17/1/23 # 1 Integers

Ring is a set with 2 operations, $\times$, $+$, satisfying some axioms

Good Example: $\mathbb{Z} = \{0, \pm1, \pm2, \pm3, \dots\}$ integers under $+, \times$.

Definition 1.1: Let $a, b \in \mathbb{Z}$, $b \neq 0$. We say b divides a (we write $b|a$) if $a = bc$ for some $c \in \mathbb{Z}$.

Example: $7 | (-21)$ as $-21 = 7 \times (-3)$

$7 \nmid 20$

$b | 0 \quad \forall b \neq 0$ as $0 = b \times 0$

division by 0, not defined ($\frac{1}{0} = x \iff 1 = \underset{0}{\underset{\shortparallel}{x \times 0}}$ $\lightning$)

Definition 1.2: An integer $p > 1$ is prime if $a | p$ (with $a \in \mathbb{Z}$) $\Rightarrow a = \pm 1$ or $a = \pm p$.

The first few primes are: 2, 3, 5, 7, 11, 13, 17, ...

Euclid: $\exists$ infinitely many primes.

Definition 1.3 (GCD): Let $a, b \in \mathbb{Z} \setminus \{0\}$. We say that a positive integer d is the greatest common divisor (we write $\gcd(a,b) = d$) if:

(1) $d | a$ and $d | b$

(2) If $s | a$ and $s | b$ then $s | d$.

If $\gcd(a,b) = 1$ then a and b are coprime (or relatively prime).

Example: $\gcd(8, 12) = 4$

$\gcd(-6, 8) = 2$

$\gcd(4, 5) = 1$ so 4 and 5 are coprime

Definition 1.4 (LCM): Let $a, b \in \mathbb{Z} \setminus \{0\}$. We say that a positive integer c is the least common multiple of a and b (we write $\operatorname{lcm}(a,b) = c$) if:

(1) $a | c$ and $b | c$;

(2) If $s \in \mathbb{Z}$ s.t. $a | s$ and $b | s$ then $c | s$

Example: $\text{lcm}(8,12)=24$

$\text{lcm}(-8,12)=24$

$\text{lcm}(-8,-12)=24$

Fact: $\gcd(a,b)\cdot \text{lcm}(a,b)=|ab|$

<u>Proposition 1.5 (Euclidean Division):</u> If $b\in\mathbb{Z}$, $b>0$ then for any $a\in\mathbb{Z}$ $\exists$ unique pair $q,r\in\mathbb{Z}$ s.t.

(1) $a=qb+r$ (q <u>quotient</u>, r <u>remainder</u>)

(2) $0\leq r<b$

Example: (1) $a=20, b=13 \Rightarrow 20=1\times 13+7$ $(q=1, r=7)$

(2) $a=-20, b=13 \Rightarrow -20=(-1)\times 13-7$

$-20=(-2)\times 13+6$ $(q=-2, r=6)$

<u>Eclidean Algorithm (to find $\gcd(a,b)$):</u>

$a=q_0 b+r_0 \quad b>r_0$

$b=q_1 r_0+r_1 \quad r_0>r_1$

$r_0=q_2 r_1+r_2 \quad r_1>r_2$

$\vdots$

$r_{n-2}=q_n r_{n-1}+r_n$

$r_{n-1}=q_{n+1} r_2+\underline{0}$

claim $\gcd(a,b)=r_n$

ex: $a=83 \quad b=13$

$83=6\times 13+5$
$13=2\times 5+3$
$5=1\times 3+2$
$3=1\times 2+1$
$2=2\times 1+0$

$\gcd(83,13)=1$, so 83 and 13 are coprime

<u>Lemma 1.7 (Bezout's Identity):</u> If a,b are positive integers and $\gcd(a,b)=d$ then $\exists\, x,y\in\mathbb{Z}$ s.t.

$ax+by=d$

Proof: Using Euclidean Alg, since $d=r_n$, we get $d=r_n=r_{n-2}-q_n r_{n-1}=r_{n-2}-q_n(r_{n-3}-q_{n-1}r_{n-2})$

$=*\cdot r_{n-2}-*\cdot r_{n-3}=\cdots=ax+by$

Example 1.8: Find $x, y \in \mathbb{Z}$ s.t. $343x + 280y = 7$ where $7 = \gcd(343, 280)$

$$343 = 1 \times 280 + 63$$

$$280 = 4 \times 63 + 28$$

$$63 = 2 \times 28 + 7 = d$$

$$28 = 4 \times 7 + 0$$

now $7 = 63 - 2 \times 28$

$$= 63 - 2 \times (280 - 4 \times 63)$$

$$= 9 \times 63 - 2 \times 280$$

$$= 9 \times (343 - 1 \times 280) - 2 \times 280$$

$$= 9 \times 343 + (-11) \times 280$$ so $x = 9$, $y = -11$

<u>Corollary 1.9:</u> a and b are coprime $\iff ax + by = 1$ for some $x, y \in \mathbb{Z}$.