ALGEBRA NOTE : MODULAR ARITHMETIC

JOHNEW ZHANG

1. Diophantine Equation

An equation with integer coefficients that one wants to solve over $\mathbb{Z}$, like $2x+3y=7$.

Observation $ax+by=c$ has a solution if and only if $gcd(a,b)|c$, and then if x_0, y_0 is one solution, all other solutions are the form:

$$x = x_0 + k\frac{b}{gcd(a,b)}k \in \mathbb{Z}$$
$$y = y_0 + k\frac{a}{gcd(a,b)}k \in \mathbb{Z}$$

2. Congruence

Definition 1. *Let $a, b \in \mathbb{Z}$ and $N \in \mathbb{N}$, we say that a and b are congruent modulo n if and only if $n|a-b$, write*

$$a \equiv b \pmod{n}$$

Properties if $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$.

Then $a_1 + b_1 \equiv a_2 + b_2 \pmod{n}$ and $a_1 b_1 \equiv a_2 b_2 \pmod{n}$.

Definition 2. *The congruence or residue class of $a \in \mathbb{Z}$ modulo n is the set $[a] = \{b \in \mathbb{Z} : a \equiv b \pmod{n}\}$.*

Definition 3. *The ring $\mathbb{Z}_n$ is the set of $\{[0], [1] \ldots [n-1]\}$ with the operation "+" and "$\cdot$" defined by $[a]+[b]=[c]$ if and only if $a+b \equiv c \pmod{n}$ and $[a][b]=[c]$ if and only if $ab \equiv c \pmod{n}$. The "zero" element will be $[0]$, and the "one" element is $[1]$.*

3. Group

Definition 4. *A group $\mathbb{G}$ is a set with a binary operation $*$,*

1) (associativity) $a*(b*c) = (a*b)*c$

2) (the existence of identity) : there exists an $e \in \mathbb{G}$ such that for all $a \in \mathbb{G}$, $a*e = e*a = a$.

3) (inverse) : there is an $a^{-1} \in \mathbb{G}$ such that $a*a^{-1} = e$

Definition 5. *A group $(\mathbb{G}, *, e)$ is commutative (or "Abelian") if for all a, $b\in \mathbb{G}$, $a*b = b*a$.*

Example :
S_N ={ permutations of $\{1, 2, 3 \ldots N\}$}.
A permutation of a set is a function from the set to itself which is:
(1) injective (one-to-one) $x = y \iff f(x) = f(y)$
(2) surjective (onto) for every $y \in \{1, 2, 3 \ldots N\}$ there is an x with $f(x) = y$.

In other words, a permutation of $\{1, 2, 3 \ldots N\}$ is a function,
$f : \{1, 2, 3 \ldots N\} \to \{1, 2, 3 \ldots N\}$ which is invertible.

4. The Ring $\mathbb{Z}_n$

Proposition : $\mathbb{Z}_n$ is a commutative ring, where $\mathbb{Z}_n$ is the set of congruence classes.

Lemma : Suppose that a, b and n are integers such that $gcd(a, b) = 1$. Then the equation

$$ax \equiv b \pmod{n}$$

has exactly one integer solution modulo n. In other words, $[a][x] = [b]$ has exactly one solution in $\mathbb{Z}_n$.

Proposition : $[a] \in \mathbb{Z}_n$ is a unit if and only if $gcd(a, n) = 1$.

Theorem : If p is a prime or 1, then $\mathbb{Z}_n$ is a field.

Proof. If N is a prime, then $gcd(a, N) = 1$ unless $N|a$
$\implies$ $[a]$ is a unit unless $[a] = [0]$.
If there is some $1 \leq a \leq N - 1$
Such that $[a]$ is not a unit.

the $gcd(a, N) \neq 1$ but $gcd(a, N) \leq a < N$.
so N is not prime. $\square$

5. Equivalence Relation

6. Chinese Remainder Theorem

CRT, V1 : If $gcd(N, M) = 1$, and $a, b \in \mathbb{Z}$
then we solve ($x \in \mathbb{Z}$):

$$x \equiv a \pmod N$$
$$x \equiv b \pmod M$$

is just the congruence class of x modulo MN :

$$x \equiv c \pmod{MN}$$

CRT, V2 : Let $M_1, \ldots, M_k$ be natural numbers with $gcd(M_i, M_j) = 1$ for all $i \neq j$. And Let $a_1, \ldots, a_k \in \mathbb{Z}$, Then there is a solution $x\mathbb{Z}$:

$$x \equiv a_1 \pmod{M_1}$$
$$\ldots$$
$$x \equiv a_k \pmod{M_k}$$

If x_0 is one solution, then x is another if and only if

$$x \equiv x_0 \pmod{M_1 \ldots M_k}$$

7. Congruence Equations

Question : How many solutions are there to $x^2 \equiv 1 \pmod N$?
Take $N = p$, p is a prime greater than 2.
$x^2 \equiv 1 \pmod p$
$\implies$ x$^2 - 1 \equiv 0 \pmod p$
$\implies$ (x-1)(x+1)$\equiv 0 \pmod p$
$\therefore, x \equiv \pm 1 \pmod p$ is two solutions.

Now consider $N = p^2$, p is a prime greater than 2 and $e \geq 1$, and if $x \in \mathbb{Z}$ satisfies $x^2 \equiv 1 \pmod{p^e}$
$\iff p^e | (x+1)(x-1)$
By unique factorization, write these two things :

$$x + 1 = cp^a$$
$$x - 1 = dp^b$$

$a + b \geq e$
if $a, b \neq 0$. then $p|(x-1), p|(x+1)$, so $p|(x+1) - (x-1) = 2$.
This is impossible, so $\min\{a, b\} = 0$.
Then we could know $b \geq e$ or $a \geq e$
$\therefore, x \equiv \pm 1 \pmod{p^e}$.
For odd prime, p, $e \geq$, $x^2 \equiv 1 \pmod{p^e}$ if and only if $x \equiv \pm 1 \pmod{p^e}$.

Consider $e \geq 1$, how many solutions to $x^2 \equiv 1 \pmod{2^e}$?
$e = 1 \implies x \equiv 1 \pmod 2$
$e = 2 \implies x \equiv \pm 1 \pmod 4$
$e \geq 3 :$ Suppose $x^2 \equiv 1 \pmod{2^e}$
Write

$$x + 1 = c2^a$$
$$x - 1 = d2^b$$

$a + b \geq e$
$\therefore 2^{min\{a,b\}} | (x+1) - (x-1) = 2$
so $\min\{a, b\} \leq 1$.
Case 1: $a = 0$ or $b = 0$
Then $x \equiv \pm 1 \pmod{2^e}$
Case 2 : $a = 1$, then $b \geq e - 1$
So $2^{e-1} | (x-1), x = 1 + 2^e k$.
If k is even, then $x \equiv 1 \pmod{2^e}$
If k is odd, then say $k = 2m + 1$.
Then $x \equiv 1 + 2^{e-1} \pmod{2^e}$
Case 3 : $b = 1$, then $x \equiv -1 + 2^{e-1} \pmod{2^e}$
Above all there are four solutions.

In conclusion, the number of solutions to $x^2 \equiv 1 \pmod{2^e}$ is one for $e = 1$, two for $e = 2$, four for $e \geq 3$.

Lemma If p is prime, $e \geq 1$, then $x^2 \equiv 1 \pmod{p^e}$ has exactly 2 solutions, except

$$p = 2, e = 1 \implies 1 solution$$
$$p = 2, e \geq 3 \implies 4 solutions$$

Theorem Let $N = 2^e p_1^{d_1} \dots p_k^{d_k}$, with p_i distinct odd primes. Then the number of solutions to $x^2 \equiv 1 \pmod N$ is exactly 2^k if $e = 0, 1$, 2^{k+1} if $e = 2$, 2^{k+2} if $e \geq 3$.

8. Fermat's Little Theorem

FLT : Let p be a prime, and $a \in \mathbb{Z}$ with $gcd(a, p) = 1$
then, $a^{p-1} \equiv 1 \pmod p$

Proof. It is easy using the idea of the permutation of a set, or the idea of function. □

9. Euler's Theorem

Definition 6. *Euler's totient function : for $m \geq 1$,*
$\varphi(m) =$ *number of values* $0 \leq k < m$ *such that* $gcd(k, m) = 1$
$=$ *number of units in the Ring* $\mathbb{Z}_n$.

Euler'sTheorem : Let $m \geq 1$ and a be an integers with $gcd(a, m) = 1$, then
$a^{\varphi m} \equiv 1 \pmod m$

Theorem : Suppose $gcd(n, m) = 1$, then $\varphi(nm) = \varphi(n)\varphi(m)$.

Lemma : If p is a prime, $e \geq 1$, then
$\varphi(p^e) = p^{e-1}(p - 1)$.