In this lecture, we prove Wilson's Theorem

Theorem: Let p be a prime number. Then:

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

Example: $p=2$ $(2-1)! = 1 \equiv -1 \pmod{2}$

$p=3$ $(3-1)! = 2 \equiv -1 \pmod{3}$

$p=5$ $(5-1)! = 24 \equiv -1 \pmod{5}$

$p=7$ $(7-1)! = 720 \equiv -1 \pmod{7}$

Definition: Let p be a prime, and let $a \in \{1, 2, \cdots p-1\}$

We define $\bar{a}$ (or a^*) to be the number

in $\{1, 2, \cdots p-1\}$ satisfying

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

$\bar{a}$ is called the <u>inverse</u> of $a \pmod{p}$.

Remark: the choice of $\bar{a}$ is dependent on the modulus. Therefore, sometimes we write $\bar{a} \pmod{p}$

Example: $p=7$ $\quad a=5$

$$5\cdot 3 = 3\cdot 5 \equiv 1 \pmod{7} \Rightarrow \bar{a} = 3 \pmod{7}$$

$p=11$ $\quad a=4$

$$3\cdot 4 = 4\cdot 3 \equiv 1 \pmod{11} \Rightarrow \bar{a} = 3 \pmod{11}$$

Proposition: For $a \in \{1, 2, \cdots, p-1\}$, $\bar{a}$ always exists and it is unique.

Proof: Existence: (We need to show: for any $a \in \{1, 2, \cdots, p-1\}$ we can $\bar{a} \in \{1, 2, \cdots p-1\}$)

Let $a \in \{1, 2, \cdots p-1\}$. Then $\gcd(a, p) = 1$.

Then we can find r, s such that

$$ra + sp = 1.$$ This also shows: $\gcd(r, p) = 1$.

By Euclidean algorithm, we can find q and r_0 such that

$$r = q\cdot p + r_0 \quad \text{with } 1 \leq r_0 \leq p-1.$$

Substitute this into the previous equation:

$$r_0 a + p(qa + s) = 1$$

This shows: $r_0 a = a r_0 \equiv 1 \pmod p$

Uniqueness: We need to show: if

$$a a_1 = a_1 a \equiv 1 \pmod p \qquad a_1 \in \{1, \dots p-1\}$$

and

$$a a_2 = a_2 a \equiv 1 \pmod p \qquad a_2 \in \{1, \dots p-1\}$$

then $a_1 = a_2 \pmod p$

Suppose that

$$a a_1 \equiv a_1 a \equiv 1 \pmod p \qquad a_1 \in \{1, \dots p-1\}$$

$$a a_2 \equiv a_2 a \equiv 1 \pmod p \qquad a_2 \in \{1, \dots, p-1\}$$

Then $a(a_1 - a_2) \equiv 1 - 1 \pmod p$

$\Rightarrow \quad a(a_1 - a_2) \equiv 0 \pmod p$

$a \in \{1, \dots p-1\} \qquad \gcd(a, p) = 1$

The equation becomes: $a_1 \equiv a_2 \pmod p$

$a_1, a_2 \in \{1, \dots p-1\} \Rightarrow a_1 = a_2$ $\square$

Fact: Let p fixed. Then:

(1) $\overline{1} = 1$

(2) $\overline{p-1} = p-1. \equiv -1 \pmod p$

(3) For $a \in \{1,2,\cdots p-1\}$. $\bar{\bar{a}} = a$.

Proof: (1) $1 \cdot 1 \equiv 1 \pmod p \Rightarrow 1 = \bar{1}$

(2) $(p-1)\cdot(p-1) = p^2 - 2p + 1 \equiv 1 \pmod p$

$\Rightarrow \overline{p-1} = p-1 \qquad p-1 \equiv -1 \pmod p$ ✓

( ) By definition:

$$a\bar{a} = \bar{a}a \equiv 1 \pmod p$$

Therefore:

$$\bar{\bar{a}}\bar{a} = \bar{a}\bar{\bar{a}} \equiv 1 \pmod p$$

Hence: $\bar{\bar{a}} = a$. ∎.

Proposition: Let p be a prime, and $a \in \{1, \cdots p-1\}$.

Then $a = \bar{a}$ if and only if $a = 1$ or $p-1$.

In other words, $a \neq \bar{a}$ for $a \in \{2, \cdots p-2\}$

Proof: Notice that: $a = \bar{a}$ if and only if $a \cdot a \equiv 1 \pmod p$

if and only if a is a solution for $x^2 \equiv 1 \pmod p$.

$a = 1$ and $a = p-1$ are solutions for $x^2 \equiv 1 \pmod p$.

Therefore, it suffices to show: the congruent equation:

$$x^2 \equiv 1 \pmod{p}$$

has at most two solutions.

Proof by contradiction: suppose not, we have:

$$a_1^2 \equiv a_2^2 \equiv a_3^2 \equiv 1 \pmod{p} \quad \text{for} \quad a_1, a_2, a_3 \in \{1, \cdots p-1\}$$

and they are <u>distinct</u> numbers

This implies: $a_1^2 \equiv a_2^2 \pmod{p} \Rightarrow p \mid a_1^2 - a_2^2 = (a_1 - a_2)(a_1 + a_2)$

$a_1^2 \equiv a_3^2 \pmod{p} \Rightarrow p \mid a_1^2 - a_3^2 = (a_1 - a_3)(a_1 + a_3)$

If $p \mid a_1 - a_2$, then $a_1, a_2 \in \{1, \cdots p-1\}$ implies that $a_1 = a_2$

If $p \mid a_1 - a_3$, then $a_1, a_3 \in \{1, \cdots p-1\}$ implies that $a_1 = a_3$

Then $p \mid a_1 + a_2$ and $p \mid a_1 + a_3$

$$\Rightarrow \quad p \mid a_2 - a_3$$

This is impossible since $a_2 \neq a_3 \in \{1, \cdots p-1\}$

A contradiction!

Therefore: $x^2 \equiv 1 \pmod{p}$ has at most two solutions. $\square$

Proof of Theorem: Let $a \in \{2, \cdots p-2\}$

Then by the uniqueness of $\overline{a}$ and the Fact,

$\overline{a} \in \{2, \cdots p-2\}$

Then we write:

$(p-1)! = 1 \cdot 2 \cdot 3 \cdots\cdots (p-3)(p-2)(p-1)$

We leave the term 1 and the term $(p-1)$.

For other terms, we group it with its inverse.

Then $1 \cdot 2 \cdot 3 \cdots (p-3)(p-2)(p-1)$

$\equiv 1 \cdot (2 \cdot \overline{2} \cdots\cdots) \cdot (p-1)$

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

$\equiv -1 \pmod{p}$ $\square$