8/24/2022
We

Last time · Well-ordering principle: any $\emptyset \neq X \subseteq \mathbb{N}$ has the least element

- Well-ordering principle $\Leftrightarrow$ mathematical induction
- "division algorithm" for $\mathbb{Z}$: $\forall\, a, d \in \mathbb{Z}$ with $d \geq 1$ $\exists!$ (exist unique) $r, q \in \mathbb{Z}$ so that
  i) $a = q \cdot d + r$
  ii) $0 \leq r < d$
- $d \mid a \Leftrightarrow \exists\, q \in \mathbb{Z}$ s.t. $a = q \cdot d$

Theorem 2.1 Let m, n, d be integers. Then

i) $n \mid n$
ii) if $d \mid n$ and $n \mid m$ then $d \mid m$
iii) if $d \mid n$ and $n \mid d$ then $n = \pm d$
iv) if $d \mid n$ and $d \mid m$ then $d \mid xn + ym$ for all $x, y \in \mathbb{Z}$.

Proof (i), (ii), (iv) - Homework

Proof of (iii): Since $d \mid n$, $n = \ell d$ for some $\ell \in \mathbb{Z}$.
Since $n \mid d$, $d = nk$ for some $k \in \mathbb{Z}$
$\Rightarrow n = \ell \cdot (kn) \Rightarrow (1 - \ell k) \cdot n = 0$

Recall if $x, y \in \mathbb{Z}$ and $x \cdot y = 0$ then $x = 0$ or $y = 0$.
Hence either $n = 0$. ~~And~~ Then $d = 0$, hence $n = d$)
Or $n \neq 0$. And then $1 - \ell k = 0$, Hence $\ell k = 1 \Rightarrow \ell = k = \pm 1$.
so $n = \pm d$ □

Definition The greatest common divisor (gcd) of two integers a and d (if it exists) is an integer $d \geq 1$ so that
1) $d \mid a$ and $d \mid b$
2) if $c \mid a$ and $c \mid b$ then $c \mid d$.

Recall $\forall k \in \mathbb{Z}$, $k \mid 0$ since $0 = 0 \cdot k$

So if $a = b = 0$ then $\forall c \in \mathbb{Z}$, $c \mid a$ and $c \mid b$

$\Rightarrow$ $\gcd(0,0)$ does not exist.

Exercise What's $\gcd(-5, 0)$? Does it exist?

Remark If $d = \gcd(a,b)$ exists, it's automatically unique.

Reason: Suppose d_1, d_2 are two gcd's of a and b.

Then $d_1 \mid a$, $d_1 \mid b$ (since d_1 is a gcd of a and b). Hence $d_1 \mid d_2$ (since d_2 is the greatest common divisor of a and b)

Similarly $d_2 \mid d_1$.

By 2.1 (iii), $d_1 = \pm d_2$. But gcd's are positive by definition

$\Rightarrow d_1 = d_2$.

Theorem 2.2 Let $a, b \in \mathbb{Z}$, not both zero. Then $\gcd(a,b)$ exists. Moreover, $\exists x, y \in \mathbb{Z}$ st $\gcd(a,b) = xa + yb$.

Proof

Let $S = \{ ua + vb \mid u, v \in \mathbb{Z},\ ua + vb \geq 1 \}$

Since $a \cdot a + b \cdot b > 0$, $a \cdot a + b \cdot b \in S$. $\Rightarrow S \neq \emptyset$. By well-ordering $\exists\ d = \min(S)$. Then (i) $d \geq 1$ and (ii) $d = xa + yb$ for some $x, y \in \mathbb{Z}$

Claim $d = \min(S)$ is (the) gcd of a and b.

2.1 (iv) $\Rightarrow \forall c$ with $c \mid a$ and $c \mid b$, $c \mid ua + vb$ $\forall u, v$. $\Rightarrow$

$\Rightarrow c \mid d\ (= xa + yb)$.

Remains to show: $d \mid a$ and $d \mid b$

Division algorithm $\Rightarrow$ $a = qd + r$ for some $q, r \in \mathbb{Z}$, $0 \leq r < d$.

We argue: $r = 0$. If $r > 0$, then $0 < r = a - qd = a - q(xa + yb)$

$= (1 - qx)a + (-qy)b$. $\Rightarrow r \in S$. But $r < d = \min S$. Contradiction.

$\therefore r = 0$ and $d \mid a$.

Similarly $d \mid b$.

Q: How does one compute $\gcd(n,m)$?

Lemma 2.3 For all $k \in \mathbb{Z}$, $\forall\, n, m \in \mathbb{Z}$

$$\gcd(n,m) = \gcd(n-km, m).$$

Proof Let $d = \gcd(n,m)$, $f = \gcd(n-km, m)$.

Since $d|n$ and $d|m$, $d \mid n-km$.

$\Rightarrow$ $d \mid \gcd(n-km, m) = f$.

Similarly, $f \mid (n-km)$, $f \mid m \Rightarrow$ $f \mid (n-km) + k \cdot m = n$

Since $f|m$ and $f|n$, $f \mid \gcd(n,m) = d$.

Since $f|d$ and $d|f$, $d = \pm f$. But $f, d \geq 1$ by definition.

$\therefore$ $f = d$. ∎

Remarks We haven't defined primes yet. We haven't proven that any integer can be uniquely factored into primes. So we are not using factorizations into primes to compute gcd's. Also, factoring into primes is computationally hard (or so I hear.)

Ex Find $d = \gcd(154, 35)$ and $x, y \in \mathbb{Z}$ s.t. $d = x \cdot 154 + y \cdot 35$.

Solution
$$154 = 4 \cdot 35 + 14 \quad \text{(division algorithm)}$$
$$35 = 2 \cdot 14 + 7$$
$$14 = 2 \cdot 7$$

Lemma 2.3 $\Rightarrow$ $\gcd(154, 35) = \gcd(154 - 4 \cdot 35, 35) = \gcd(35, 14) =$
$= \gcd(35 - 2 \cdot 14, 7) = \gcd(14, 7) = 7.$

Moreover,
$$7 = 35 + (-2) \cdot 14$$
$$14 = 154 - 4 \cdot 35$$
$$\therefore\ 7 = 35 + (-2) \cdot (154 - 4 \cdot 35) = \big(1 + (-2)(-4)\big) \cdot 35 + (-2) \cdot 154$$
$$= (-2) \cdot 154 + 9 \cdot 34$$

Definition Two integers a and b are relatively prime if $1 = \gcd(a,b)$.

Lemma 2.4 $\gcd(a,b) = 1 \iff \exists x, y \in \mathbb{Z}$ s.t. $xa + yb = 1$

Proof ($\Rightarrow$) in theorem 2.2

($\Leftarrow$) Suppose $xa + yb = 1$ for some $x, y \in \mathbb{Z}$. Then, since $\gcd(a,b) \mid a$ and $\gcd(a,b) \mid b$, $\gcd(a,b) \mid xa + yb = 1$

On the other hand $1 \mid \gcd(a,b)$. $\therefore 1 = \pm \gcd(a,b)$.

(recall: $c \mid d$ & $d \mid c \Rightarrow c = \pm d$). But $\gcd(a,b) \geq 1$.

$\therefore \gcd(a,b) = 1$ □

Theorem 2.5 [tricky, important!] Suppose $\gcd(a,n) = 1$ and $a \mid (mn)$. Then $a \mid m$.

Proof Since $\gcd(a,n) = 1$, $\exists x, y \in \mathbb{Z}$ s.t. $ax + ny = 1$.

$\Rightarrow m = m \cdot 1 = mxa + mny$

Now, $a \mid mxa$ and $a \mid mny$ since $a \mid mn$.

$\therefore a \mid m = mxa + mny$. □

Definition An integer $p \geq 2$ is prime iff the only positive integers that divide p are p and 1

Remark p is prime $\iff$ ($p = ab \Rightarrow a = \pm 1$ or $b = \pm 1$)