Number theory: the study of the integers 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 $1 < a, b < n$ s.t. $n = a \cdot b$.

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

you'll prove: there's a unique way to do this for every $n \in \mathbb{N}$

Def'n Given $m, n \in \mathbb{Z}$ we say m is a **divisor** of n iff $m \mid n$, i.e. iff $\exists k \in \mathbb{Z}$ s.t. $n = mk$

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, n, written $\gcd(m,n)$, is the largest $d \in \mathbb{N}$ dividing both m and 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 $42 \mid 0$

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

---

next theorem says: if we divide out by gcd, we end up w/ #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.

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

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

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

$\Rightarrow$ but d = 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 cover 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 proof: example illustrating pf.

if $b = 14$ $a = 3$

Consider:

$3 \cdot 1 = 3$	$14 - 3 \cdot 1 = 11 > 3$
$3 \cdot 2 = 6$	$14 - 3 \cdot 2 = 8 > 3$
$3 \cdot 3 = 9$	$14 - 3 \cdot 3 = 5 > 3$
$3 \cdot 4 = 12$	$14 - 3 \cdot 4 = 2 < 3$

$\rightarrow 14 = 3 \cdot 4 + 2$

---

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

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

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

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

- 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 is 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 suppose $q', r' \in \mathbb{Z}$ with $0 \leq r' < a$

and $b = aq' + r'$

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

Well: either $r \geq r'$ or $r' \geq r$.

Let's assume $r \geq r'$, other case is similar.

then: $r - r' = aq' - aq$

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

$\Rightarrow a \mid r - r'$. 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: ① Let $a = 15$, $b = 107$.

Then $107 = 15 \cdot 7 + 2$ $(q = 7, r = 2)$

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 (one) fundamental result about divisibility

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

Then $\exists m, n \in \mathbb{Z}$ s.t.

$$d = am + bn$$

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

note: m, n not unique

Furthermore: d is the least natural # 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. $21(-1) + 27(1) = 6$)

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. $21m+27n=3$

but there are not m', n' s.t. $21m'+27n'=1$ or 2.

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 e.g. $|a| + |b| \in S$.
- Hence by WOP: S has a least el't 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: by division algorithm we can write $a = q \cdot d + r$ $0 \le r < d$ (WTS: $r = 0$)

$$\Rightarrow r = a - qd$$
$$= a - q(am+bn)$$
$$= (1-qm)a + (-qn)b$$

- hence r is a linear combo of a, b.
- we knew $r \geq 0$. If $r > 0$, then $r \in S$.
- but $r < d$, so $r \in S$ would contradict minimality of d.
- hence $r \notin S$, i.e. $r = 0$.

$\Rightarrow a = q \cdot d$ so $d \mid a$.

② similarly can 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 $t \leq d$.

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

So $d = am + bn$

$= \ell t m + kt n$

$= t(\ell m + kn)$

$\Rightarrow t \mid d$.

Claim ① + Claim ② establishes theorem ✓

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

Corollary 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: $25(-23) + 36(16) = 1$

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. $pm + qn = 1$, by Bezout.

e.g. if $p = 7$ $q = 31$ then

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

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, also $\exists m, n \in \mathbb{Z}$ s.t.

$$am + bn = 1$$

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

$\Rightarrow a \mid c$

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 sps $p \nmid a$.

- then must be $\gcd(p, a) = 1$
- hence by Euclid: $p \mid b$ ✓

Thm (Fund thm of arithmetic)

Every $n \in \mathbb{N}$, $n > 1$, can be written uniquely (up to the order of factors) as a product of primes.

Pf: Two parts: (i) existence: every $n > 1$ can be written as a product of primes ✓ (proved already by strong induction)

(ii) uniqueness: HW.

Ex's ① $21 = 3 \cdot 7 = 7 \cdot 3$ — no other way to factor into primes.

$21 \neq 2 \cdot 2 \cdot 5$

$\neq 2 \cdot 11$

② $200 = 2 \cdot 100 = 2 \cdot 2 \cdot 50$

$= 2 \cdot 2 \cdot 2 \cdot 25$

$= 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$

$= 2^3 5^2$

③ $97 = 97$ (is prime)

We proved following thm on day 1, but lets prove again (using FTOA)

Thm There are infinitely many primes

Pf:- Sps there are only finitely many primes, say $p_1, \dots, p_N$.

- Define $P = p_1 p_2 \cdots p_N + 1$
- By FTOA, P has a prime factorization in particular P is divisible by some prime p.
- must have $p \in \{p_1, \dots, p_N\}$ (these are the only primes), i.e. $p = p_j$ for some j $1 \le j \le N$.
- Hence $P = p_j \cdot k$

But we know: $P = p_1 \cdot p_2 \cdots p_N + 1$

$$= p_j \underbrace{(p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_N)}_{M} + 1$$

$$= p_j \cdot M + 1$$

Hence $P = p_j k = p_j M + 1$

$$\Rightarrow 1 = p_j M - p_j k$$

$$= p_j (M - k) = 1 \Rightarrow p_j \mid 1,$$

a contradiction, as $p_j > 1$ (since prime) ✓

Note: proof actually shows that if $\{p_1, p_2, \ldots, p_N\}$ is any set of primes then $p_1 p_2 \cdots p_N + 1$ can only be divisible by primes $p \notin \{p_1, \ldots, p_N\}$

e.g. consider $\{3,5,7\}$

$3 \cdot 5 \cdot 7 + 1 = 106 = 2 \cdot 53$

↗ no 3, 5, 7 in factors.

Modular arithmetic: Recall: if $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$ then $a \equiv b \pmod n$ means $n \mid b - a$.

- $\equiv \pmod n$ is an equiv. relation
- $\mathbb{Z}/n\mathbb{Z}$ denotes $\{[a]_n \mid a \in \mathbb{Z}\}$

Let's finally prove:

Prop'n Fix $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Then $a \equiv b \pmod n$ iff a, b have same remainder when divided by n.

Pf: By division algorithm $\exists$ unique integers q_1, r_1, q_2, r_2 with $0 \le r_1, r_2 < n$ s.t.

$a = q_1 n + r_1 \quad b = q_2 n + r_2$

So: $b-a = (q_2-q_1)n + (r_2-r_1)$

($\Rightarrow$) Assume $a \equiv b \pmod n$ i.e. $n \mid b-a$.

- then $b-a = nk$ for some $k \in \mathbb{Z}$.
- hence $nk = (q_2-q_1)n + (r_2-r_1)$

$\Rightarrow n(k-q_2+q_1) = r_2-r_1$

$\Rightarrow n \mid r_2-r_1$

but since $r_1, r_2 < n$ must have $|r_2-r_1| < n$

Hence $n \mid r_2-r_1 \Rightarrow r_2-r_1 = 0$, i.e. $r_2 = r_1$ ✓

($\Leftarrow$) Assume $r_2 = r_1$

Then $b-a = (q_2-q_1)n$

$\Rightarrow n \mid b-a \Rightarrow a \equiv b \pmod n$ ✓

Ex: $17 \equiv 37 \pmod 4$

↳ could check: $4 \mid 37-17$

↳ or observe $37 = 9 \cdot 4 + 1$, $17 = 4 \cdot 4 + 1$ ⇝ same r.

Since only poss. remainders when dividing by n are $0, 1, \ldots, n-1$, the prop'n justifies another fact:

$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$$