

①

(§2.2) The Division Algorithm.

Thm 2.9) Let a, b be integers, $b > 0$.

Then $\exists!$ integers $q \& r$ s.t. $a = bq + r$, $0 \leq r < b$.

Proof : ③ (existence of $q \& r$)

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

① If $0 \in S \Rightarrow b$ divides a ($\exists k$ s.t. $a = bk$) \Rightarrow if we let $q = \frac{a}{b}$ ($b > 0$) and $r = 0 \Rightarrow a = b \cdot \frac{a}{b} + 0$.

② If $0 \notin S \Rightarrow$ let us use WOP. Show $S \neq \emptyset$:

If $a > 0 \Rightarrow \overbrace{a - b \cdot 0}^{=a \geq 0} \in S$ ($k=0$)

$a < 0 \Rightarrow a - b(\underbrace{\lfloor \frac{a}{b} \rfloor}_{\leq 0}) = \underbrace{a}_{< 0} (\underbrace{1 - \lfloor \frac{a}{b} \rfloor}_{\geq 0}) \in S$ ($k=\lfloor \frac{a}{b} \rfloor$)

($a \neq 0$ since if $a = 0$, $S = \{-bk : k \in \mathbb{Z}, k \leq 0\} \ni 0$ when $k=0$), but $0 \notin S$)

By WOP, S has a smallest element, since $S \subset \mathbb{N}$.
Say, $r = a - bq > 0$, for some $q \in \mathbb{Z}$. Then

$a = bq + r$, $r > 0$. Show $r < b$. If $r > b \Rightarrow$

$a - b(q+1) = \underbrace{a - bq}_{r} - b = r - b > 0 \Rightarrow a - b(q+1) \in S$,

but since $a - b(q+1) = a - bq - b < a - bq \Rightarrow a - b(q+1)$ is the smallest element of S , so it's not possible. Thus, $r \leq b$. Since $0 \notin S \Rightarrow r \neq b$

(otherwise, $r = b = a - bq \Rightarrow a = b(q+1)$, i.e. for $k=q+1$, $a - bk = 0$, but $0 \notin S$!) $\Rightarrow r < b$. Thus, we conclude that there exist q, r ($0 \leq r < b$) s.t. $a = bq + r$.

① (uniqueness), let us assume $\exists q, r, q', r'$ s.t. $a = bq + r = bq' + r'$. Let $r' \geq r$ $0 \leq r, r' < b$ $\Rightarrow b(q - q') = r' - r \Rightarrow b$ divides $r' - r$ and

$0 \leq r' - r < b \Rightarrow$ it is only possible if $r' - r = 0$ (2)

 $\Rightarrow r' = r \Rightarrow q' = q.$

$b \mid r' - r$ and
 $r' - r < b$

□

Some terminology:

Let $a, b \in \mathbb{Z}$. Then

say $a \nmid b$
if doesn't

- if $b = ak$ for $k \in \mathbb{Z}$, we write $a \mid b$ ("a divides b").

- $d \in \mathbb{Z}$ is a common divisor of a & b if $d \mid a$ & $d \mid b$.

- The greatest common divisor of a, b is $d \in \mathbb{Z}$,
 $d > 0$ s.t. $d \mid a$, $d \mid b$ and any other common divisor $d' \mid d$. we write: $d = \gcd(a, b)$

Examples: $\gcd(4, 5) = 1$, $\gcd(4, 10) = 2$,
 $\gcd(15, 40) = 5$, $\gcd(2^2 \cdot 3^2 \cdot 5, 2 \cdot 3^3 \cdot 7^2) = 2 \cdot 3^2$

- a, b are relatively prime if $\gcd(a, b) = 1$.
 \hookrightarrow or "coprime" (e.g., 12 & 13 are rel. prime)

Thm. (2.10) Let $a, b \in \mathbb{Z}$, $a, b \neq 0$. Then $\exists r, s \in \mathbb{Z}$
s.t. $\gcd(a, b) = ar + bs$. Also, $\gcd(a, b)$ is unique.

Proof: Show existence of r, s (using WOP)

Let $S = \{am + bn \mid m, n \in \mathbb{Z}, am + bn > 0\}$

Note $S \neq \emptyset$ (since by choosing $m = +1$ or -1 and $n = +1$ or -1 , we have $am + bn > 0$). Therefore, as a non-empty subset of \mathbb{N} , S is well-ordered \Rightarrow

S has a smallest member, $d = ar + bs$ for some $(d > 0)$ $r, s \in \mathbb{Z}$.

We claim that $d = \gcd(a, b)$. Let us show this. By the division algorithm, $a = dq + r'$, $0 \leq r' < d$ and if $r' = 0 \Rightarrow d \mid a$. If we let $r' > 0$ then

$$r' = a - dq = a - (\underbrace{ar + bs}_q)q = a(1 - rq) + b(-sq) \in S, \text{ but}$$

(3)

it leads to a contradiction, since $r', d \in S$, and $r' < d$, the smallest member of S . Thus, $r' = 0 \Rightarrow d | a$. Similarly, one can show $d | b$.

So, d is a common divisor of a & b .

Let d' be another common divisor of a, b , i.e. $d' | a, d' | b$. Then $a = d'h, b = d'k \Rightarrow d = ar + bs = (d'h)r + (d'k)s = d'(hr + ks) \Rightarrow d' | d$. So, $d = \gcd(a, b)$ is unique.

□

Corollary : Let $a, b \in \mathbb{Z}$ be relatively prime.
(2.11) Then $\exists r, s \in \mathbb{Z}$ s.t. $ar + bs = 1$.

Examples :

$$\textcircled{1} \quad a = 17, b = 5, \quad a = -23, b = 6, \quad \begin{array}{cccc} a & b & r & s \\ 17 & = 5 \cdot 3 + 2 & & \\ -23 & = 6(-4) + 1 & & \end{array} \quad \left. \begin{array}{l} \text{by division alg.} \\ \text{or } 4 \cdot (-11) + 15 \cdot 3 = 1 \end{array} \right\}$$

$$\textcircled{2} \quad \underbrace{\gcd(4, 15) = 1}_{\text{coprime}}, \quad \underbrace{4 \cdot 4 + 15(-1) = 1}_{\text{Thm. 2.10}} \quad \text{or } 4 \cdot (-11) + 15 \cdot 3 = 1$$

$$\underbrace{\gcd(4, 10) = 2}_{\text{not coprime}}, \quad \underbrace{4(-2) + 10 \cdot 1 = 2}_{\text{or } 4 \cdot 3 + 10(-1) = 2} \quad \underline{r, s \text{ are not unique!}}$$

Q: How do we compute $\gcd(a, b) = d$?

Repeat divisions to obtain a decreasing sequence of positive $r_1 > r_2 > \dots > r_n = d$:

$$a = b \cdot q_1 + r_1 \quad b > 0 \quad (r_{n+1} = 0)$$

$$b = r_1 \cdot q_2 + r_2$$

$$r_1 = r_2 \cdot q_3 + r_3$$

$$\vdots$$

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

$$r_{n-1} = r_n \cdot q_{n+1} (+ 0)$$

$$"d = \gcd(a, b)"$$

← stop here!
 (alg. terminates, as
 $r_i \downarrow, r_i \geq 0$)

Example: (see 2.12 in text as well)

$$\gcd(270, 192)$$

$$270 = 192 \cdot 1 + 78$$

$$192 = 78 \cdot 2 + 36$$

$$78 = 36 \cdot 2 + 6$$

$$36 = \boxed{6} \cdot 6 + \boxed{0} \Rightarrow 6 | 36 \Rightarrow 6 | 78 \Rightarrow 6 | 192$$

$\Rightarrow 6 | 270 \Rightarrow 6$ divides both 270, 192

If $d' \neq 6$, $d' | 270$, $d' | 192$ then $d' | 6$ as well! So,

$$\gcd(270, 192) = 6.$$

Q: How do we find r, s s.t. $ar + bs = d$ ($= \gcd(a, b)$)?

$$d = r_n = r_{n-2} - r_{n-1} q_n = r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2})$$

$$= -q_n r_{n-3} + (1 + q_n q_{n-1}) r_{n-2} = \dots = ra + sb.$$

Try for 270, 192:

$$6 = 78 - 36 \cdot 2 = 78 - (192 - 72 \cdot 2) \cdot 2$$

$$= 78 \cdot 5 + 192 \cdot (-2) = (270 - 192 \cdot 1) \cdot 5 + 192 \cdot (-2)$$

$$= 270 \cdot 5 + 192 \cdot (-7)$$

(r, s are not unique!)
 $\underbrace{}_r$ $\underbrace{}_s$

Algorithm above to find $\gcd(a, b)$ and r, s s.t. $\gcd(a, b) = ar + bs$ is called

the Euclidean algorithm.

Prime Numbers.

→ 2, 3, 5, 7, 11, ... 89, ... 97, ...

Def: An integer $p > 1$ is a prime number (or p is prime) if the only positive numbers that divide p are 1 and p itself. An integer $q > 1$ which is not prime is called composite.

Euclid's Lemma (2.13)

If p is prime and $p \mid ab$ ($a, b \in \mathbb{Z}$), then $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$, then we are done.

Assume $p \nmid a$. p is prime \Rightarrow if

$d = \gcd(p, a)$ then $d \mid p$, $d \mid a$ and d could be either p or 1, but since $p \nmid a \Rightarrow d = 1 \Rightarrow$

(a & p are relatively prime) $\Rightarrow \exists r, s \in \mathbb{Z}$ st.

$ar + ps = 1$ (Corollary 2.11) $\Rightarrow b = b(ar + ps)$

$= (ab)r + p(bs)$. Given $p \mid ab$ and "

$p \nmid p$, we have $p \mid b$.

□

Note: Lemma fails for not prime #'s:

$6 \mid 4 \cdot 3$, but $6 \nmid 4$ and $6 \nmid 3$.

Thm. 2.14 (Euclid) There exist an infinite # of primes.

Proof: (By contradiction) Suppose \exists finite # primes:

$p_1 = 2 < p_2 = 3 < \dots < p_r$. Consider $P = p_1 p_2 \dots p_r + 1$.

- (1) P is prime \Rightarrow contradiction! (P is another prime not in list)
- (2) P is not prime \Rightarrow let $p_i \mid P$ ($1 \leq i \leq r$)

(6)

then since $p_i \mid P$ and $p_i \mid p_i \Rightarrow$

 $(p_i > 1)$

$p_i \mid (P - p_1 p_2 \dots p_i \dots p_r) \Rightarrow p_i \mid 1 \Rightarrow$ not possible.

$\Rightarrow p_1, \dots, p_r$ would not be all primes, and

$\exists p \neq p_i$ that divides P . \square

Thm. 2.15 Fundamental Theorem of Arithmetic.

Every integer $n > 1$ can be written as

$n = p_1 p_2 \dots p_k$ where p_i is prime, $i = 1, \dots, k$
 (not necessarily distinct) in exactly one way
 (up to reordering).

Ex: $70 = 2 \cdot 5 \cdot 7$ $228 = 2 \cdot 2 \cdot 3 \cdot 19$

Proof: (see text as well)

① Prove by induction that $n = p_1 p_2 \dots p_k$.

Basis step: $n = 2$, 2 is prime, so we are done.

Assume that $\forall 2 \leq k \leq n$, k can be written

as a product of primes.

Inductive step: consider $k+1$. If it is prime, then we are done; if not, then

$\underbrace{k+1}_{\text{composite}} = ab$ for $1 < a, b < k+1$, i.e. $a, b \in \mathbb{Z}$
 $a, b \leq k$ ($2 \leq k \leq n \Rightarrow$ true)

\Rightarrow by hypothesis, $a = \underbrace{p_1 \dots p_r}_{\text{prime #'s}}$, $b = \underbrace{q_1 \dots q_s}_{\text{prime #'s}}$

$\Rightarrow k+1 = \underbrace{p_1 \dots p_r}_{\text{prime #'s}} \underbrace{q_1 \dots q_s}_{\text{prime #'s}}$.

② Uniqueness of factorization.

Let $n = p_1 \dots p_r = q_1 \dots q_s$. Consider p_1 .

 Second proof
("strong")

(7)

$p_1 | n \Rightarrow p_1 | q_1 \cdots q_s \Rightarrow$ by Euclid's Lemma,

$p_1 | q_i$ for some $1 \leq i \leq s \Rightarrow p_1 = q_i \Rightarrow$
 $(\text{prime } \# \text{'s}!)$

rename q_i to $q_1 = p_1$. Then

$$n = p_1 p_2 \cdots p_r = p_1 q_2 \cdots q_s \Rightarrow p_2 \cdots p_r = q_2 \cdots q_s$$

Repeat. Then $p_2 = q_j$, etc. We'll see $\forall p_k$,

$p_k = q_k$ and $r=s \Rightarrow n$ is factored in exactly one
 (after renaming) way.

(See text for different proof) \square

One more definition: least common multiple

$\text{lcm}(a, b)$ is the smallest positive integer
 $a, b \neq 0$ that is a multiple of both
 $a, b \in \mathbb{Z}$ & a & b .

Ex:

$$\begin{aligned} \text{lcm}(4, 6) &= 12 \\ \text{lcm}(4, 8) &= 8 \end{aligned}$$

$$\begin{aligned} \text{lcm}(6, 5) &= 30 \\ \text{lcm}(10, 12) &= 60 \end{aligned}$$