Greatest Common Divisors

Lemma: Let $a, b \in \mathbb{Z}$ not both zero.
There exists a unique $d \in \mathbb{N}$ such that

① $d \mid a$ and $d \mid b$ (d is a common divisor)
② For all $d' \in \mathbb{N}$, if $d' \mid a$ and $d' \mid b$, then $d' \leq d$.

We say d is the greatest common divisor of a and b, and write $d = \gcd(a, b)$.

Proof: Consider the set of all positive integers which are common divisors of a and b.

This set is non-empty (1 is a common divisor) and finite (every common divisor d satisfies $d \leq |a|$ or $d \leq |b|$), so it has a largest element. ∎

Warm-Up: Compute

$\gcd(10, 24)$
$\gcd(45, 15)$
$\gcd(1, 37)$
$\gcd(0, 37)$

Note: The book uses a slightly different name (highest common factors) and definition.

Ex: If $a \in \mathbb{N}$, then $\gcd(a,0) = a$.

Ex: Why do we not allow $a=b=0$?
Every integer divides 0.

Lemma: Let $a, b \in \mathbb{Z}$ not both zero.
(a) $\gcd(a,b) = \gcd(b,a)$
(b) $\gcd(a,b) = \gcd(a,-b)$

Proof: (a) The definition is symmetric in a and b.
(b) Divisors of $-b$ are precisely divisors of b. $\square$

How to compute $\gcd(a,b)$?

- If a and b are small, can list divisors.
- $\gcd(270, 192)$? Larger numbers?

The Euclidean Algorithm

Lemma: Let $a, b, q, r \in \mathbb{Z}$ such that

$$a = bq + r.$$

Then for all $d \in \mathbb{N}$, d is a common divisor of a and b if and only if d is a common divisor of b and r.

In particular, $\gcd(a,b) = \gcd(b,r)$.

Proof: HW 14.

Algorithm (Euclidean): INPUT: $a, b \in \mathbb{N}$ with $a \geq b$.
OUTPUT: $\gcd(a,b)$.

Set $r_{-1} = a$ and $n = 0$.
$r_0 = b$

While $r_n \neq 0$:

- Divide r_{n-1} by r_n to get

$$r_{n-1} = r_n q_{n+1} + r_{n+1}$$

- If $r_{n+1} = 0$, output r_n and STOP.
- Else, increment $n \to n+1$.

Ex: $a = 270$, $b = 192$

$\begin{pmatrix} r_{-1} = 270 \\ r_0 = 192 \end{pmatrix}$

$270 = 192(1) + 78$ $\quad q_1 = 1,\ r_1 = 78$

$192 = 78(2) + 36$ $\quad q_2 = 2,\ r_2 = 36$

$78 = 36(2) + 6$ $\quad q_3 = 2,\ r_3 = 6$

$36 = 6(6) + 0$ $\quad q_4 = 6,\ r_4 = 0$

STOP and output 6.

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

Why does this work?

We must show

① The algorithm terminates.

② The output is correct.

<u>Proof of termination</u>: By the division algorithm,

$$\underbrace{r_{-1} \geq r_0}_{a \geq b \text{ is given}} > r_1 > r_2 > \cdots \geq 0$$

Since the remainder decreases at every step, some remainder must eventually be zero. ✓

<u>Proof of correctness</u>: We have

$$r_{-1} = r_0 q_1 + r_1$$

$$r_0 = r_1 q_2 + r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n$$ ← Last non-zero remainder

$$r_{n-1} = r_n q_{n+1} + 0$$

So

$$\begin{aligned}\gcd(a,b) &= \gcd(r_{-1}, r_0)\\ &= \gcd(r_0, r_1)\\ &= \gcd(r_1, r_2)\\ &\ \vdots\\ &= \gcd(r_{n-1}, r_n)\\ &= \gcd(r_n, 0) = r_n\end{aligned}$$

✓

Soon, we'll prove

<u>Thm</u>: Let $a, b \in \mathbb{Z}$, not both zero. Set $d = \gcd(a,b)$. Then there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = d.$$

Ex: $a = 270$, $b = 192$ (so $d = 6$ by above)

From the Euclidean algorithm, we get

$$6 = 78 - 36(2)$$

$$= 78 - [192 - 78(2)] \cdot 2 = 78(5) + 192(-2)$$

$$= [270 - 192] \cdot 5 + 192(-2)$$

$$= 270(5) + 192(-7).$$

So $x = 5$, $y = -7$ solves

$$270x + 192y = 6.$$