Ch 0 - Preliminaries

1. Properties of integers

<u>well ordering principle</u>:

$\mathbb{Z}_+$ - positive integers

$S \subseteq \mathbb{Z}_+$ non-empty $\Rightarrow$ S has a smallest element

Note: not true for $\mathbb{Z}$

$\mathbb{Z}_+$ doesn't have largest element.

<u>Theorem</u>: division w/ remainder

$a, b \in \mathbb{Z}$ $b > 0$

$\Rightarrow$ $\exists!$ $q, r \in \mathbb{Z}$ such that

$a = b \cdot q + r$ and $0 \leq r < b$

Notation:

r - remainder
rem(a, b)

q - quotient
quo(a, b)

Example 1. $a = 218$ $b = 40$

2. Driver's Licence in Florida

Last 3 digits

Males $40(m-1) + b$

Females $40(m-1) + b + 500$

where m - birth month b - birth day

6/16 $\rightarrow$ $200 + 16 + 500 = 716$

Determine the birthdays & gender

(a) 218 (b) 953

Find range for males & females

$1 \leq$ man's number ≤ 471

$501 \leq$ woman ≤ 971

(a) 6/18

(b) 12/13

Proof of Theorem

Given $a \mid b \in \mathbb{Z}$ $\quad b > 0$

Let $S = \{ a - bk : k \in \mathbb{Z} \ \& \ a - bk \geq 0 \}$

if $0 \in S \Rightarrow$ a is a multiple of b

$$b \mid a$$

$\Rightarrow r \overset{def}{=} 0 \quad q := k \quad s.t \quad a - bk = 0$

$\Rightarrow a = b \cdot q + 0 \quad 0 \leq 0 = r < b$

if $0 \notin S$

S is non-empty

b/c if $a > 0 \Rightarrow a - 0b = a \in S$

if $a < 0 \quad a - (2a) \cdot b = \underset{\uparrow 0}{a}(1 - \underset{\uparrow 0}{2b}) > 0$

if $a = 0$ but $0 \notin S$ #. ↯

Proof cont.

$\Rightarrow \quad S \subseteq \mathbb{Z}_+$ non-emphy

WOP $\Rightarrow$ S has a smallest element

$r := \min S$ $\quad q = k$ s.t. ~~$a = bk + r$~~ $\quad r = a - bk$

Claim $\quad a = bq + r$ ✓ $\quad 0 \le r < b$

$0 \le r$ b/c $r \in S$

if $r \ge b$ than $0 \le r - b = a - b(k+1) \in S$

$r - b < r \Rightarrow$ ↯ of $r = \min S$

Uniqueness:

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

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

$\Rightarrow b(q - q') = r' - r$

$\Rightarrow b \mid r' - r$ and $r' - r \le r' < b \Rightarrow r' - r = 0$, $q' - q = 0$.

Greatest Common divisor

Def: $a, b \in \mathbb{Z}$ non-zero

$d = \gcd(a,b) \iff d \mid a \quad d \mid b$

and if $d' \mid a \quad d' \mid b \Rightarrow d' \mid d$

a, b are relatively prime if $\gcd(a,b) = 1$

2 ways to compute gcd:

① Euclid's Algorithm

Example: Find $\gcd(126, 38)$

$$126 = 38 \cdot \underline{3} + \underline{12}$$
$$38 = 12 \ \underline{3} + \underline{2}$$
$$12 = 2 \ \underline{6} + \underline{0}$$

$\gcd(126, 38) = 2$

Theorem: $\gcd(126, 38)$ is the last remainder before getting

In general $r_0 = a$ $r_1 = b$

$r_0 = r_1 \cdot q_1 + r_2$ $\quad r_2 = \text{rem}(r_0, r_1)$

$r_1 = r_2 \cdot q_2 + r_3$ $\quad r_3 = \text{rem}(r_1, r_2)$

$\vdots$

$r_\ell = \text{rem}(r_{\ell-2}, r_{\ell-1})$

$\gcd(a,b) = r_{\ell-1}$ if ℓ is the first time $r_\ell = 0$.

---

② method : via prime decomposition

Fundamental Theorem of Arithmetic:

$n \in \mathbb{Z}$ $n \geq 2$ $\Rightarrow$ n is a prime number or n is a product of finitely many primes. This product is unique (up ordering of primes)

$$a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$$

$$b = p_1^{\beta_1} \cdots p_r^{\beta_r}$$

$$\begin{matrix}\alpha_1 \dots \alpha_r \\ \beta_1 \dots \beta_r\end{matrix} \in \mathbb{Z}_{\geq 0}$$

$$\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_r^{\min(\alpha_r,\beta_r)}$$

Find $\gcd(126, 38)$

$126 = 2 \cdot 3^2 \cdot 7$

$38 = 2 \cdot [redacted] \cdot 19$

$\gcd = 2^1 \; 3^0 \; 7^0 \; 19^0 = 2$

Theorem GCD is a linear combination

$a, b \in \mathbb{Z}$ non-zero

$\Rightarrow \exists\ s, t \in \mathbb{Z}$ $as + bt = \gcd(a, b)$ (see proof in book)

Example:

$\gcd(126, 38) = 2$

Find s, t $126 \cdot s + 38 \cdot t = 2$

$126 = 38 \cdot 3 + 12 \rightarrow 12 = 126 - 3 \cdot 38$

$38 = 12 \cdot 3 + 2$

$2 = 38 - 3 \cdot 12$

$2 = 38 - 3(126 - 3 \cdot 38)$

$= \underline{-3}\ 126 + \underline{10}\ 38$

Theorem Euclid's Lemma

if p is a prime and $p \mid a \cdot b$

$\Rightarrow$ $p \mid a$ or $p \mid b$

Proof:

Assume $p \mid a \cdot b$ $\quad p$ prime $\quad \gcd(a, p) = \begin{cases} 1 \\ p \end{cases}$

$\gcd(a, p) = p \Rightarrow p \mid a$ ✓

$\gcd(a, p) = 1$

$1 = sa + tp$

$b = sab + btp$

$p \mid sab$ $\quad p \mid btp$

$\Rightarrow p \mid b$ ✓