on both sides to get

$$a^p \equiv a \,(\mathrm{mod}\, p)$$

□

Remark. There is a different proof of COROLLARY 4.1, using induction on a. We first prove it for $a \in \mathbb{N}$. The statement is clearly true for $a = 0$ and $a = 1$. Assuming that the statement is true for some $a \in \mathbb{N}$, we shall prove that it is true for $a+1$ also. In light of the binomial theorem,

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} = a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1$$

Observe that

$$\binom{p}{k} \equiv 0 \,(\mathrm{mod}\, p) \;\text{ for }\; 1 \leq k \leq p-1$$

because note that

$$k! \binom{p}{k} = p(p-1) \cdots (p-k+1) \equiv 0 \,(\mathrm{mod}\, p)$$

and so $p \mid k!$ or $p \mid \binom{p}{k}$, but $p \mid k!$ implies that $p \mid l$ for some l satisfying $1 \leq l \leq k \leq p-1$, which is absurd. This gives

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \,(\mathrm{mod}\, p)$$

Now, if $a < 0$, then $a \equiv r \,(\mathrm{mod}\, p)$ for some r satisfying $0 \leq r \leq p-1$. So we still have

$$a^p \equiv r^p \equiv r \equiv a \,(\mathrm{mod}\, p)$$

□

LEMMA 1. If p and q are distinct primes with $a^p \equiv a \,(\mathrm{mod}\, q)$ and $a^q \equiv a \,(\mathrm{mod}\, p)$, then

$$a^{pq} \equiv a \,(\mathrm{mod}\, pq)$$

PROOF. Using COROLLARY 4.1, we have

$$a^{pq} = (a^q)^p \equiv a^p \equiv a \,(\mathrm{mod}\, p)$$

Similarly, we have

$$a^{pq} \equiv a \,(\mathrm{mod}\, q)$$

Hence,

$$a^{pq} \equiv a \,(\mathrm{mod}\, pq)$$

□

4 Euler's generalization

Euler extended Fermat's theorem which concerns congruences with prime moduli, to arbitrary moduli. While doing so, he defined an important number-theoretic function, described below.

4.1 Euler's phi-function $\phi(n)$

DEFINITION 1. For $m \geq 1$, $\phi(m)$ denotes the number of positive integers not exceeding m that are relatively prime to m, i.e., the number of integers n such that $0 < n \leq m$ and $(n, m) = 1$.

There are $\phi(m)$ classes of residues (mod m) relatively prime to m, and any such set of $\phi(m)$ residues, one from each class, is called a *complete system* (or *set*) *of residues relatively prime to* m. One such set is the set of $\phi(m)$ positive integers less than and relatively prime to m.

THEOREM 5. If $a_1, a_2, \ldots, a_{\phi(m)}$ is a complete set of residues relatively prime to m and $(k, m) = 1$, then $ka_1, ka_2, \ldots, ka_{\phi(m)}$ is also such a set.

PROOF. Since $(k, m) = 1$ and $(a_i, m) = 1$, so $(ka_i, m) = 1$. Now, as in the proof of THEOREM 2,

$$ka_i \equiv ka_j \,(\mathrm{mod}\, m) \implies a_i \equiv a_j \,(\mathrm{mod}\, m)$$

which is impossible unless $i = j$, by hypothesis. □

DEFINITION 2. A function f is said to be *multiplicative* if $(m, m') = 1$ implies

$$f(mm') = f(m)f(m')$$

THEOREM 6. The function ϕ is multiplicative.

PROOF. If $(m, m') = 1$, then by THEOREM 3, $a'm + am'$ runs through a complete set of residues (mod mm') when a and a' run through complete sets of residues (mod m) and (mod m') respectively. We have

$$\begin{aligned}
&(a'm + am', mm') = 1 \\
\iff &(a'm + am', m) = 1, (a'm + am', m') = 1 \\
\iff &(am', m) = 1, (a'm, m') = 1 \\
\iff &(a, m) = 1, (a', m') = 1
\end{aligned}$$

Thus, the $\phi(mm')$ numbers less than and relatively prime to mm' are the least positive residues (mod mm') of the $\phi(m)\phi(m')$ values of $a'm + am'$ for which a and a' are relatively prime to m and m' respectively, i.e.,

$$\phi(mm') = \phi(m)\phi(m')$$

□

Incidentally we have proved the following theorem.

THEOREM 7. If $(m, m') = 1$, a runs through a complete set of residues relatively prime to m and a' runs through a complete set of residues relatively prime to m'. Then $a'm + am'$ runs through a complete set of residues (mod mm').

We can now find the value of $\phi(m)$ for any integer $m > 1$. It is sufficient to

calculate $\phi(m)$ when m is a power of a prime, given by the following theorem.

THEOREM 8. If p is a prime and $k > 0$, then

$$\phi\left(p^c\right) = p^c - p^{c-1} = p^c\left(1 - \frac{1}{p}\right)$$

PROOF. There are $p^c - 1$ positive integers less than p^c, of which only the first $p^{c-1} - 1$ multiples of p namely $1p, 2p, \ldots, (p^{c-1} - 1)p$ are divisors of p^c. Thus,

$$\phi(p^c) = p^c - 1 - (p^{c-1} - 1) = p^c - p^{c-1} = p^c\left(1 - \frac{1}{p}\right)$$

□

Using THEOREM 6 and THEOREM 8, we immediately have the more general theorem for any integer $m > 1$.

THEOREM 9. If an integer $m > 1$ has prime factorization $m = \prod_{i=1}^{k} {p_i}^{c_i}$, then

$$\phi(m) = \prod_{i=1}^{k}\left({p_i}^{c_i} - {p_i}^{c_i - 1}\right) = m\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$$

5 Pseudoprimes

Over 25 centuries ago, Chinese mathematicians claimed that n is prime if and only if $n \mid 2^n - 2$, a counter-example to which was discovered in 1819 that $341 \mid 2^3 41$ but $341 = 11 \cdot 31$. However, this statement is true for all $n \leq 340$.

DEF. A composite n is called *pseudoprime* if $n \mid 2^n - 2$.