Number theory

↳ study of the integers $\mathbb{Z}$ and their arithmetic

"The queen of mathematics"
— Gauss

↳ since primes are the multiplicative building blocks of all integers, they play an important role.

Def'n: Fix $n \in \mathbb{N}$, $n > 1$.

① n is prime iff its only positive divisors are 1 and n.

② n is composite iff it is not prime, i.e. iff $\exists a, b \in \mathbb{N}$ with $a, b > 1$ s.t. $n = a \cdot b$.

We proved (by strong induction): any $n > 1$ can be written as a product of primes:

or (tw you'll prove: unique way to do this.

Divisors: **Def'n** m is a divisor of n iff $m \mid n$, i.e. iff $\exists k \in \mathbb{Z}$ s.t. $n = m \cdot k$.

Note every $n \in \mathbb{Z}$ is a divisor of 0, since $0 = 0 \cdot n$. However, if $n \neq 0$ and $m \mid n$, then $|m| \leq |n|$.

Def'n: Fix $m, n \in \mathbb{Z}$, not both 0. The greatest common divisor of m and n, written $\gcd(m,n)$, is the largest $d \in \mathbb{N}$ dividing both m, n.

Ex: ① What is $\gcd(42, 60)$?

Divisors of 42 $= \{\pm 1, \pm 2, \pm 3, \pm 6, \pm 7, \pm 14, \pm 21, \pm 42\}$

Divisors of 60 $= \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 10, \pm 12, \pm 15, \pm 20, \pm 30, \pm 60\}$

Common divisors $= \{\pm 1, \pm 2, \pm 3, \pm 6\}$

$\Rightarrow \gcd(42, 60) = 6$

② $\gcd(42, 0) = 42$, since 42 is largest divisor of 42 and also $42 \mid 0$.

③ $\gcd(-42, 60) = 6$. (still positive)

---

next theorem says: if we divide out by gcd, get #s with no common factors except ± 1.

Theorem: Fix $m, n \in \mathbb{Z}$ (not both 0) and let $d = \gcd(m,n)$.

Then: $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$.

Pf: • Let $a = \gcd\left(\frac{m}{d}, \frac{n}{d}\right)$ WTS: $a = 1$.

• so $a \geq 1$ and $a \mid \frac{m}{d}$ and $a \mid \frac{n}{d}$

• i.e. $\exists k, \ell \in \mathbb{Z}$ s.t.

$$\frac{m}{d} = ak \qquad \frac{n}{d} = a\ell$$

$\Rightarrow m = (ad)k \qquad n = (ad)\ell$

$\Rightarrow ad \mid m$ and $ad \mid n$

$\Rightarrow$ so ad is a common divisor of m, n

$\Rightarrow$ but d is the greatest common divisor of m, n, so $ad \leq d$

$\Rightarrow a \leq 1$

$\Rightarrow a = 1$ ✓

ex: $\gcd\left(\frac{42}{6}, \frac{60}{6}\right) = \gcd(7, 10)$

$= 1$ (as expected from theorem)

Q: is there a better way of finding $\gcd(m,n)$ than writing out all divisors of m, n?

A: yes! the Euclidean algorithm (will do later...)

First: Theorem (Division algorithm)

- Fix $b \in \mathbb{Z}$ and $a \in \mathbb{N}$

Then: there exist unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < a$ s.t.

$$b = aq + r.$$

(q is the quotient of b when divided by a, r is the remainder).

---

before pf: example illustrating idea.

if $b = 14$, $a = 3$

Consider:

$3 \cdot 1 = 3$ $\quad$ $14 - 3 \cdot 1 = 11 > 3$

$3 \cdot 2 = 6$ $\quad$ $14 - 3 \cdot 2 = 8 > 3$

$3 \cdot 3 = 9$ $\quad$ $14 - 3 \cdot 3 = 5 > 3$

$3 \cdot 4 = 12$ $\quad$ $14 - 3 \cdot 4 = 2 < 3$ → $14 = 3 \cdot 4 + 2$

---

pf: Define $S = \{ n \in \mathbb{N} \cup \{0\} \mid (\exists k \in \mathbb{Z})\ n = b - ak \}$

(e.g. if $b=14, a=3$, then $S=\{2,5,8,11,\ldots\}$)

Observe: • $S \neq \emptyset$ since $b-ak \geq 0$ whenever $b \geq ak$ (k can be negative)

• but $S \subseteq \mathbb{N}\cup\{0\}$, hence by WOP, S has a least elt r.

• So let $q \in \mathbb{Z}$ be the integer s.t.

$$b-aq=r$$

$$\Rightarrow b = aq+r.$$

Claim: $r<a$

Pf: - If not, $r \geq a$

- So $r = a+r_1$ with $r_1 \geq 0$ and $r_1 < r$

- but then: $b = aq+r = aq+a+r_1$

$$= a(q+1)+r_1$$

- hence $r_1 \in S$

↪ contradiction, as r was least in S. ✓

- So we've proved existence of r, q s.t. $b=aq+r$ and $r<a$.

- need to prove uniqueness of r and q.

- So sps $q', r' \in \mathbb{Z}$ with $0 \leq r' < a$ and $b = aq'+r'$.

WTS: $q = q'$ and $r = r'$

Will: either $r \geq r'$ or $r' \geq r$.
Let's assume $r \geq r'$; other case is similar.

Then: $r - r' = aq' - aq$

$\Rightarrow r - r' = a(q' - q)$

$\Rightarrow a \mid r - r'$. But $0 \leq r - r' < a$.

Hence it must be $r - r' = 0$

i.e. $r = r'$.

$\Rightarrow b = aq + r = aq' + r$

$\Rightarrow aq = aq' \Rightarrow q = q'$ ✓

Ex's ① Let $a = 15$, $b = 107$

Then $107 = 15 \cdot 7 + 2$ (i.e. $q = 17, r = 2$)

② Let $a = 6$, $b = -29$

Then $-29 = 6(-5) + 1$ ($q = -5, r = 1$)

③ $a = 3$, $b = 12$

Then $b = 3 \cdot 4 + 0$. ($q = 4, r = 0$)

Next theorem is the (IMO) Fundamental result about divisibility.

Bezout's Theorem: Fix $a, b \in \mathbb{Z}$ (not both 0) and let $d = \gcd(a,b)$

Then $\exists\, m, n \in \mathbb{Z}$ such that

$$d = am + bn$$

"d can be written as a linear combination of a, b"

note: m, n not unique

and d is the least natural number that can be so written

Example before proof: Consider $a = 27$, $b = 21$

Q: if we +/− 21's and 27's in any combination: how small a positive number can we get?

e.g. $27 - 21 = 6$, i.e. $21(-1) + 27(1) = 6$

or better yet: $21(4) + 27(-3) = 3$

can we do better than 3? Doesn't seem so, but we can get 3 in more than one way, e.g. $21(-5) + 27(4) = 3$.

Notice: $\gcd(21, 27) = 3$. Bezout says: our discovery above is no accident.

i.e. $\exists m, n \in \mathbb{Z}$ s.t. $21m + 27n = 3$

and there are no $m', n' \in \mathbb{Z}$ s.t.

$0 < 21m' + 27n' < 3$.

Pf of Bezout:

- Define $S = \{c \in \mathbb{N} \mid (\exists m, n \in \mathbb{Z})\ c = am+bn\}$

  = set of positive linear combinations of a, b.

- Observe: S is not empty since $|a|+|b| \in S$.
- Hence by WOP: S has a least elt d.
- Fix $m, n \in \mathbb{Z}$ s.t. $d = am+bn$ (possible since $d \in S$).
- WTS: $d = \gcd(a,b)$.

Claim: ① $d \mid a$ and ② $d \mid b$.

Pf: (1) by division algorithm we can write: $a = q \cdot d + r \quad 0 \le r < d$ (WTS: $r = 0$)

$$\Rightarrow \quad r = a - q \cdot d$$
$$= a - q(am+bn)$$
$$= (1-qm)a + (-qn)b.$$

- hence r is a linear combo of a, b
- we know $r \geq 0$. If $r > 0$, then would have $r \in S$.
- but $r < d$, so $r \in S$ would contradict minimality of d.
- hence $r \notin S$, i.e. $r = 0$.
- i.e. $a = q \cdot d$, so $d \mid a$. ✓
- similarly prove $d \mid b$ ✓

Claim 2 d is greatest common divisor of a, b.

PF: - Sps $t \in \mathbb{N}$ and $t \mid a$ and $t \mid b$
- we prove $t \mid d$, which gives $t \leq d$

$\exists k, \ell \in \mathbb{Z}$ s.t. $a = \ell t$ $b = kt$.

so: $d = am + bn$
$= \ell t m + k t n$
$= (\ell m) t + (kn) t$
$= t[\ell m + kn]$
$\Rightarrow t \mid d$. ✓

Claim 1 + Claim 2 $\Rightarrow$ $d = \gcd(a, b)$ ✓

Defn Fix $a, b \in \mathbb{Z}$. We say a, b are relatively prime iff $\gcd(a,b) = 1$.

Cordlary of Bezout: if $a, b \in \mathbb{Z}$ are relatively prime then $\exists m, n \in \mathbb{Z}$ s.t.

$$am + bn = 1.$$

Pf: immediate since $\gcd(a,b) = 1$.

Ex's ① $\gcd(25, 36) = 1$. So Bezout guarantees $\exists m, n \in \mathbb{Z}$ s.t. $25m + 36n = 1$.

And indeed:

$$25(-23) + 36(16) = 1.$$

$$(-575 + 576 = 1)$$

② Observe: if p is prime, then for any $a \in \mathbb{Z}$, either $p \mid a$ or $\gcd(p,a) = 1$

In particular: if p, q are distinct primes then $\gcd(p,q) = 1$. Hence $\exists m, n$ s.t. $pm + qn = 1$.

eg if $p = 7$, $q = 31$ then:

$$7(9) + 31(-2) = 1.$$

Theorem (Euclid's Lemma)

Fix $a,b,c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$.

Pf: Sps $a \mid bc$ and $\gcd(a,b) = 1$.

- then $\exists \ell \in \mathbb{Z}$ s.t. $bc = a\ell$
- by Bezout we also have: $\exists m,n \in \mathbb{Z}$ s.t.

$$am + bn = 1.$$

- hence

$$\begin{aligned} & c \cdot 1 = c \\ \Rightarrow \quad & c(am+bn) = c \\ \Rightarrow \quad & acm + bcn = c \\ \Rightarrow \quad & acm + a\ell n = c \\ \Rightarrow \quad & a(cm + \ell n) = c \\ \Rightarrow \quad & a \mid c. \end{aligned}$$

Corollary: Fix $a,b \in \mathbb{Z}$, and $p \in \mathbb{N}$ a prime. If $p \mid ab$ then either $p \mid a$ or $p \mid b$ (or both)

Pf: - If $p \mid a$, we are done. So suppose $p \nmid a$.
- then must be $\gcd(p,a) = 1$
- hence by Euclid: $p \mid b$ ✓