Lecture 4

Modular Arithmetic We give an example of a different, finite, number system.

$\mathbb{Z}_m := \{0, 1, 2, \ldots, m-1\}$.

$a +_b b := a+b \pmod m$ → take $a+b$ and divide by m, the remainder $\in \mathbb{Z}_m$ ($r = 0$ or $0 < r < m$)

This is $a+b \pmod m$ $\quad 0 \le r < m$

$a \cdot_b b := ab \pmod m$.

Def (Congruence). We say $a \equiv b \pmod m$ if $m \mid a-b$.
This is read a is congruent to b.

Remark: $a \equiv b \pmod m$ if and only if they both leave the same remainder when divided by m.

Properties

- $+$: associative, commutative, additive identity $= 0$,
- $\cdot$: associative, commutative, mult identity $= 1$

} All these are inherited from numbers.

Distributive

Examples

$m = 2$

$+$	0	1
0	0	1
1	1	0

– add inverse of 1 is 1

$\times$	0	1
0	0	0
1	0	1

– non zero elements have mult. inverse

Prop: Let $a, b \in \mathbb{N}$. Let

$S = \{ax+by \in \mathbb{N} \mid x, y \in \mathbb{Z}\}$ (integers).

Let d be the least element of S (it exists by WOP).
Then $d \mid s$ for all $s \in S$.

Proof: Let $s = ax+by$ for $x, y \in \mathbb{Z}$, $s \in S$.
Let $d = ax_0 + by_0$.
By division algorithm, there are q and r s.t.

$s = dq + r$, where $r = 0$ or $0 < r < d$.

If $r = 0$, then $d \mid s$ and there is nothing to prove.
So $r \neq 0$. Then

$r = s - dq$
$= ax+by - d(ax_0+by_0)$
$= a(x-dx_0) + b(y-dy_0)$
$= ax' + by' \in S$

$\to\leftarrow$ to d being least.
So r must be 0. □

Def (GCD) Let $a, b \in \mathbb{N}$. Then d is the greatest common divisor of a, b denoted (a,b), if (a) $d \mid a$ and $d \mid b$ (common divisor)
(b) if d' is a common divisor, then $d' \mid d$.

HCF, gcd(a,b) also used.

Remark: The d in above prop is (a,b).
by prop: $d \mid a$ and $d \mid b$ (common divisor).
If any other $d' \mid a$ and $d' \mid b$, then
$d' \mid ax_0+by_0 = d$.
So d is biggest.

Not very interesting is it?

$0 = F$, $1 = T$

$+$	F	T
F	F	T
T	T	F

model for exclusive OR

$\times$	F	T
F	F	F
T	F	T

model for AND

$n = 3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

mult inverse of 2 is 1
– all non-zero numbers have mult. inv.

inverse of a is $-a = m-a$

$n = 4$

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

additive inverses ✓

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

← 2 has no mult inv.
3 has.

Back to our question.
$ax - my = 1$.
must have $(a,m) = 1$ for a soln to exist.
When do all inverses exist? $(a,m) = 1$ for all $a = 1, 2, \ldots, m-1$
if $b \mid m$, then $(b,m) = b$ so b cannot be bigger than 1.

So ans:
m has to be such that it has no divisors in $\mathbb{Z}_m$ other than 1.

Def. (Prime) A number $p > 1$ is prime if it has no divisors other than 1 and p itself.

Example (How to list primes / Eratosthenes Sieve)

~~1~~ 2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~
11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

Ex. list all primes ≤ 100.

Prop. Let $a, b \in \mathbb{Z}$ and let a', b' be such that $a \equiv a' \pmod m$, $b \equiv b' \pmod m$. Then
(1) $a+b \equiv a'+b' \pmod m$
(2) $ab \equiv a'b' \pmod m$

Proof: ex.

Prop: The relation $\equiv \pmod m$ is an equivalence relation.
Let $[k] := \{n \in \mathbb{Z} \mid n \equiv k \pmod m\}$ (called the equivalence class corresponding to k, for $k = 0, 1, \ldots, m-1$. Then
(1) The equivalence classes are disjoint
(2) Their union is $\mathbb{Z}$.
(1) and (2) is expressed as: The equivalence classes partition $\mathbb{Z}$.

$n = 5$ ← Class activity.

	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$1^{-1} = 1$
$2^{-1} = 3$
$3^{-1} = 2$
$4^{-1} = 4$
} – all have inverses.

Def: A field $\mathbb{F}$ is a set F with operations $+$ and $\times$ s.t.

$+$	$\cdot$
– associative	– associative
– comm	– commutative
– 0	– unity 1
– add inverse	– non-zero have inv.

$\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$ are fields, $\mathbb{Z}_4$ is not.
Mult inv: can solve equations like $ax = b$.

Problem: – When are $\mathbb{Z}_m$ fields?
Boils down to saying can we solve eqn

$ax = 1 \pmod m$
or $m \mid ax - 1$ or
or there is y s.t. $ax - 1 = my$
or $ax - my = 1$.

Ex. $0 \cdot a = 0$ in a field

– Why are $+, \cdot$ well defined? ✓ if $a \equiv a' \pmod m$, $b = b' \pmod m$
Is $a+b \equiv a'+b'$ and $ab \equiv a'b' \pmod m$?

Proof: $a \equiv a$ ✓, $a \equiv b \Rightarrow b \equiv a$ ✓
$a \equiv b$, $b \equiv c \Rightarrow a \equiv c$ (Ex)

What is $[k]$? $[k] = \{k, k \pm m, k \pm 2m, \ldots\}$

Clearly $[k] \cap [l] = \emptyset$ unless $k \equiv l \pmod m$
– $\bigcup_{k=1}^{m} [k] = \mathbb{Z}$. → also clear. □

Remark: We can 'think of' $\mathbb{Z}_m$ as $\{[0], [1], [2], \ldots, [m-1]\}$
Here, $0, 1, 2, \ldots, m-1$ are called the representatives of eq. class.
Can define $[k] + [l] := [k+l]$
$[kl] := [kl]$, etc.

Thm: $\mathbb{Z}_m$ is a field if and only if m is a prime.

Proof: ($\Leftarrow$) Let $m = p$, a prime. We first show $\mathbb{Z}_p$ is a field.

$+$	$\cdot$
associative ✓	Associative ✓
Commutative ✓	Commutative ✓
Additive identity: 0 ✓	Mult. identity: 1 ✓
Additive inverse $a + (p-a) = p \equiv 0 \pmod p$ ✓	Mult. inverse ✓ – let $a \neq 0$. by prop there is x, s.t. $ax \equiv 1 \pmod p$, $x = a^{-1}$.

Distributive law ✓

Proof ($\Rightarrow$) Let $\mathbb{Z}_p$ be a field, p not prime. So $p = a \cdot b$, for $a, b < p$.
$\Rightarrow$ $ab \cdot b^{-1} \equiv 0 \pmod p$ (since b^{-1} exists)
$\Rightarrow$ $a \equiv 0 \pmod p$ $\to\leftarrow$. □