8/16/17

$\mathbb{Z}$ = set of integers.

$(\mathbb{Z}, +, \cdot)$

$(\mathbb{Z}, +)$ group (abelian)

(1) $m, n \in \mathbb{Z}$, $m+n \in \mathbb{Z}$

(2) $m, n, k \in \mathbb{Z}$, $(m+n)+k = m+(n+k)$

(3) $0 \in \mathbb{Z}$, $m+0 = m$ for all $m \in \mathbb{Z}$

(4) $m \in \mathbb{Z}$, $-m \in \mathbb{Z}$ s.t. $m+(-m) = 0$

(5) $m+n = n+m$ for all $m, n \in \mathbb{Z}$

(6) $m, n \in \mathbb{Z}$, $m \cdot n \in \mathbb{Z}$

(7) $(m \cdot n) \cdot k = m \cdot (n \cdot k)$, $m, n, k \in \mathbb{Z}$

(8) $1 \in \mathbb{Z}$, $m \cdot 1 = m$, $m \in \mathbb{Z}$

(9) $m \cdot (n+k) = (m \cdot n) + (m \cdot k)$

(10) $(n+k) \cdot m = (n \cdot m) + (k \cdot m)$

$\Rightarrow (\mathbb{Z}, +, \cdot)$ ring.

(11) $m \cdot n = n \cdot m$ (commutative)

- $\mathbb{Z}$ is an ordered set

(i.e. $\forall$ $m, n \in \mathbb{Z}$, $m \geq n$ or $m < n$.)

($\forall$ = for all)

Well Ordering Principle (WOP):

Every nonempty set S of positive integers has a smallest member.

Division Algorithm:
$a, b \in \mathbb{Z}$, $b > 0$. $\exists$ unique integers $q, r \in \mathbb{Z}$, $0 \leq r < b$ such that

$$a = bq + r.$$

Pf: Existence:

$$S = \{a - bk \mid k \in \mathbb{Z},\ a - bk \geq 0\}$$

nonempty.
Suppose $0 \in S$. Then $\exists\ q \in \mathbb{Z}$ s.t.

$$a - bq = 0 \Rightarrow a = bq + \underbrace{0}_{r}$$

Assume $0 \notin S$. Then S is a nonempty set of positive integers. Hence by WOP $\exists\ r \in S$ which is smallest.
$\Rightarrow \exists\ q \in \mathbb{Z}$ s.t. $a - bq = r \Rightarrow a = bq + r$.
Need to show $r < b$.
Suppose $r \geq b$. Then

$$\underbrace{a - bq - b}_{a - b(q+1)} = r - b \geq 0$$

$\Rightarrow r - b \in S$
This is a contradiction since $r - b < r$.
$\Rightarrow r < b$.

Uniqueness: Suppose

$$a = bq + r, \quad 0 \le r < b$$
$$a = bq' + r', \quad 0 \le r' < b$$

Without loss of generality, assume $r' \ge r$.

We have

$$bq + r = bq' + r'$$

$$\Rightarrow \quad b(q - q') = r' - r \ge 0$$

$$\Rightarrow b \mid (r' - r)$$

$r' - r \le r' < b$ which is a contradiction if $r' - r > 0$.

$$\Rightarrow r' - r = 0 \Rightarrow r' = r \Rightarrow bq = bq'$$
$$\Rightarrow q' = q. \qquad //$$

8/18

$a, b \in \mathbb{Z}_{\neq 0}$

Greatest Common Divisor (gcd):
$\gcd(a,b) = d$ if

(1) $d > 0$
(2) $d \mid a$, $d \mid b$
(3) $c \mid a$, $c \mid b \Rightarrow c \mid d$.

Least common Multiple (lcm):
$\operatorname{lcm}(a,b) = \kappa$ if
(1) $\kappa > 0$
(2) $a \mid \kappa$, $b \mid \kappa$
(3) $a \mid m$, $b \mid m \Rightarrow \kappa \mid m$.

Fact: $\gcd(a,b)\operatorname{lcm}(a,b) = ab$
for $a, b \in \mathbb{Z}_{>0}$

Thm: $a, b \in \mathbb{Z}_{\neq 0}$, $d = \gcd(a,b)$.
Then $\exists\ s, t \in \mathbb{Z}$ such that
$d = as + bt$.

Pf (idea)
- $S = \{am+bn \mid m, n \in \mathbb{Z},\ am+bn > 0\} \neq \phi$
- By WOP $\exists$ a smallest member $d \in S$.
- $d = \gcd(a,b)$.

Example! $a = 6,\ b = 4$

$\gcd(6,4) = 2$

$2 = 6(1) + 4(-1)$

$= 6(-1) + 4(2)$

($\Rightarrow$ s, t in the Thm are not unique.)

Thm: $a, b \in \mathbb{Z}_{\neq 0}$, $b > 0$. By Divison Algorithm $a = bq + r$, $0 \leq r < b$.

$\Rightarrow \gcd(a,b) = \gcd(b,r)$.

Pf: $d = \gcd(a,b) = as + bt$, $s, t \in \mathbb{Z}$

$= (bq + r)s + bt$

$= b(qs + t) + r(s)$

$\Rightarrow d = \gcd(b,r)$.

Example! $a = 236$, $b = 42$

$\gcd(236, 42)$ $\qquad 236 = 42(5) + 26$

$= \gcd(42, 26)$ $\qquad 42 = 26(1) + 16$

$= \gcd(26, 16) = 2$

$2 = 26(-3) + 16(5) = 26(-3) + (42 + 26(-1))(5)$

$= 42(5) + 26(-8) = 42(5) + (236 + 42(-5))(-8)$

$= 236(-8) + 42(45)$.

Defn: $a \in \mathbb{Z}_{>1}$ is prime if
$d \mid a \Rightarrow d = 1$ or a.

Euclid Lemma: $a, b \in \mathbb{Z}$, p prime
Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.
Pf: Suppose $p \mid ab$ & $p \nmid a$.

$\Rightarrow \gcd(p, a) = 1$

$\Rightarrow 1 = ps + at$, $s, t \in \mathbb{Z}$

$\Rightarrow b = p(bs) + (ab)t$

$p \mid p(bs)$, $p \mid (ab)t$ since $p \mid ab$.

$\Rightarrow p \mid p(bs) + (ab)t = b$ //

Example: $6 \mid (4)(3)$ but $6 \nmid 4$ or $6 \nmid 3$.

Fundamental Theorem of arithmetic:
Any $n \in \mathbb{Z}_{>1}$ is either prime or
$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, $p_1, p_2, \cdots, p_k$ prime
$a_1, a_2, \cdots, a_k \in \mathbb{Z}_{\geq 1}$, $p_1 < p_2 < \cdots < p_k$.
(This factorization is unique.)

Example: $n = 12$, $m = 15$

$12 = (2^2)(3)$, $15 = (3)(5)$

$\gcd(12, 15) = 3$

$\text{lcm}(12, 15) = (12)(5) = 60$

$\gcd(12, 15)\,\text{lcm}(12, 15)$

$= (3)(60) = (12)(15)$

HW, page 23 # 1, 2, 4, 6, 8, 12, 19

08/21

P24 #12

$$(7)(5n+3)+(-5)(7n+4)=1$$

$\Rightarrow \gcd(5n+3, 7n+4)=1$ for all n.

Principle of Mathematical Induction (PMI):

Let S be a nonempty set of integers containing 'a'. Suppose S has the property that if $k \in S$, then $k+1 \in S$. Then S contains all integers $n \geq a$.

Example: Use PMI and show that $3 \mid (2^{2n}-1)$ for all $n \in \mathbb{Z}$.

Take $S = \{a \in \mathbb{Z} \mid 3 \mid (2^{2a}-1)\}$

$0 \in S$ since $3 \mid (2^{2(0)}-1)$

Suppose $k \in S \Rightarrow 3 \mid (2^{2k}-1)$

$$2^{2(k+1)}-1 = 2^{2k}\cdot 2^2 - 1$$
$$= 2^2(2^{2k}-1)+(2^2-1)$$

$3 \mid (2^{2k}-1) \Rightarrow 3 \mid 2^2(2^{2k}-1)$, $3 \mid (2^2-1)$

$\Rightarrow 3 \mid 2^2(2^{2k}-1)+(2^2-1) = 2^{2(k+1)}-1$

$\Rightarrow k+1 \in S$. $\Rightarrow$ By PMI, $n \in S$ for all $n \geq 0$.

$\Rightarrow 3 \mid (2^{2n} - 1)$ for all $n \geq 0$.

Suppose $n \in \mathbb{Z}_{<0}$

$\Rightarrow n = -m$, $m \in \mathbb{Z}_{>0}$

$\Rightarrow 3 \mid (2^{2m} - 1) \Rightarrow 3 \mid (2^{2(-n)} - 1)$

$2^{2(-n)} - 1 = 2^{-2n} - 1 = 2^{-2n}(1 - 2^{2n})$

$= -2^{-2n}(2^{2n} - 1)$

$3 \mid -2^{-2n}(2^{2n} - 1) \Rightarrow 3 \mid (2^{2n} - 1)$ since $3 \nmid -2^{-2n}$.

Equivalence Relation:

S nonempty set. A relation $\sim$ on S is an equivalence relation if

(1) $a \sim a$ for all $a \in S$ (reflexive)

(2) $a, b \in S$ and $a \sim b \Rightarrow b \sim a$ (symmetry)

(3) $a, b, c \in S$, and $a \sim b$, $b \sim c$ $\Rightarrow a \sim c$. (transitive)

For $a \in S$, the subset

$\{x \in S \mid a \sim x\} = [a]$

is called the equivalence class of a.

Thm: For $a, b \in S$,

$$[a] \cap [b] = \phi \text{ or } [a] = [b]$$

$\Rightarrow S = [a_1] \cup [a_2] \cup \cdots \cup [a_k]$ (distinct) partition of equivalence classes.

Example: $a, b \in \mathbb{Z}$, $a \sim b$ if $3 \mid (a-b)$

- $a \sim a$ since $3 \mid (a-a)$
- ~~$a \sim b \Rightarrow b \sim a$~~
- $a \sim b \Rightarrow 3 \mid (a-b) \Rightarrow 3 \mid -(a-b) = b-a$
  $\Rightarrow b \sim a$
- $a \sim b$ & $b \sim c \Rightarrow 3 \mid (a-b)$ & $3 \mid (b-c)$
  $\Rightarrow 3 \mid (a-b)+(b-c) = a-c \Rightarrow a \sim c$

$\therefore \sim$ is an equivalence relation on $\mathbb{Z}$.

$[0] = \{x \in \mathbb{Z} \mid 3 \mid (x-0)\}$
$= \{0, \pm 3, \pm 6, \cdots\}$

$[1] = \{\cdots, -5, -2, 1, 4, 7, 10, \cdots\}$

$[2] = \{\cdots, -4, -1, 2, 5, 8, 11, \cdots\}$