Number Theory

- "Number theory" is the 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 $\exists a, b \in \mathbb{N}$, $a, b > 1$ s.t. $n = a \cdot b$.

We proved (by strong induction): any $n \in \mathbb{N}$ except 1 can be written as a product of primes

↳ on HW you will prove: a unique way to do this!

Testing Primality → hard!

Q: how to check a given $n \in \mathbb{N}$ is prime?

↳ could just divide by every $k < n$ to see if there's a divisor

↳ or be a bit smarter:

Theorem Fix $n \in \mathbb{N}$. Suppose $n = a \cdot b$. Then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Pf: Sps not. Then $a > \sqrt{n}$ and $b > \sqrt{n}$

but then $ab > \sqrt{n}\sqrt{n} = n$, contradiction ✓

↳ so to check if n is prime only need to test for divisors $k \leq \sqrt{n}$.

ex: determine if 91 or 97 are prime.

Sol'n: - observe $9 < \sqrt{91} < \sqrt{97} < 10$
- so only need to test for prime divisors up to 9.

91: $2 \nmid 91$ $3 \nmid 91$, $5 \nmid 91$, but $7 \mid 91$
so 91 is not prime

97: $2 \nmid 97$, $3 \nmid 97$, $5 \nmid 97$, $7 \nmid 97$
so 97 is prime.

Divisors: Def'n m is a divisor of n iff $m \mid n$

$m \mid n$ iff $\exists k \in \mathbb{Z}$ $n = mk$

$\boxed{\text{Note}}$ For every $n \in \mathbb{Z}$, we have n divides 0, since $0 = 0 \cdot n$

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 natural number d 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 $= \{\pm 1, \pm 2, \pm 3, \pm 6\}$

$\hookrightarrow \gcd(42, 60) = 6.$

② $\gcd(42, 0) = 42$
(42 is largest divisor of 42 and $42 | 0$)

③ $\gcd(-42, 60) = 6.$

$\hookrightarrow$ if we divide out by gcd, we get numbers w/ no common factors but ± 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 $a = \gcd(\frac{m}{d}, \frac{n}{d})$
- 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.
$\frac{m}{d} = ak \qquad \frac{n}{d} = a\ell$
- so $m = (ad)k \qquad n = (ad)\ell$.
- so $ad \mid m$ and $ad \mid n$
i.e. ad is a common divisor of m, n
- but then by def'n of gcd:
$ad \leq d$
$\Rightarrow a \leq 1$
So $1 \leq a \leq 1 \Rightarrow a = 1$, as claimed ✓

ex: $\gcd(\frac{42}{6}, \frac{60}{6}) = \gcd(7, 10)$
$= 1$ (as expected)

Q: better way of finding $\gcd(a,b)$ than writing out all divisors of a, b?

↳ Euclidean algorithm will give such a way
→ long way to go before we get there.

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 quotient of b when divided by a, r is remainder) idea: consider $b = 14$ $a = 3$

$3 \cdot 1 = 3$ and so $14 - 3 \cdot 1 = 11 > 3$

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

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

$3 \cdot 4 = 12$ so $14 - 3 \cdot 4 = 2 < 3$ $\to$ $14 = 3 \cdot 4 + 2$

q a r

S

the challenge in # theory: realize that is something to prove!

Pf: Define

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

Observe: $S \neq \emptyset$

since $b - ak \geq 0$

whenever $b \geq ak$

can be –

e.g. if $b = 14$ $a = 3$

$S = \{14 - 3 \cdot 4, 14 - 3 \cdot 3, 14 - 3 \cdot 2, 14 - 3 \cdot 1, 14 - 3 \cdot 0, 14 - 3(-1), \ldots\}$

$= \{2, 5, 8, 11, 14, 17, \ldots\}$

- hence by WOP

S has a least element r

- let $q \in \mathbb{Z}$ be s.t.

$b - aq = r$

- then $b = aq + r$

Claim: $r < a$

pf: - if not, $r \geq a$

- so we can write $r = a + r_1$

where $0 \leq r_1 < r$

- 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.

$\hookrightarrow$ hence $r < a$ as claimed ✓

So we've proved existence of r, q s.t. $b = aq + r$ and $0 \leq r < a$

need to prove <u>uniqueness</u>

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

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

We have:
$b = aq + r = aq' + r'$

either $r \ge r'$ or $r' \ge r$
Assume $r \ge r'$, since other case is similar

then: $r - r' = aq' - aq$
$\Rightarrow r - r' = a(q' - q)$

so $a \mid r - r'$
but $0 \le r - r' < a$
so must have $r - r' = 0$, i.e. $r = r'$
but then
$b = aq + r = aq' + r$
so $q = q'$ too ✓

(i)

<u>Ex's</u> 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 one of the fundamental results about divisibility

<u>Bezout's Theorem</u>
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"

<u>and</u> d is least natural number that can be so written.

<u>Example before proof:</u>
Consider $a = 6$ $b = 15$
Q: if we +/− 6's and 15's how small a positive number could we get?

$15 - 6 = 9$

$15 - 6 - 6 = 3$, i.e. $6(-2) + 15(1) = 3$

can we do better than 3?

(ii)

Doesn't seem so, but we can get 3 in more than one way

e.g.

$6+6+6-15=3$ i.e. $6(3)+15(-1)=3$

Notice: $3=\gcd(6,15)$

Bezout says our discovery above is no accident:

$\exists m,n\in\mathbb{Z}$ s.t. $6m+15n=3$ (e.g. $m=-2$, $n=1$ or $m=3$, $n=-1$ work)

and there are no m,n s.t. $6m+15n=2$ or $=1$.

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 el't d.

- Fix $m,n\in\mathbb{Z}$ s.t. $d=am+bn$
- we WTS: $d=\gcd(a,b)$

(iii)

Claim 1: ① $d \mid a$ and ② $d \mid b$

① by division algorithm we can write

$$a = q \cdot d + r \qquad 0 \leq r < d$$

WTS: $r = 0$

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

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

② similar arg proves $d \mid b$.

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

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

↳ we have $\exists k, \ell \in \mathbb{Z}$ 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 + 2 $\Rightarrow d = \gcd(a, b)$

<u>Def'n</u> Fix $a, b \in \mathbb{Z}$. We say a, b are <u>relatively prime</u> iff $\gcd(a,b) = 1$

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

$$am + bn = 1.$$

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

<u>Ex</u> ① $\gcd(25, 36) = 1$ so Bezout says $\exists m, n \in \mathbb{Z}$ s.t. $25m + 36n = 1$ and indeed:

$$25(-23) + 36(16) = 1$$
$$576 - 575 = 1$$

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

<u>So</u>: if p, q are distinct primes then of course $\gcd(p,q) = 1$ so $\exists m, n \in \mathbb{Z}$ s.t.

$$pm + qn = 1$$

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

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

Here's a useful application of Bezout:

(V)

Prop'n (Euclid's Lemma)
Fix $a, b, c \in \mathbb{Z}$. If
$a \mid bc$ and $\gcd(a,b) = 1$
then actually $a \mid c$

Pf: Sps $a \mid bc$ and $\gcd(a,b) = 1$
- then $\exists \ell \in \mathbb{Z}$ s.t. $a\ell = bc$
- also: by Bezout $\exists m, n \in \mathbb{Z}$ s.t.
  $am + bn = 1$
- hence:

$$c(am + bn) = c$$
$$\Rightarrow acm + bcn = c$$
$$\Rightarrow acm + a\ell n = c$$
$$\Rightarrow a(cm + \ell n) = c$$
$$\Rightarrow a \mid c \checkmark$$

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

Pf: - If $p \mid a$ we are done
- so sps $p \nmid a$
- then it must be $\gcd(p,a) = 1$
  why: $\gcd(p,a) = 1$ or p since p is prime and we know $p \nmid a$.

- hence by Euclid's Lemma $p \mid b \checkmark$