Math 322, lecture 3, 14/9/2017

Last time

(1) gcd (2) congruence mod n

(3) $\mathbb{Z}/n\mathbb{Z}$, addition, multiplication

specifically $(\mathbb{Z}/n\mathbb{Z}, +)$ has associative, commutative law + has $[0]_n$, negatives $-[a]_n = [-a]_n$

$\Rightarrow$ "additive group mod n".

map $f: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ respects +, i.e. "map of groups".

$f(a) = [a]_n$

Today: - Multiplicative group

- multiplication tables
- isomorphism

Def: $(\mathbb{Z}/n\mathbb{Z})^\times \overset{\text{def}}{=} \{a \in \mathbb{Z}/n\mathbb{Z} \mid \exists b \in \mathbb{Z}/n\mathbb{Z} : ab = [1]_n\}$

note: $[0]$ never there.

PS1: $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ iff $\gcd(a,n) = 1$

Lemma: $(\mathbb{Z}/n\mathbb{Z})^\times$ closed under multiplication, inverses

Pf: say $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, with $a a' = [1]$, $b \cdot b' = [1]$

Then $(ab)\cdot(a'b') = (aa')(bb') = [1]\cdot[1] = [1]$ so $ab \in (\mathbb{Z}/n\mathbb{Z})^\times$

mult in $\mathbb{Z}/n\mathbb{Z}$ is commutative, associative

Also $a' a = a \cdot a' = [1]$ so $a' \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Conclusion: $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ has associative, commutative law has $[1]$, has inverses

Examples: (0) $(\mathbb{Z}/1\mathbb{Z}, +)$:

+	0
0	0

(1) $(\mathbb{Z}/2\mathbb{Z}, +)$

+	0	1
0	0	1
1	1	0

(2) $(\mathbb{Z}/3\mathbb{Z}, +)$

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

(2) $(\mathbb{Z}/3\mathbb{Z})^\times$

$\cdot$	1	2
1	1	2
2	2	1

, $(\mathbb{Z}/4\mathbb{Z})^\times$

$\cdot$	1	3
1	1	3
3	3	1

Observe: have bijections between $(\mathbb{Z}/2\mathbb{Z}, +)$, $(\mathbb{Z}/3\mathbb{Z})^\times$, $(\mathbb{Z}/4\mathbb{Z})^\times$ respect operations

Say these structures are isomorphic.

(a map that respects operations is called a homomorphism)

(3) $(\mathbb{Z}/4\mathbb{Z}, +)$

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

$((\mathbb{Z}/5\mathbb{Z})^\times, \cdot)$

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

CHW: map $i \to [2]^i$ is isomorphism $(\mathbb{Z}/12\mathbb{Z}, +) \to (\mathbb{Z}/13\mathbb{Z})^\times$.

General: if p is prime, $(\mathbb{Z}/p\mathbb{Z})^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z}, +)$

bijection $(\mathbb{Z}/4\mathbb{Z}, +)$, $(\mathbb{Z}/5\mathbb{Z})^\times$ is

0	1
1	2
2	4
3	3

(Check!)

$(\mathbb{Z}/8\mathbb{Z})^\times$:

$\cdot$	1	3	5	7
1	1			
3		1		
5			1	
7				1

__not__ isomorphic to $(\mathbb{Z}/4\mathbb{Z},+)$

__reason:__ in $(\mathbb{Z}/8\mathbb{Z})^\times$ we have $x^2=1$ for all x

in $(\mathbb{Z}/4\mathbb{Z},+)$ we have $[1]+[1]=[2]\neq 0$

__Terminology:__ $(\mathbb{Z}/n\mathbb{Z},+)$ is also called the "cyclic group of order n"

$(\mathbb{Z}/8\mathbb{Z})^\times$ is called the "four-group".

__Def:__ Call $p\in\mathbb{Z}_{\geq 2}$ __prime__ if it has no divisors other than 1 and itself.

__Note:__ p is prime iff $(\mathbb{Z}/p\mathbb{Z})^\times=\{[1],[2],\dots,[p-1]\}$

__Cor:__ $p\mid ab$ iff $p\mid a$ or $p\mid b$ $\quad$ (if $x,y\in\mathbb{Z}/p\mathbb{Z}$ are non-zero so is xy)

__Thm:__ Every non-zero integer has a unique representation in the form $\quad \varepsilon\prod_{p\text{ prime}}p^{e_p}$ where $\varepsilon\in\{\pm 1\}$, $e_p\in\mathbb{Z}_{\geq 0}$, almost all zero

---

__The Chinese Remainder theorem__

Example of a homomorphism:

let $n_1 | N$ be positive (e.g. $2|6$)

Then consider map $\mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z}$ e.g. $\begin{matrix}0\\1\\2\\3\\4\\5\end{matrix} \mapsto \begin{matrix}0\\1\\0\\1\\0\\1\end{matrix}$

$[a]_N \to [a]_{n_1}$

well defined: if $a \equiv a' \ (N)$

then $N | a-a'$ so $n_1 | a-a'$

and $a \equiv a' \ (n_1)$

also surjective (every residue is possible)

respects both $+, \cdot$ (both defined via representatives)

Now suppose both $n_1, n_2 | N$, consider map

$$[a]_N \mapsto ([a]_{n_1}, [a]_{n_2})$$

Still respects $+, \cdot$ (defined component-wise)

<u>Def:</u> Call n_1, n_2 <u>relatively prime</u> if $\gcd(n_1, n_2) = 1$

<u>Thm:</u> let $N = n_1 n_2$ with $\gcd(n_1, n_2) = 1$. Then the map above $f: \mathbb{Z}/N\mathbb{Z} \to (\mathbb{Z}/n_1\mathbb{Z}) \times (\mathbb{Z}/n_2\mathbb{Z})$ is a bijection respecting $+, \cdot$

<u>Corollary:</u> $(\mathbb{Z}/N\mathbb{Z}, +) \cong (\mathbb{Z}/n_1\mathbb{Z}, +) \times (\mathbb{Z}/n_2\mathbb{Z}, +)$

<u>Pf:</u> By Bezout's thm we have $x, y \in \mathbb{Z}$ s.t. $n_1 x + n_2 y = 1$

Then $\begin{cases} n_1 x \equiv 0 & (n_1) \\ n_1 x \equiv 1 & (n_2) \end{cases}$, $\begin{cases} n_2 y \equiv 1 & (n_1) \\ n_2 y \equiv 0 & (n_2) \end{cases}$

It follows that image of f contains $([0]_{n_1},[1]_{n_2})$ and $([1]_{n_1},[0]_{n_2})$

by closure under addition (and f respecting it) f is surjective

On $([a]_{n_1},[b]_{n_2}) = ([a],[a])\cdot([1],[0]) + ([b],[b])\cdot([0],[1])$

$([a],[b]) = f([a]_N\cdot[n_2 y]_N + [b]_N\cdot[n_1 x])$

Both sets $\mathbb{Z}/N\mathbb{Z}$, $(\mathbb{Z}/n_1\mathbb{Z})\times(\mathbb{Z}/n_2\mathbb{Z})$ have cardinality $N=n_1 n_2$

by the pigeon-hole principle, f is injective as well.