Chap 2. Divisibility

Def 2.1 For $a, b \in \mathbb{Z}$. We say "b divides a", written as $b \mid a$ to mean there exists an integer $c \in \mathbb{Z}$ such that $a = bc$.

and we'll write $b \nmid a$ to mean this is not so, i.e. there is no such integer c.

eg. $2 \mid 10$ since $10 = 2 \cdot \underline{5}$ c

$4 \mid 12$ since $12 = 4 \cdot 3$ c

$3 \nmid 10$ since we cannot find an integer c to complete $10 = 3 \cdot \underline{c}$

b is termed a <u>divisor</u>/<u>factor</u> of a.

a is termed a <u>multiple</u> of b

Technically divisibility is a binary relation on $\mathbb{Z}$.

"$b|a$" it's true or false

Theorem 2.1

Proofs of these follow straight from the definition, or are straightforward observations about $\mathbb{Z}$.

1. $\forall a \in \mathbb{Z} \quad a|a$.

Proof since $a = a \underbrace{1}_{\in \mathbb{Z}}$. ✓

2. Assume $a|b$ & $b|c$.

$\Rightarrow \exists \beta, \gamma \in \mathbb{Z}$ such that $b = \beta a$, $c = \gamma b$

$\Rightarrow c = a \underbrace{\beta \gamma}_{\in \mathbb{Z}}$, coming from substitution with

$\Rightarrow a|c$.

3. For $a, b, c \in \mathbb{Z}$.

If $a|b$ & $a|c$ then $a \mid nb + mc$

for every choice of $\underline{\underline{n, m \in \mathbb{Z}}}$.

Assume $\boxed{a|b \;\&\; a|c}$

$\Rightarrow \exists\ \underline{\underline{\beta, \gamma \in \mathbb{Z}}}$ such that $b = \beta a$, $c = \gamma a$

Then $nb + mc = n\beta a + m\gamma a$

$$\Rightarrow nb + mc = a\underline{(n\beta + m\gamma)}$$

$\in \mathbb{Z}$?

$$\Rightarrow \boxed{a \mid nb + mc}$$

This property will be mentioned.

4. For $a \in \mathbb{Z}$ $1|a$ because $a = 1\,\underline{a}$

5. For all $a \in \mathbb{Z}$ $a|0$, because $0 = a \cdot \underline{0}$

6. If $0|a$, then $a = 0$.

Assume $0|a$, so $\exists\ c \in \mathbb{Z}$

such that $\boxed{a = 0 \cdot c = 0}$

7. For $c \neq 0$. $a|b \Leftrightarrow ac|bc$.

Assume $a|b$

$\Leftrightarrow \exists\ x \in \mathbb{Z}$ $b = ax$

$\Leftrightarrow \exists x \in \mathbb{Z} \quad \underline{\underline{bc}} = \underline{\underline{ac}}x$

$\Leftrightarrow ac \mid bc$

2.3. Common divisors

For a pair of integers $a, b \in \mathbb{Z}$, how can we measure/capture what divisibility they share?

Def 2.3. "d is a common divisor of a, b" means $d \mid a$ and $d \mid b$.

Def 2.4 The $\boxed{\gcd(a,b)}$ is the greatest common divisor of a, b. This is the largest integer d such that $d \mid a$ and $d \mid b$.

$2 = 2 \cdot 36 + -5 \cdot 14$

$$\boxed{\gcd(36, 14) = 2}$$

$$\gcd(100, 75) = 25$$

If $\gcd(a,b)=1$ we say a,b are coprime.

The Euclidean Algorithm calculates gcd very quickly. It's based on "integer division with remainder"

Theorem 2.2

Eg.

20 divided by 3, goes in 6 times with remainder 2.

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

$20 = 3 \cdot 6 + 2.$

Do examine the proof.

Theorem 2.3

If $d = \gcd(a,b)$, then there exist $m, n \in \mathbb{Z}$ s.t. $d = ma + nb$ and moreover d is the smallest positive linear combination of a,b.

Proof: Consider the subset $\subseteq$ of positive integers

$$S = \{\alpha a + \beta b : \alpha, \beta \in \mathbb{Z},\ \alpha a + \beta b > 0\}$$

By the well ordered axiom S has a smallest element. Call this $d \in S$

so $d = ma + nb$, for some $m, n \in \mathbb{Z}$.

Claim $d \mid a$ and $d \mid b$

Proof by contradiction

Suppose $d \nmid a$ $\quad q, r \in \mathbb{Z}$.

then $a = qd + r$, $0 < r < d$

$$\Rightarrow r = a - qd$$
$$= a - q(ma + nb)$$
$$= \underbrace{(1 - qm)}_{\in \mathbb{Z}}a - \underbrace{qn}_{\in \mathbb{Z}}b$$

$\Rightarrow \{ r \in S. \}$

This is a contradiction, as d is the smallest integer in S.

So therefore $d \mid a$. Similarly, can prove $d \mid b$.

So d is a common divisor of a, b.

And if e is any other positive common divisor, i.e. $e \mid a$, $e \mid b$

$\Rightarrow e \mid d$, since $d = ma + nb$ by 3 of Th. 2.1.

$\Rightarrow e \leq d$.

So $d = \gcd(a, b)$.

2.4. The Euclidean algorithm is an efficient algorithm for

• calculates $\gcd(a,b)$

(extended) • produces m, n such that

$$\boxed{\gcd(a,b) = ma + nb.}$$

Bezout's Identity.

Lemma 2.4. For a, b, q, r.

If $a = bq + r$

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

Proof. By proving a,b and b,r have the same common divisors.

Assume $d \mid a$, and $d \mid b$.

Notice $r = a - bq$

$\Rightarrow d \mid r$, by ③ Th 2.1

So d is a common divisor of b, r.

Assume $d \mid b$ and $d \mid r$

Notice $a = bq + r$

$\Rightarrow d \mid a$.

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

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

Euclidean Algorithm Alg. 2.1

$\gcd(525, 90) = ? = 15.$

$525 = 5 \cdot 90 + \underline{\underline{75}}$, $\underline{\gcd(525,90)} = \gcd(90,75)$

$90 = 1 \cdot 75 + 15$, $\underline{\gcd(90,75)} = \gcd(75,15)$

$75 = 5 \cdot 15 + \underline{\underline{0}}$ $\quad \underline{\gcd(75,15)} = \underline{\gcd(\underline{\underline{15}},0)} = \underline{15}$

Finding Bezout's identity for 525, 90

$15 = 525 \, \underline{(-1)} + 90 \, \underline{6}$

Work backwards through the sequence of integer divisions.

$15 = 90 - 1 \cdot 75$

$= \underline{\underline{90}} - (525 - 5 \cdot \underline{\underline{90}})$

$= 6 \cdot 90 - 525$

Let's $\gcd(119, 272) = ?$