Section 1 — Integers

Warm-up How many numbers can you pick from $\{1, 2, \ldots, 20\}$ so that no pair of numbers you picked add up to another number you picked.

- second half OR odds

We start with a fundamental notion.

Def Let $d, n \in \mathbb{Z}$. We say that d divides n if there is an integer $c \in \mathbb{Z}$ such that $n = dc$. In this case, we also say that d is a divisor of n.

Notation

- "d divides n" $\longleftrightarrow$ $d \mid n$
- "d does not divide n" $\longleftrightarrow$ $d \nmid n$

Ex Justify each of the following:

(a) $2 \mid 14$ $\quad 14 = 2 \cdot 7$

(b) $-6 \mid 48$ $\quad 48 = (-6)(-8)$

(c) $0 \nmid 10$

$0 \mid 10 \Rightarrow 0 \cdot d = 10$
but $0 \cdot d = 0$ for all $d \in \mathbb{Z}$

Ex Write each statement using "bar" notation.

(a) 7 divides c

$7 \mid c$

(b) x is not a divisor of y

$x \nmid y$

(c) n is divisible by 5

$5 \mid n$

(d) z is even

$2 \mid z$

Lemma 1 Let $a, b, d \in \mathbb{Z}$. If $\underbrace{d \mid a}$ and $\underbrace{d \mid b}$, then $\underbrace{d \mid a+b}$.

conclusion

hypotheses

pf

where to start? where to end?

hypotheses

Suppose $d \mid a$ and $d \mid b$. Then

- $a = de$ for some $e \in \mathbb{Z}$
- $b = df$ for some $f \in \mathbb{Z}$

Thus $a+b = de + df = d(\underbrace{e+f}_{g})$. Let $g = e+f$

Then $g \in \mathbb{Z}$ and $a+b = dg$, so $d \mid a+b$. $\square$

conclusion

Lemma Let $a, b, d \in \mathbb{Z}$. If $d \mid a$, then $d \mid a \cdot b$.

pf

Suppose $d \mid a$. Then $a = de$ for some $e \in \mathbb{Z}$.

Now, $ab = deb = d(eb)$. Let $c = eb$.

Then $c \in \mathbb{Z}$ and $ab = dc$, so $d \mid ab$. $\square$

Question Does 3 divide $21 + 24 + 99$? How did you think about this?

Lemma 2 Let $a_1, \ldots, a_n, c_1, \ldots, c_n, d \in \mathbb{Z}$. If $d \mid a_i$ for all $1 \le i \le n$, then $d \mid (c_1 a_1 + \cdots + c_n a_n)$.

pf

Similar to before. (See the book.)

Ex Suppose you have 99 coins made up of pennies, dimes, and quarters. Is it possible that you have exactly \$5.00?

We want to solve

$$\left.\begin{array}{ll} ① & p+d+q=99 \qquad p,d,q\in\mathbb{Z} \\ ② & p+10d+25q=500 \end{array}\right\}\ \text{Diophantine system}$$

Importantly, we want to know if there is an <u>integer</u> solution.

Notice that

$$② - ① \implies 9d+24q=401$$

$$\implies 3(3d+8q)=401$$

If there is a solution with $p,d,q\in\mathbb{Z}$, then 3 divides 401. But 3 does <u>not</u> divide 401, so there is not an integer solution.

Final answer: $\boxed{\text{Not possible}}$

Common divisors

<u>Def</u> Let $a_1,\dots,a_n\in\mathbb{Z}$. We say $d\in\mathbb{Z}$ is a <u>common divisor</u> of $a_1,\dots,a_n$ if d divides each of $a_1,\dots,a_n$ (i.e $d\mid a_1,\dots,d\mid a_n$).

Ex Find all common divisors

(a) $8, 12$ $\pm 1, \pm 2, \pm 4$ gcd is 4

(b) $-15, 25$ ± 5 gcd is 5

(c) $-15, 25, 6$ ± 1 gcd is 1

Notice: there is always a greatest common divisor.

Def Let $a, b \in \mathbb{Z}$ with a, b not both 0. Then

$d \in \mathbb{Z}$ is called the greatest common divisor of a and b if

(1) d is a common divisor of a and b;

(2) if c is any common divisor of a and b then $c \le d$.

- we denote the gcd by $\gcd(a,b)$ or just $\boxed{(a,b)}$
- notice that $\gcd(0,0)$ is undefined.
- also $\gcd(a,b) \ge 1$.

used in the book

Ex Find $\gcd(12, -30)$.

① list common divisors: $\pm 1, \pm 2, \pm 3, \pm 6$

② answer: $\gcd(12, -30) = 6$.

Questions: what's the use of gcd's & how to find them?

Def Integers a and b are relatively prime if $\gcd(a,b) = 1$.

thus, the only common divisors are ± 1

Theorem 1 Let $a, b \in \mathbb{Z}$. If $d = \gcd(a,b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

we saw $\gcd(12, -30) = 6$

then $\gcd\left(\frac{12}{6}, \frac{-30}{6}\right) = \gcd(2, -5) = 1$

pf

Let $c = \gcd\left(\frac{a}{d}, \frac{b}{d}\right)$. WTS $c = 1$

① $\boxed{c \geq 1}$ b/c gcd's are always at least 1.

② $\boxed{c \leq 1}$ b/c ...

$$c = \gcd\left(\frac{a}{d}, \frac{b}{d}\right) \Longrightarrow \begin{array}{l} \frac{a}{d} = c \cdot r \\ \frac{b}{d} = c \cdot s \end{array} \quad \text{for } r, s \in \mathbb{Z}$$

$$\Longrightarrow \begin{array}{l} a = crd \\ b = csd \end{array}$$

$\Longrightarrow$ cd is a common divisor of a and b

$\Longrightarrow cd \leq d$

$\Longrightarrow c \leq 1.$

since d is positive

Since $c \geq 1$ and $c \leq 1$, $c = 1$. $\square$

Euclidean Algorithm

for computing gcd's

We start with an essential theorem about divisibility ...

<u>Question</u>: Recall that

$$6\,\overline{)\,22}^{\;3} \qquad \begin{array}{r} 22 \\ -18 \\ \hline 4 \end{array}$$

. what does this mean? Quotient is 3, remainder is 4. Thus

$$22 = 3 \cdot 6 + 4$$

<u>Follow-up</u>: Does 6 divide 22? Why? No, remainder of 4.

a workhorse of algebra

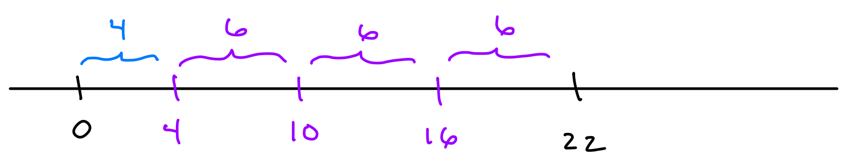
<u>Theorem 2</u> (Division Algorithm) Let $a, b \in \mathbb{Z}$ with $b \neq 0$. Then there exist unique integers q (quotient) and r (remainder) with $0 \leq r < b$ such that

$$a = qb + r.$$

! Notice that $b \mid a \iff r = 0$.

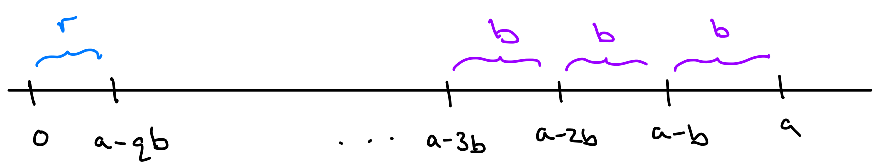
<u>pf idea</u>

Example:



$$22 = 3 \cdot 6 + 4$$

In general:



consider the set of all non-negative integers of the form $a - kb$. Choose the smallest one and call it r. Then $r = a - qb$ for some $q \in \mathbb{Z}$ and

- $0 \leq r < b$

AND

- $a = qb + r$ for some $q \in \mathbb{Z}$.

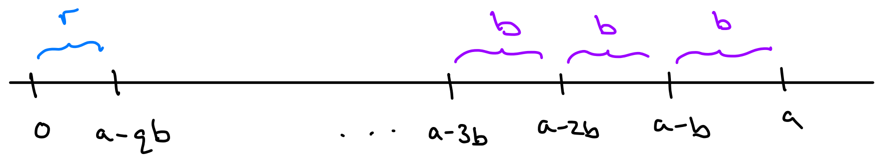
$\square$

Lemma 3 If $a, b, q, r \in \mathbb{Z}$ with $a = qb + r$, then
$$\gcd(a,b) = \gcd(b,r).$$

pf

Optional

Consider:



Step 1: if d divides a and b, then d must also divide r. Why?

$r = a - qb$ so $d \mid a$ and $d \mid b$ implies $d \mid r$.

by Lemma 2

Thus $\gcd(a,b) \leq \gcd(b,r)$.

Step 2: if d divides b and r, then d must also divide a. why

$a = qb + r$ so $d \mid b$ and $d \mid r$ implies $d \mid a$.

Thus, $\gcd(b,r) \leq \gcd(a,b)$.

By 1 and 2, the common divisors of a and b are the same as the common divisors of b and r. So both pairs have the same gcd. $\square$

Strategies for finding $\gcd(a,b)$

① Find all factors of a and all factors of b. Then choose the largest.

② Use the Euclidean Algorithm (see below)

Euclidean Algorithm (By Example)

Ex Find $\gcd(578, 442)$.

Idea: Lemma 3.

Lemma 3

$$\underbrace{578}_{a} = \underbrace{1}_{q} \cdot \underbrace{442}_{b} + \underbrace{136}_{r} \qquad \gcd(578,442) = \gcd(442,136)$$

$$\underbrace{442}_{a} = \underbrace{3}_{q} \cdot \underbrace{136}_{b} + \underbrace{34}_{r} \qquad \gcd(442,136) = \gcd(136,34)$$

$$136 = 4 \cdot 34 + 0 \qquad \gcd(136,34) = \gcd(34,0)$$

So

$$\gcd(578,442) = \gcd(34,0) = \boxed{34}$$

Ex Find $\gcd(7644, 1302)$

$$7644 = 5 \cdot 1302 + 1134 \qquad \gcd(7644,1302) = \gcd(1302,1134)$$

$$1302 = 1 \cdot 1134 + 168 \qquad \gcd(1302,1134) = \gcd(1134,168)$$

$$1134 = 6 \cdot 168 + 126 \qquad \gcd(1134,168) = \gcd(168,126)$$

$$168 = 1 \cdot 126 + 42 \qquad \gcd(168,126) = \gcd(126,42)$$

$$126 = 3 \cdot 42 + 0 \qquad \gcd(126,42) = \gcd(42,0)$$

So,

$$\gcd(7644,1302) = \gcd(42,0) = \boxed{42}$$

- The Euclidean Algorithm is very important computationally.
- The following theorem is very important theoretically.

<u>Theorem 4</u> Suppose $a, b \in \mathbb{Z}$. Let $d = \gcd(a,b)$. Then there exists $x, y \in \mathbb{Z}$ such that

$$ax + by = d.$$

<u>Pf</u> follows from the Euclidean Algorithm as we see in the next example.

<u>Ex</u> We saw that $\gcd(7644, 1302) = 42$. Find x, y such that $7644x + 1302y = 42$.

<u>Process</u>

(1) Perform the Euclidean Algorithm

<u>Recall:</u>

$$7644 = 5 \cdot 1302 + \underline{1134}$$
$$1302 = 1 \cdot 1134 + \underline{168}$$
$$1134 = 6 \cdot 168 + \underline{126}$$
$$168 = 1 \cdot 126 + \underline{42}$$
$$126 = 3 \cdot 42 + 0$$

② Solve for the remainders

$$^{***}\underline{1134} = 7644 - 5 \cdot 1302$$

$$^{**}\underline{168} = 1302 - 1134$$

$$^{*}\underline{126} = 1134 - 6 \cdot 168$$

$$\underline{42} = 168 - 126$$

③ Work from "bottom to top" making substitutions

$$\begin{aligned}
42 &= 168 - \overset{*}{126} \\
&= 168 - (1134 - 6 \cdot 168) \\
&= -1134 + 7 \cdot \overset{**}{168} \\
&= -1134 + 7(1302 - 1134) \\
&= 7 \cdot 1302 - 8 \cdot \overset{***}{1134} \\
&= 7 \cdot 1302 - 8(7644 - 5 \cdot 1302) \\
&= \underbrace{-8}_{x} \cdot 7644 + \underbrace{47}_{y} \cdot 1302
\end{aligned}$$

$$\boxed{x = -8 \text{ and } y = 47}$$

The next 3 corollaries illustrate how Theorem 4 can be used to prove new results.

Q: If $d \mid ab$, must it be true that $d \mid a$ or $d \mid b$?

Ex: $10 \mid 2 \cdot 50$ and $10 \mid 50$

but $10 \mid 4 \cdot 25$ but $10 \nmid 4$ and $10 \nmid 25$.

Corollary 1 Let $a, b, d \in \mathbb{Z}$. If $d \mid ab$ and $\gcd(d,a)=1$, then $d \mid b$.

pf

Assume

- $d \mid ab$

AND

- $\gcd(d,a) = 1 \xRightarrow{\text{Theorem 4}} xd + ya = 1$ for some $x, y \in \mathbb{Z}$.

Thus

$$xd + ya = 1 \implies (xd+ya)b = b$$
$$\implies xdb + yab = b$$

Note that

- $d \mid xdb$ since $xdb = d(xb)$
- $d \mid y\overset{ds}{ab}$ since $d \mid ab$ by hypothesis

By Lemma 2, if $d \mid xdb$ and $d \mid yab$, then $d \mid xdb + yab$, so $d \mid b$.

$\square$

<u>Corollary 2</u> Let $a,b,c \in \mathbb{Z}$. If $c \mid a$ and $c \mid b$, then $c \mid \gcd(a,b)$.

<u>pf</u>

By Theorem 4, there exists $x, y \in \mathbb{Z}$ s.t.

$$ax + by = \gcd(a,b).$$

Since $c \mid a$ and $c \mid b$, c divides the entire LHS by Lemma 2. Thus $c \mid \gcd(a,b)$.

$\square$

<u>Corollary 3</u> Let $a,b,c \in \mathbb{Z}$. If $a \mid c$ and $b \mid c$ and $(a,b)=1$, then $\underline{\underline{ab \mid c}}$.

this is about c

<u>pf</u>

By Theorem 4, there exists $x, y \in \mathbb{Z}$ s.t.

$$ax + by = 1.$$

Multiplying by c,

$$acx + bcy = c.$$

Also,

$$\begin{matrix} a \mid c \\ b \mid c \end{matrix} \implies \begin{matrix} c = as \\ c = bt \end{matrix} \quad \text{for } s, t \in \mathbb{Z}.$$

Thus,

$$abtx + basy = c$$

$$\implies ab(tx + sy) = c \quad \text{with } tx + sy \in \mathbb{Z}.$$

$$\implies ab \mid c.$$

$\square$