Proofs of Number Theory Theorems

Frank Yu

Sichuan University

Contents

Fermat's Little Theorem

If there exist integers a and p, where p is a prime number, and a and p are coprime, then:

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

Proof of Fermat's Little Theorem

- **Lemma1** If a, b, c are any three integers, and m is a positive integer, if $(c, m) = 1$, $c \cdot a \equiv c \cdot b \pmod{m}$
then
$$a \equiv b \pmod{m}$$
- **Proof of lemma1**
Since $c \cdot a \equiv c \cdot b \pmod{m}$, we can write:
$$c \cdot a - c \cdot b = k \cdot m \quad \text{for some integer } k.$$
that is
$$c \cdot (a - b) = k \cdot m \quad (1)$$
Since $\gcd(c, m) = 1$, by Bézout's Thm, there exist integers x and y such that:
$$c \cdot x + m \cdot y = 1. \quad (2)$$
Multiplying both sides of equation (1) by x gives:
$$c \cdot x \cdot (a - b) = k \cdot m \cdot x \quad (3)$$

Proof of Fermat's Little Theorem

- **Lemma1** If a, b, c are any three integers, and m is a positive integer, if $(c, m) = 1$, $c \cdot a \equiv c \cdot b \pmod{m}$ then
$$a \equiv b \pmod{m}$$
- **Proof of lemma1**
Since $c \cdot a \equiv c \cdot b \pmod{m}$, we can write:
$$c \cdot a - c \cdot b = k \cdot m \quad \text{for some integer } k.$$
that is
$$c \cdot (a - b) = k \cdot m \quad (1)$$
Since $\gcd(c, m) = 1$, by Bézout's Thm, there exist integers x and y such that:
$$c \cdot x + m \cdot y = 1. \quad (2)$$
Multiplying both sides of equation (1) by x gives:
$$c \cdot x \cdot (a - b) = k \cdot m \cdot x \quad (3)$$

- **Proof of lemma1(continued)**
  Substituting (2) into (3):

$$(1 - m \cdot y) \cdot (a - b) = k \cdot m \cdot x \quad (4)$$

  that is

$$(a - b) - m \cdot y \cdot (a - b) = k \cdot m \cdot x$$

  Therefore:

$$a \equiv b \pmod{m}.$$

Complete Residue System

- **Definition** A complete residue system modulo m is a set of integers such that each integer is congruent to exactly one element of the set modulo m. In other words, for a positive integer m, a set of integers $S = \{a_1, a_2, \ldots, a_m\}$ is a complete residue system modulo m if:
  1. For every integer n, there exists exactly one $a_i \in S$ such that:
  $$n \equiv a_i \pmod{m}.$$
  2. All elements in S are distinct modulo m.
- **Example** For $m = 5$, one possible complete residue system modulo 5 is:
  $$S = \{0, 1, 2, 3, 4\}.$$
  Other examples of complete residue systems modulo 5 include:
  $$S = \{-2, -1, 0, 1, 2\}, \quad S = \{3, 4, 5, 6, 7\}.$$

Proof of Fermat's Little Theorem

- **Lemma2** Let m be an integer with $m > 1$, and let b be an integer such that $\gcd(m, b) = 1$. If $a[1], a[2], a[3], \ldots, a[m]$ is a complete residue system modulo m, then:

  $$b \cdot a[1], b \cdot a[2], b \cdot a[3], \ldots, b \cdot a[m]$$

  also forms a complete residue system modulo m.
- **Proof of lemma2**
  Proof by contradiction Suppose

  $$b \cdot a[1], b \cdot a[2], b \cdot a[3], \ldots, b \cdot a[m]$$

  does not form a complete residue system modulo m By definition, there exists i,j, such that

  $$b \cdot a[i] \equiv b \cdot a[j] \pmod{m}.$$

  By Lemma1,

  $$a[i] \equiv a[j] \pmod{m}.$$

  Contradiction

Proof of Fermat's Little Theorem

Construct a complete residue system modulo the prime p, consider the set:

$$P = \{1, 2, 3, \ldots, p-1\}.$$

By Lemma2 the set:

$$A = \{a, 2a, 3a, \ldots, (p-1)a\}$$

is also a complete residue system modulo p.
By the properties of a complete residue system, we have:

$$1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-1) \equiv a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \pmod{p}.$$

Canceling $(p-1)!$ from both sides (by lemma1, because $(p-1)!$ and p are coprime), we obtain:

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

Wilson's Theorem

The congruence:

$$(p-1)! \equiv -1 \pmod{p}$$

is a necessary and sufficient condition for p to be a prime number.

Proof of Wilson's Theorem

- If

$$(p-1)! \equiv -1 \pmod{p}$$

then p is a prime number.

- **Proof**

Proof by contrapositive. Suppose p is a composite. Then $1, 2, ..., p-1$ include all its factors. Hence

$$(p-1)! \equiv 0 \pmod{p}$$

So p is a prime.

Proof of Wilson's Theorem

- If p is a prime number, then

$$(p-1)! \equiv -1 \pmod p$$

.

- **Proof**
  Note that

$$1 \cdot (p-1) \equiv -1 \pmod p$$

So we need to prove:

$$2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1 \pmod p.$$

Let $S = \{2, 3, ..., p-2\}$
For $a \in S, gcd(a, p) = 1$, by Bézout's Thm, there exists integers b, x, such that,

$$a \cdot b + x \cdot p = 1$$

Proof of Wilson's Theorem

- **Proof(continued)**
  Which implies
  $$a \cdot b \equiv 1 \pmod{p}$$
  We could find b' in $\{1, 2, ..., p-1\}$, such that
  $$b' \equiv b \pmod{p}$$
  that is
  $$a \cdot b' \equiv 1 \pmod{p}$$
  Firstly, we prove that $b' \neq 1$ OTW,
  $$a \equiv 1 \pmod{p}$$
  but no element in S satisfies it
  Secondly, we prove that $b' \neq p-1$ OTW,
  $$a \cdot (p-1) \equiv 1 \pmod{p}$$
  that is
  $$a \equiv -1 \pmod{p}$$

Proof of Wilson's Theorem

- **Proof(continued)**
  But also, no element in S satisfies it
  Hence, $b' \in S$
  We conclude that for $a \in S$, we could find $b' \in S$, such that
  $$a \cdot b' \equiv 1 \pmod{p} \quad (1)$$
  After the proof of the existence of b', we prove the uniqueness. Suppose for $c' \in S$,
  $$a \cdot c' \equiv 1 \pmod{p} \quad (2)$$
  From (1) (2)
  $$a \cdot (b' - c') \equiv 0 \pmod{p}$$
  As $gcd(a, p) = 1$, By Lemma1,
  $$b' \equiv c' \pmod{p}$$
  with the condition of $b', c' \in S$, $b' = c'$

Proof of Wilson's Theorem

- **Proof(continued)**
  Next prove that $b' \neq a$ OTW,

$$a \cdot a \equiv 1 \pmod{p}$$

that is $p|(a+1)(a-1)$ but
$gcd(p, a+1) = 1, gcd(p, a-1) = 1$, contradiction
THUS, we could divide S into $(p-3)/2$ pairs (p=2 is trivial, we do not need to discuss here)
each pair (a, b) satisfies $a \neq b$,

$$a \cdot b \equiv 1 \pmod{p}$$

Hence

$$2 \cdot 3 \cdot \dots \cdot (p-2) \equiv 1^{(p-3)/2} \pmod{p}.$$

Q.E.D.