CONGRUENCES

Fix a natural number N.

Let a and b be two integers.

We say a is congruent to b modulo N if and only if a & b leave same remainder when divided by N.

We write it as $a \equiv b \pmod{N}$.

Example

$5 \equiv 2 \pmod{3}$

$4 \equiv 1 \pmod{3}$

$3 \equiv 0 \pmod{3}$

Discussion: How many remainders are there for a fixed N?

N remainders

$\{0, 1, 2, 3, \ldots, N-1\}$

Fix $N \geq 1$.

Define a relation on $\mathbb{Z}$ as follows.

$$a \sim b \iff a \equiv b \pmod{N}$$

1) Is $\sim$ reflexive?

2) Is $\sim$ symmetric?

3) Is $\sim$ transitive?

1) Yes, because $a \equiv a \pmod{N}$ for every integer a.

2) Yes, if $a \equiv b \pmod{N}$, then $b \equiv a \pmod{N}$

3) Yes, if $a \equiv b \pmod{N}$ & $b \equiv c \pmod{N}$ then $a \equiv c \pmod{N}$

$\sim$ is an equivalence relation and gives a partition of $\mathbb{Z}$

For example: when $n=2$

$$\mathbb{Z} = [0] \sqcup [1]$$

$[0]$: Even, $[1]$: odd

When $n=3$

$$\mathbb{Z} = [0] \sqcup [1] \sqcup [2]$$

$[0]$: Multiples of 3, $[1]$: $3k+1$, $[2]$: $3k+2$

In general for N

$$\mathbb{Z} = [0] \sqcup [1] \sqcup \cdots \sqcup [N-1]$$

Partition into N classes

Some arithmetic

$a_1 \equiv b_1 \pmod N$

$a_2 \equiv b_2 \pmod N$

Then $a_1 + a_2 \equiv b_1 + b_2 \pmod N$

$a_1 - a_2 \equiv b_1 - b_2 \pmod N$

$a_1 a_2 \equiv b_1 b_2 \pmod N$

Let's see a proof.

$a_1 \equiv b_1 \pmod N \iff N \mid a_1 - b_1$

$a_2 \equiv b_2 \pmod N \iff N \mid a_2 - b_2$

$N \mid (a_1 - b_1) + (a_2 - b_2)$

$\iff a_1 + a_2 \equiv b_1 + b_2 \pmod N$

Discuss multiplication, an example.

Diophantine Equations

1) Show that $x^4 + 16y^7 = 2011$ has no solutions in $\mathbb{Z}$.

2) Show that $x^3 + 700y = 140002$ has no solutions in $\mathbb{Z}$.

1) $x^4 + 16y^7 = 2011$

Mod 4, this becomes

$$x^4 \equiv 3 \pmod 4$$

↓

Only possibilities are $0, 1$

So no solution

2) $x^3 + 700y = 140002$

Modulo 7 this becomes

$$x^3 \equiv 2 \pmod 7$$

↓

Only possibilities are $0, 1, -1$ so no solutions.

Linear Congruences

We want to solve $ax \equiv b \pmod{m}$ for x in $\mathbb{Z}$.

Rewrite this as $ax - b = my$ for some $y \in \mathbb{Z}$

$$ax - my = b$$

when does this has a solution?

$ax \equiv b \pmod{m}$ has a solution

$\iff$ $\gcd(a, m)$ divides b.

Solve $23x \equiv 1 \pmod{50}$

$x = 37$

There are 2 ways to do this

1) Work out every possibility mod 50 and see which one fits

2) Use Euclidean algorithm & reduce mod 50.

Additive inverse

Fix N

We say b is additive inverse of a mod N if $ab \equiv 0 \pmod N$.

Multiplicative inverse

We say b is multiplicative inverse of a mod N if $ab \equiv 1 \pmod N$.

Existence of inverses

Discuss modulo primes & some examples of composite N.

Divisibility test for 3 & 9

$$a = a_0 + 10a_1 + 100a_2 + 1000a_3 + \cdots + 10^n a_n$$

$$\equiv a_0 + a_1 + a_2 + a_3 + \cdots + a_n \pmod 3$$

$$\equiv a_0 + a_1 + a_2 + \cdots + a_n \pmod 9$$

a is divisible by 3 or 9

$\iff$ Sum of its digits is divisible by 3 or 9.

Let p be a prime. We know that

$$ab \equiv 0 \pmod p \iff a \equiv 0 \pmod p \text{ or } b \equiv 0 \pmod p$$

Does this hold if we replace p by a Composite number ?

No, Example $4 \cdot 9 \equiv 0 \pmod{36}$

but $4 \not\equiv 0 \pmod{36}$

& $9 \not\equiv 0 \pmod{36}$

Suppose $a \not\equiv 0 \pmod p$.

Then $ax \equiv 1 \pmod p$ has a unique

Solution. (why?) (b/c $x \equiv \bar{a}^{-1} \pmod p$ exists b/c $\gcd(a,p) = 1$)

(Cancellation Property) If $a \not\equiv 0 \pmod p$, then

$$ax \equiv ay \pmod p$$
$$\iff x \equiv y \pmod p$$

In general if $\gcd(a,m) = 1$, then

$$ax \equiv ay \pmod m$$
$$\iff x \equiv y \pmod m$$

Qn: Which primes can be represented as sum of two squares?

Suppose $p = a^2 + b^2$, then what can we say about p?

$p = 2$ or $p \equiv 1 \pmod 4$

We will prove converse later!

Polynomials modulo p

A **Polynomial mod p** is an expression of the form

$$F(T) = a_0 + a_1 T + a_2 T^2 + \cdots + a_n T^n$$

a_i are integers mod p

One can add, subtract or multiply two Polynomials.

Degree (F) = Highest Power

Root of (F) is $a \iff F(a) \equiv 0 \pmod{p}$

Find roots of $3T^2 = 5 \pmod 7$

Method 1:

Try out every thing from 0 to 6.

Only roots are 2, 5

Method 2:

We pretend that we are solving this in $\mathbb{R}$.

$$3T^2 - 5 = 0 \iff T = \pm\sqrt{5/3}$$

Then try to make sense of this modulo 7.

$\frac{1}{3}$ is 5 (b/c $5 \cdot 3 \equiv 1 \pmod 7$))

$\sqrt{5/3}$ "=" $\sqrt{25} = 5$

So, $T = \pm 5$ or $2, 5$

Degree product formula

if Deg (F) = r

Deg (G) = s , then Deg (FG) = r+s.

Absolute value of a polynomial A $(A \neq 0)$

$$|A| = p^{\deg(A)}$$

$$|AB| = p^{\deg(AB)} = p^{\deg A + \deg B} = p^{\deg A}\, p^{\deg B} = |A|\,|B|$$

If $A = 0$, then $|A| = 0$

Lemma: Suppose A and B are polynomials, $B \neq 0$. Then $|A| \leq |AB|$

Equivalently, $\deg(A) \leq \deg(AB)$

Pf: $|B| = p^{\deg(B)} \geq 1$

$|A| \leq |AB|$

In $\mathbb{Z}/\mathbb{Z}[i]/\mathbb{Z}[\omega]$, we have

$$|x+y| \leq |x| + |y|.$$

For polynomials (mod p), we have

$$|A+B| \leq \max\{|A|, |B|\}$$

If A or B is 0, then

$$|A+B| = |A| \text{ or } |B| \leq \max\{|A|, |B|\}$$

If A & B are non-zero, then

$$\deg(A+B) \leq \max\{\deg(A), \deg(B)\}$$

$$|A+B) \leq \max\{|A|, |B|\}$$

(Stronger than triangle inequality)

Division in polynomials

(Will Discuss on Wednesday)

→ Start with an example

A, B polynomials mod p $\quad B \neq 0 \mod p$

$A = BQ + R \quad 0 \leq |R| < |B|$

Uniqueness

$$BQ_1 + R_1 \equiv Q_2 B + R_2 \pmod p$$

$$Q_1 \equiv Q_2 \pmod p$$

$$\Rightarrow R_1 \equiv R_2 \pmod p$$