week 5

Recall for a positive integer modulus n.

we have the two groups

- $(\mathbb{Z}_n, +)$ $\quad \mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$
- $(U(n), \times)$ $\quad U(n) = \{x \in \mathbb{Z}_n : \underbrace{\gcd(x,n)=1}\}$

needed in order for x^{-1} modulo n to exist.

We've seen how if we take an element $g \in G$ from a group we can form $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ the cyclic <u>subgroup of G generated by g</u>.

The size of $\langle g \rangle$ is known as the order of $\langle g \rangle$, or simply the order, $|g|$, of the element g.

i.e. $|g|$ = least positive integer k such that $g^k = e$.

If k finite

$\Rightarrow \langle g \rangle = \{ g^0 = e, g^1 = g, g^2, g^3, \dots, g^{k-1} = g^{-1} \}$

For the groups $U(n)$, what can $|x|$ be, for $x \in U(n)$?

Eg $p = 13$, $U(13) = \{ x \in \mathbb{Z}_{13} : \gcd(a, 13) = 1 \}$

$= \{ 1, 2, \dots, 12 \}$

So $|U(13)| = 12$

$\{ |x| : x \in U(13) \} = \{ 1, 2, 3, 4, 6, 12 \}$

$\{ |x| : x \in U(17) \} = \{ 1, 2, 4, 8, 16 \}$

$\{ |x| : x \in U(31) \} = \{ 1, 2, 3, 5, 6, 10, 15, 30 \}$

We seem to be seeing all the factors of $p-1$ in each case.

or in other words. The sizes of cyclic subgroups in $U(p)$, seem to be factors of $p-1$, $p-1 = |U(p)|$

What about non-primes.

$|U(100)| = 40$, orders of elements in $U(100) = \{1, 2, 4, 5, 10, 20\}$

again, all are factors of $|U(100)|$, but not <u>all</u> the factors.

$|U(500)| = 200$, orders $= \{1, 2, 4, 5, 10, 20, 25, 50, \cancel{200}\ 100\}$

Could we conjecture.

$\boxed{\text{for any } g \in G,\ \text{if } |G| \text{ is finite then } |g| = |\langle g \rangle| \text{ divides } |G|.}$

in fact something stronger is true.

Lagrange's Theorem

$\boxed{\text{If } |G| \text{ finite, and } H \text{ is a subgroup of } G, \text{ then } |H| \text{ divides } |G|.}$

There's a special name for $|U(n)|$. The Euler totient function $\phi(n)$ is defined as

$\phi(n) = |U(n)| =$ number of integers m, $1 \leq m \leq n$, such that $\gcd(m,n) = 1$.

We've seen $\phi(p) = p-1$

$\phi(100) = 40$, $\phi(500) = 200$.

But what is $\phi(n) = ?$ in general.

First we'll prove a couple of special cases of Lagrange's Theorem in number theory.

Fermat's Little Theorem p prime.

For any $a \in U(p) = \{1, \ldots, p-1\}$ (or $\gcd(a,p)=1$ or $p \nmid a$)

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

or $a^{p-1} = 1$ in $U(p)$.

this implies that $|\langle a \rangle| = |a|$ divides $p-1$

Proof

Consider the product $\prod_{j=1}^{p-1} j$

$$\prod_{j=1}^{p-1} j = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-1) = (p-1)!$$

and then this same product in a different order.

Consider the sequence.

$a, 2a, 3a, 4a, \ldots\ldots, (p-1)a$ (*)

What we're looking at here is a permutation of $1, 2, 3, \ldots, p-1$.

Pf: $ja = ka$
$\Rightarrow jaa^{-1} = kaa^{-1}$ } in $U(p)$
$\Rightarrow j = k$

Therefore.

$$\prod_{j=1}^{p-1} j = (p-1)! \equiv \prod_{j=1}^{p-1} aj \pmod p$$

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

But $(p-1)! \in U(p)$, hence $((p-1)!)^{-1}$ exist in $U(p)$

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

For non-prime modulus F.L.T. generalises to

Euler's theorem

For any $a \in U(n)$,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

<u>Proof</u> Repeat the same argument for F.L.T. but with

$$\left(\prod_{j \in U(n)} j \right)$$

in place of $(p-1)!$

and remember that $\phi(n) = |U(n)|$.

One application of this is to simplifying large powers in $U(n)$.

$$x^M \equiv ? \pmod{n}$$

, for M very large.

If we find fixed $M \equiv m \mod \phi(n)$

i.e. $M = q\phi(n) + m$, $0 \leq m < \phi(n)$

$$x^M = x^{(q\phi(n)+m)}$$

$$= \left(x^{\phi(n)}\right)^q x^m$$

$$\equiv 1^q x^m \pmod n$$

$$\equiv x^m \pmod n$$

much easier computationally than

See Q2. on CWK.

Short break $\longrightarrow$ discover a formula for $\phi(n)$.

Apology: in NT notes $U(n)$ is written as $\mathbb{Z}_n^\times$

Theorem 5.1 Formula for $\phi(n)$.

For $n = \prod_{i=1}^{r} p_i^{a_i}$, p_i distinct prime factors
a_i are the exponents.
$a_i \geq 1$.

then

$$\phi(n) = \prod_{i=1}^{r} \left(p_i^{a_i - 1} (p_i - 1) \right)$$

we saw $\phi(100) = 40$

verify $\phi(100) = \phi(2^2 \cdot 5^2)$

$$= 2^1 (2-1) 5^1 (5-1)$$

$$= 40 \checkmark$$

$$\phi(500) = \phi(2^2 \cdot 5^3)$$

$$= 2^1 \cdot (2-1) \cdot 5^2 \cdot (5-1) = 200,$$ as we saw in Sage earlier

Approach of Th. 5.1 ~~we~~ bit by bit.

We've seen enough to say that for p prime.

$\phi(p) = p - 1$, this is an instance of the formula for the special case of $n = p$

Lemma 5.2 For a prime p and exponent $a \geq 1$

$$\boxed{\phi(p^a) = p^{a-1}(p-1).}$$

Proof: Consider all the integers.

$$1, 2, 3, \ldots\ldots, p^a - 1, p^a \quad (*)$$

$\phi(p^a)$ = number here that are coprime to p^a.

Let's count the ones that are not coprime to p^a.

Let $1 \leq x \leq p^a$ and consider

$$\gcd(x, p^a) \neq 1.$$

How does this happen? The factors of p^a are $1, p, p^2, p^3, \ldots, p^a$

$$\gcd(x, p^a) \neq 1 \iff p \mid x.$$

So in $(*)$ how many x are there that are multiples of p?

These are

$$p, 2p, 3p, 4p, \ldots\ldots, p^{a-1} \cdot p$$

This is a list of $\underline{p^{a-1}}$ integers.

So the number of x that are coprime to p^a must be.

$$\boxed{\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1)}$$

Next few lemmas will establish that ϕ is a multiplicative function. (in NT).

ie: $\boxed{\gcd(a,b)=1 \Rightarrow \phi(ab) = \phi(a)\phi(b)}$

without the gcd condition the property is called "completely multiplicative"

Assuming this for the moment. we can prove Th. 5.1.

Pf: Let $n = \prod_{i=1}^{r} p_i^{a_i}$

then $\boxed{\phi(n)} = \phi\left(\prod_{i=1}^{r} p_i^{a_i}\right)$

$$= \prod_{i=1}^{r} \phi\left(p_i^{a_i}\right)$$

, since ϕ is multiplicative and

$\gcd(p_i^{a_i}, p_j^{a_j}) = 1$ for $i \neq j$

i.e. $p_i \neq p_j$

$$\boxed{= \prod_{i=1}^{r} p_i^{a_i - 1} (p_i - 1)},$$ by lemma 5.2.

Tomorrow we'll prove ϕ is multiplicative.

Let's try some more examples.

eg. $n = 23456$.

$= 2^5 \cdot 733$

So $\phi(23456) = 2^4(2-1) \cdot 733^0 \cdot (733-1)$

$= 2^4 \cdot 732$