Math 425: Abstract Algebra 1

Section 1.2: Divisors and Prime Factorization

Mckenzie West

Last Updated: September 12, 2022

Last Time.

- Induction

Today.

- Division Algorithm
- GCD
- Bézout's Identity
- Euclidean Algorithm
- Prime Factorization Theorem

The Division Algorithm (Thm 1.2.1).

Let $n \in \mathbb{Z}$ and $d \geq 1$ be an integer. Then there exists uniquely determined $q, r \in \mathbb{Z}$ such that

$$n = qd + r \text{ and } 0 \leq r < d.$$

Note.

I prove this in the video for today.

Definition.

For $a, b, d \in \mathbb{Z}$:

- We write $a \mid b$ to mean *a divides b*, which is defined formally as

$$a \mid b \Leftrightarrow b = ak \text{ for some } k \in \mathbb{Z}.$$

- We say d is *a common divisor of a and b* if $d \mid a$ and $d \mid b$.
- The *greatest common divisor of a and b* is the largest integer that is a common divisor of a and b. Denote this value by $\gcd(a, b)$.

Bézout's Identity (Thm 1.2.2).

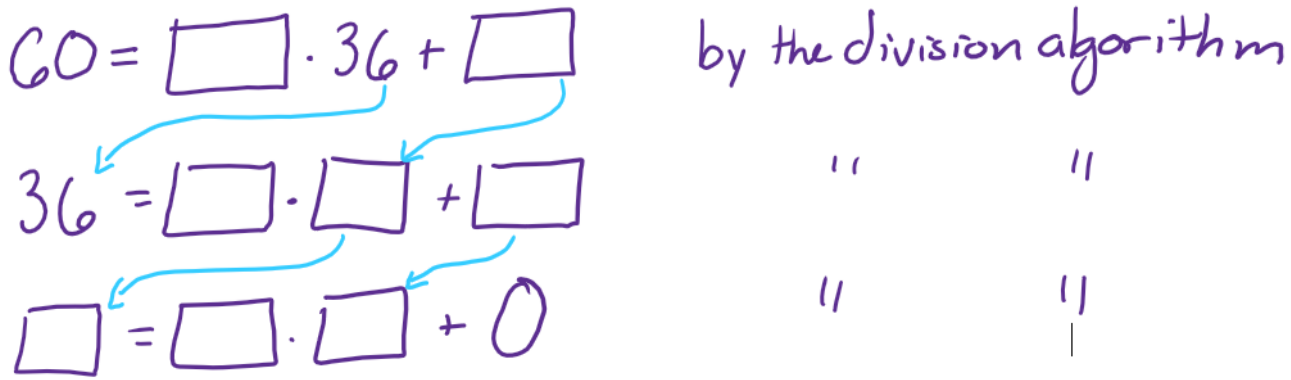
Let a and b be integers, not both zero. Then there exist $r, s \in \mathbb{Z}$ such that $\gcd(a, b) = ra + sb$.

Idea.

Run the Euclidean algorithm in reverse. - See the next slides.

Exercise 1.

The Euclidean Algorithm (via an example)
Compute gcd(36, 60):



Stop when the remainder is zero. The previous remainder is the gcd.

Exercise 2.

Now we know that $\gcd(36, 60) = 12$ and we want to write

$$12 = 36r + 60s.$$

Start with the second to last row of the Euclidean Algorithm:

$$12 = 36 - 1 \cdot 24.$$

Use the line above that to replace 24:

$$12 = 36 - 1 \cdot (\_\_\_\_\_).$$

Simplify

$$12 = 36 \cdot (\_\_\_\_\_) + 60 \cdot (\_\_\_\_\_).$$

Definition.

We say that $m, n \in \mathbb{Z}$ are `relatively prime` if $\gcd(m, n) = 1$.

Theorem 1.2.4.

Let $m, n \in \mathbb{Z}$ not both zero. Then

$$m, n \text{ relatively prime} \Leftrightarrow \exists r, s \in \mathbb{Z} \text{ such that } 1 = rm + sn$$

Theorem 1.2.4.

Let $m, n \in Z$ not both zero. Then

$$m, n \text{ relatively prime} \Leftrightarrow \exists r, s \in \mathbb{Z} \text{ such that } 1 = rm + sn$$

Proof idea.

($\Rightarrow$) Bézout

($\Leftarrow$) Assume $1 = rm + sn$ for some $r, s \in \mathbb{Z}$. Let c be a common divisor of m and n.

$\Rightarrow$ $c \mid (rm + sn)$ why

$\Rightarrow$ $c \mid 1$ why

$\Rightarrow$ $\gcd(m, n) = 1$ why

□

Brain Break.

Which superpower would you like to have?

1. Mind reading
2. Invisibility
3. Teleportation
4. Flying
5. _____
6. I already have a superpower

Euclid's Lemma.

Let p be a prime number.

1. If $p \mid mn$ where $m, n \in \mathbb{Z}$, then $p \mid m$ or $p \mid n$.
2. If $p \mid m_1 m_2 \cdots m_r$ where $m_i \in \mathbb{Z}$ for all i, then $p \mid m_i$ $\exists i$.

Note.

Proof is in the book. I'll write some examples quick. Think of your own too.

Prime Factorization Theorem (Theorem 1.2.7).

1. Every integer $n \geq 2$ is a product of (one or more) primes.
2. This factorization is unique (up to order of the factors). That is, if

$$n = p_1 p_2 \cdots p_r \text{ and } n = q_1 q_2 \cdots q_2,$$

then $r = s$ and the q_j can be relabeled so that $p_i = q_i$ for $i = 1, 2, \ldots, r$.

Note.

I'll walk through the proof of (2) - we'll see similar proofs later in the semester when we talk about UFDs (Unique Factorization Domains).

"Proof" (1).

Strong induction. (See page 26 Example 7.) □

Proof (2)

Assume toward contradiction that (2) fails. Then by WOP there is a smallest integer m such that

$$m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

are two distinct prime factorizations of m.
Thus m is not prime. why? So $r, s \geq 2$.
Notice that

why? $p_1 \mid q_1 q_2 \cdots q_s$ so $p_1 | q_j$ for some $1 \leq j \leq s$.

Proof (2) Continued.

By relabeling we can assume $p_1 \mid q_1$. Observe that $p_1 = q_1$. why?
Since

$$m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \text{ and } p_1 = q_1,$$

we see that

$$\frac{m}{p_1} = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_s$$

are two distinct factorizations of the integer $\frac{m}{p_1}$.

This is a contradiction. why? □

Corollary.

Two integers are relatively prime if there exists no prime that divides them both.

Corollary.

Every $n \in \mathbb{Z}_{\geq 2}$ can be written uniquely as

$$n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$$

where the p_i are distinct primes and $n_i \geq 1$ for all i.

Theorem 1.2.8.

Let $n \geq 2$ be an integer with prime factorization

$$n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$

where the p_i are all distinct primes and $n_i \geq 1$ for all i. Then

$$d \mid n \Rightarrow d = p_1^{d_1} p_2^{d_2} \cdots p_r^{d_r} \text{ where } 0 \leq d_i \leq n_i \ \forall i.$$

Exercise 3.

(a) Write 60 as $p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$

(b) Use Theorem 1.2.8 to find all divisors of 60.

Question 4.

How many divisors does $p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ have?

Theorem 1.2.9.

Let $\{a, b, c, \dots\}$ be a finite set of positive integers and write

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} \\ b &= p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r} \\ c &= p_1^{c_1} p_2^{c_2} \cdots p_r^{c_r} \end{aligned}$$

where there is an exponent of zero if the prime is not a factor. Then

$$\gcd(a, b, c, \dots) = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

where $k_i = \min(a_i, b_i, c_i, \dots)$ for each i, and

$$\operatorname{lcm}(a, b, c, \dots) = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r},$$

where $m_i = \max(a_i, b_i, c_i, \dots)$ for each i.

Exercise 5.

$$28665 = 3^2 \cdot 5 \cdot 7 \cdot 13 \text{ and } 22869 = 3^3 \cdot 7 \cdot 11^2$$

Compute

(a) $\gcd(28665, 22869)$

(b) $\text{lcm}(28665, 22869)$