Chapter 9

In this lecture, we prove the following theorem:

Theorem 9.1 (Fermat's Little Theorem)

Let p be a prime number, and let a be any number with $a \not\equiv 0 \pmod{p}$. Then:

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

Example: Take $p=7$ and $a=3$

$$3^{7-1} = 3^6 = 729$$

$$729 - 1 = 728 = 7 \cdot 104$$

$$\Rightarrow \quad 3^{7-1} \equiv 1 \pmod{7}.$$

We will give two proof for Fermat's Little Theorem.

The 1st proof is based on the following observation:

we again look at $p=7$ and $a=3$.

We list all nonzero incongruent number for $p=7$:

$(*)$ $\quad 1, 2, 3, 4, 5, 6.$

(Sometimes they are also called residue classes if we write:

$1 \pmod 7)$, $2 \pmod 7$, $3 \pmod 7$, $4 \pmod 7$, $5 \pmod 7$ $6 \pmod 7$

We multiply (*) by 3, and reduce modulo 7:

x	1	2	3	4	5	6
$x \pmod 7$	1	2	3	4	5	6
$3x$	3	$3\cdot 1$	$3\cdot 2$	$3\cdot 4$	$3\cdot 5$	$3\cdot 6$
$3x \pmod 7$	3	6	2	5	1	4

Each of 1, 2, 3, 4, 5, 6 appears exactly one time in row 2 (and row 4)

This means:

$$(3\cdot 1)(3\cdot 2)(3\cdot 3)(3\cdot 4)(3\cdot 5)(3\cdot 6) \equiv (1)(2)(3)(4)(5)(6) \pmod 7$$

$$\|$$

$$3^6\cdot(1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6) \equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6 \pmod 7$$

$$3^6\cdot(6!) \equiv 6! \pmod 7$$

We can show: $\gcd(6!, 7) = 1$

We can cancel $6!$ on each side. and it becomes:

$$3^6 \equiv 1 \pmod 7.$$

Now we introduce several lemmas before the 1st proof:

Lemma 1: If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$,

then $a \equiv b \pmod m$

Proof: Homework!

Lemma 2: Let p be a prime, then

$$\gcd((p-1)!, p) = 1.$$

Proof: Suppose not. Then we can find another prime

q such that $p' \mid \gcd((p-1)!, p)$

$q \mid p \Rightarrow q = p.$

Therefore $p \mid (p-1)!$

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

p divides at least one of them.

This is impossible since $1, 2, 3, \cdots p-1 < p$

(If $p \mid n$, then $n > p$) $\square$

Lemma 3: Let p be a prime number, and let a be a number satisfying $a \not\equiv 0 \pmod{p}$.

Then the numbers:

$$a, 2a, 3a, \cdots (p-1)a \pmod{p}$$

are the same as:

$$1, 2, 3, \cdots (p-1) \pmod{p}.$$

although they may be in a different order.

Proof: The list of $a, 2a, 3a, \cdots (p-1)a$ contains $\underline{p-1}$ numbers and none of them are divisible by p.

Claim: every two numbers ja, ka ($j \neq k$) in the list are <u>not</u> congruent $(1 \leq j \leq p-1,\ 1 \leq k \leq p-1)$

Suppose not, then we can find ja, ka such that $p \mid ja - ka = (j-k)a$

Then $p \mid (j-k)$ or $p \mid a$.

$p \nmid a$ ($a \not\equiv 0 \bmod p$) and hence $p \mid (j-k)$

However, we take $1 \leq j \leq p-1$

$1 \leq k \leq p-1$

$-(p-2) \leq j-k \leq p-2$

This implies $j-k=0$ and $\underline{j=k}$ A contradiction.

Therefore, in the list

$a \pmod p$, $2 \pmod p$ $\cdots$ $(p-1)a \pmod p$

there are $p-1$ distinct nonzero values mod p.

However, there are exactly $p-1$ distinct nonzero values mod p:

$1 \pmod p$, $2 \pmod p$ $\cdots$ $(p-1) \pmod p$

Therefore,

$$\{a \pmod p,\ 2a \pmod p,\ \cdots\ (p-1)a \pmod p\}$$
$$= \{1 \pmod p,\ 2 \pmod p, \cdots\ (p-1) \pmod p\}.$$

1st proof of Fermat's Little Theorem:

By Lemma 3, the sets above are ~~the~~ same.

Multiply them together, we get:

$$(a\cdot 1)(a\cdot 2)\cdots(a\cdot(p-1)) \equiv (1)(2)\cdots(p-1) \bmod p$$
$$\|$$
$$a^{p-1}\cdot(p-1)! \equiv (p-1)! \pmod p$$

Lemma 2 shows: $\gcd((p-1)!, p) = 1$

By Lemma 3: we can cancel $(p-1)!$ on both sides:

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