Number Theory

↳ The study of the integers $\mathbb{Z}$ and their arithmetic.
↳ Since primes are the "multiplicative building blocks" of all integers, play an important role.

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

- n is prime iff its only divisors are 1 and itself.
- n is composite iff $\exists\, a, b \in \mathbb{N}$ $a, b > 1$ s.t. $n = a \cdot b$.
- we proved: n can be written as a product of primes
  ↳ you will prove: any such factorization is unique.

Testing Primality: How can we check whether a given $n \in \mathbb{N}$ is prime?
- could just try dividing by every $k < n$
- can do a bit better:

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

Pf: If $a > \sqrt{n}$ and $b > \sqrt{n}$
then $ab > n$
but $ab = n$ a contradiction.

↳ hence to test if a given $n \in \mathbb{N}$ is prime, only need to test for divisors k up to $\sqrt{n}$

ex: determine whether 91 or 97 are prime.

Sol'n: – $9 < \sqrt{91} < \sqrt{97} < 10$
– so only need to test 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

Note: by convention, every $n \in \mathbb{Z}$ 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 and n.

ex ① $\gcd(42, 60) \stackrel{?}{=}$

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 $\gcd(42, 0) = 42$
(42 is largest divisor of 42 and everything divides 0)

③ $\gcd(-42, 60) = 6.$

$\rightarrow$ if we "divide out" by the gcd we get numbers w/ no common factors besides ± 1.

Thm: Fix $m, n \in \mathbb{Z}$ and let $d = \gcd(m,n)$.

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

Pf - let $a = \gcd\left(\frac{m}{d}, \frac{n}{d}\right)$

- then $a \mid \frac{m}{d}$
- i.e. $\exists l \in \mathbb{Z}$ s.t. $al = \frac{m}{d}$

  hence $(ad) l = m$

  hence $ad \mid m$
- similarly $\exists k \in \mathbb{Z}$ s.t. $ak = \frac{n}{d}$

  hence $(ad)k = n$

  hence $ad \mid n$
- since $a \geq 1$ and ad, is a common divisor of m, n must have $ad = d$
- hence $a = 1$ as claimed.

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

$= 1$.

→ The <u>Euclidean Algorithm</u> will give us an <u>efficient</u> way of computing gcds
→ first we need some preliminary results.

<u>Thm</u> (Division algorithm)
Fix $a, b \in \mathbb{Z}$ with $a > 0$. Then there exist unique integers $q, r \in \mathbb{Z}$ with $0 \leq r < a$ s.t.
$$b = aq + r$$

(-q is called the <u>quotient</u> of b when divided by a
-r is the <u>remainder</u>)

<u>Pf</u>: Define $S = \{n \in \mathbb{N} \cup \{0\} \mid (\exists k \in \mathbb{Z})\ n = b - ak\}$

<u>Observe</u>: $S \neq \emptyset$
since $b - ak \geq 0$ whenever $k \leq \frac{b}{a}$.
(so in fact S is infinite)

<u>ex</u>: if $b = 5, a = 2$
$S = \{\ldots, 5-2(-1), 5-2\cdot1, 5-2\cdot2, \ldots\}$
$= \{\ldots, 7, 5, 3, 1\}$
$= \{1, 3, 5, 7, \ldots\}$

- Hence by WOP, S has a least element r.
- Let $q \in \mathbb{Z}$ be s.t. $b - aq = r$.
- then $b = aq + r$

<u>Observe</u>: $r < a$.

<u>Why</u>: - if not, then $r \geq a$.
- hence $r = a + r_1$ where $r_1 \geq 0$ and $r_1 < r$.
- hence $b = aq + a + r_1$
$= a(q+1) + r_1$
- hence $b - a(q+1) = r_1$
- hence $r_1 \in S$
- contradiction, since r was least in S.

So we have proved <u>existence</u> of q, r s.t. $b = aq + r$.

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

$$b = aq' + r'$$

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

Observe: - either $r \geq r'$ or $r' \geq r$.
Assume WLOG $r \geq r'$

- Now: $0 = b - b = aq + r - (aq' + r')$
$= a(q - q') + (r - r')$

- hence $a(q' - q) = r - r'$
- hence $a \mid r - r'$
- but $0 \leq r - r' < a$ (since $r < a$)
- hence $r - r' = 0$
i.e. $r = r'$

but then $a(q - q') = 0$
hence $q = q'$

$\Rightarrow$ thus proves uniqueness. ✓

Ex's

① Let $a = 15$ $b = 107$
Then
$107 = 15 \cdot 7 + 2$ So $q = 7$, $r = 2$

② $a = 6$ $b = -29$
Then
$-29 = 6(-5) + 1$ $q = -5$, $r = 1$

3) $a = 3 \qquad b = 12$

Then

$b = 3 \cdot 4 + 0$. $\qquad q = 4$, $r = 0$

Next theorem lies at the base of a lot of results on divisibility.

Theorem (Bezout)

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

Then there exist integers $m, n \in \mathbb{Z}$ s.t.

$$d = am + bn$$

(i.e. d can be written as a "linear combination" of a and b)

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

Before proof, example.

- $\gcd(6,15) = 3$
- thm says $\exists m, n \in \mathbb{Z}$

s.t. $6m + 15n = 3$

and indeed if $m=-2$ $n=1$
we have
$$6(-2)+15(1)=3$$

- these integers are not unique,
e.g.
$$6\cdot(3)+15(-1)=3 \text{ too}$$

- thm also says cannot find
$m,n\in\mathbb{Z}$ s.t.
$$6m+15n=2$$
or $6m+15n=1$

Pf of thm:

Define $S=\{c\in\mathbb{N} \mid (\exists m,n\in\mathbb{Z})\, c=am+bn\}$
= set of (positive) linear combinations of a and 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 want to prove $d=\gcd(a,b)$

Claim 1: ① $d | a$ and ② $d | b$

pf: ① – by the division algorithm can write

$$a = q \cdot d + r \quad \text{where } 0 \leq r < d$$

(WTS $r = 0$)

– hence $r = a - q \cdot d$

$$= a - q(am + bn)$$

$$= (1 - qm)a + (-qn)b$$

– 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 this would contradict minimality of d.

– hence $r = 0$

– hence $a = q \cdot d$ i.e. $d | a$

② – by a symmetric argument, $d | b$ also.

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

PF: – Suppose $t \in \mathbb{N}$ and $t | a$ and $t | b$.

we will prove $t|d$.

- we have $\exists k, l \in \mathbb{Z}$ s.t. $a = lt$ and $b = kt$

- hence
$$d = am + bn = ltm + ktn = t(lm + kn)$$
- hence $t|d$, as claimed
- hence $t \le d$.
- hence $d = \gcd(a,b)$ ✓

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

- The following is the most commonly used instance of Bezout's theorem

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

$$am + bn = 1$$

Pf: immediate.

ex: ① Since $\gcd(25,36)=1$ theorem says $\exists m,n\in\mathbb{Z}$ s.t.
$36m+25n=1$
– and indeed

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

② – if p is prime and $a\in\mathbb{Z}$ then either $p\mid a$ or $\gcd(p,a)=1$.
– in particular if p,q are distinct primes then $\gcd(p,q)=1$ so can find $m,n\in\mathbb{Z}$ s.t.
$pm+qn=1$
– e.g. if $p=7$ $q=31$

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

One useful application of Bezout's theorem is:

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

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

- Then $\exists l \in \mathbb{Z}$ s.t. $al = bc$
- By Bezout $\exists m,n \in \mathbb{Z}$ s.t.

$$am + bn = 1$$

- hence

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

<u>Corollary</u>: Fix $a,b,p \in \mathbb{Z}$ with p prime. If $p \mid ab$ then either $p \mid a$ or $p \mid b$.

<u>Pf</u>: - If $p \mid a$ we are done

- So suppose $p \nmid a$
- then p and a are relatively prime

<u>Why</u>: since p prime,
$\gcd(a,p) = 1$ or p
hence $= 1$ since $p \nmid a$

- So by Euclid's Lemma $p \mid b$

Theorem (Fundamental Theorem of arithmetic)

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

Pf: Two parts:

existence: every n can be written as a product of primes ✓

uniqueness: you guys.

ex's ① $200 = 2 \cdot 100$

$= 2 \cdot 2 \cdot 50$

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

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

$= 2^3 \cdot 5^2$

any other product of primes that is not exactly $2 \cdot 2 \cdot 2 \cdot 5 \cdot 5$ will not equal 200.

② $289 = 17 \cdot 17 = 17^2$

③ $97 = 97$ (is prime)

We proved the following theorem day 1, but let's remember the proof (uses FTOA)

Theorem: There are infinitely many primes.

Pf: - Suppose not
- then there are only finitely many primes $p_1, p_2, \ldots, p_N$
- Define
$$P = p_1 \cdot p_2 \cdots p_N + 1$$
- By FTOA, P has a prime factorization
- in particular some prime p divides P
- must have $p = p_j$ for some j $1 \le j \le n$
- So $P = p_j \cdot K$

OTOH: $P = p_j (p_1 p_2 \cdots p_{j-1} p_{j+1} \cdots p_N) + 1$
$= p_j M + 1$

So $p_j K = p_j M + 1$
$p_j (K - M) = 1$ hence $p_j \mid 1$
a contradiction

Counting divisors

ex: Consider

$$1800 = 2 \cdot 900$$
$$= 2 \cdot 2 \cdot 450$$
$$= 2 \cdot 2 \cdot 2 \cdot 225$$
$$= 2 \cdot 2 \cdot 2 \cdot 9 \cdot 25$$
$$= 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5$$
$$= 2^3 \cdot 3^2 \cdot 5^2$$

- if $d \mid 1800$ then any p that divides d divides 1800
- hence only possible factors of d are 2, 3, 5
- and their powers cannot exceed 3, 2, 2 respectively

i.e. if $d \mid 1800$

then

$$d = 2^k 3^l 5^m \quad \text{where } 0 \le k \le 3, \; 0 \le l \le 2, \; 0 \le m \le 2$$

We can use this observation to count # of positive divisors of 1800

- 4 possibilities for k
- 3 poss. for l
- 3 poss for m

so $4 \times 3 \times 3 = 36$ total possibilities for d.

list of divisors of 1800

$2^0 3^0 5^0 = 1$

$2^1 3^0 5^0 = 2$

$2^1 3^1 5^0 = 6$

$\vdots$

(2) Count # of positive divisors of 60:

$60 = 2^2 \cdot 3 \cdot 5$

so if $d \mid 60$ $d = 2^k 3^l 5^m$

$0 \leq k \leq 2$

$0 \leq l \leq 1$

$0 \leq m \leq 1$

$3 \times 2 \times 2 = 12$ possibility

~~$2^0 3^0 5^0 = 1$~~ ~~$2^0 3^0 5^1 = 5$~~

~~$2^1 3^0 5^0 = 2$~~ ~~$2^0 3^1 5^0 = 3$~~

~~$2^1 3^1 5^0 = 6$~~

~~$2^1 3^0 5^1 = 10$~~

~~$2^1 3^1 5^1 = 30$~~

List:

$2^0 3^0 5^0 = 1$
$2^0 3^0 5^1 = 5$
$2^0 3^1 5^0 = 3$
$2^0 3^1 5^1 = 15$
$2^1 3^0 5^0 = 2$
$2^1 3^0 5^1 = 10$
$2^1 3^1 5^0 = 6$
$2^1 3^1 5^1 = 30$
$2^2 3^0 5^0 = 4$
$2^2 3^0 5^1 = 20$
$2^2 3^1 5^0 = 12$
$2^2 3^1 5^1 = 60$

Modular arithmetic

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

- this is an equiv relation
- denote set of equiv classes by $\mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} = \{ [a]_n \mid a \in \mathbb{Z} \}$$

We previously took next result for granted:

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

<u>PR</u>. By the division algorithm
$\exists$ unique integers $q_1, r_1, q_2, r_2 \in \mathbb{Z}$
with $0 \leq r_1 < n$ $0 \leq r_2 < n$
s.t.

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

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

($\Rightarrow$) assume $a \equiv b \pmod{n}$
then $b - a = kn$ for some $k \in \mathbb{Z}$.
hence $kn = (q_2 - q_1) n + r_2 - r_1$
$\Rightarrow (k - (q_2 - q_1)) n = r_2 - r_1$
$\Rightarrow n \mid r_2 - r_1$

but $r_2, r_1 < n$
hence $-n < r_2 - r_1 < n$

but then $n \mid r_2 - r_1 \Rightarrow \underset{=0}{r_2 - r_1}$

i.e. $r_2 = r_1$ ✓

($\Leftarrow$) suppose $r_2 = r_1$
- then $b - a = (q_2 - q_1)n$
- hence $n \mid b - a$
- i.e. $a \equiv b \pmod n$

__ex__ $17 \equiv 37 \pmod 4$

__why__: $17 = 4 \cdot 4 + 1$

$37 = 4 \cdot 9 + 1$

so in fact both $17, 37 \equiv 1 \pmod 4$

Since the only possible remainders when divided by n are $0, 1, \ldots, n-1$ this prop'n justifies another fact we've been using, namely that $\mathbb{Z}/n\mathbb{Z}$ has exactly n equiv classes:

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

on HW you guys proved:

<u>Prop'n</u> Fix $n \in \mathbb{N}$, and $a, b, k \in \mathbb{Z}$.

1. if $a \equiv b \pmod n$ then $a+k \equiv b+k \pmod n$
2. if $a \equiv b \pmod n$ then $ak \equiv bk \pmod n$

This can be generalized slightly:

<u>Theorem</u> (Modular arithmetic lemma).
Fix $n \in \mathbb{N}$. Fix $a, b, k, k' \in \mathbb{Z}$.
and suppose $a \equiv b \pmod n$ and $k \equiv k' \pmod n$

Then
1. $a+k \equiv b+k' \pmod n$
2. $ak \equiv bk' \pmod n$

Pf: you try.

Examples

① $6 \equiv 21 \pmod 5$

and $12 \equiv 2 \pmod 5$

hence $6 + 12 \equiv 21 + 2 \pmod 5$

i.e. $18 \equiv 23 \pmod 5$ ✓

and $6 \cdot 12 \equiv 21 \cdot 2 \pmod 5$

i.e. $72 \equiv 42 \pmod 5$ ✓

② Fix $x \in \mathbb{Z}$.

Then $x + 10 \equiv x + 3 \pmod 7$

because $10 \equiv 3 \pmod 7$

③ Fix $x, y \in \mathbb{Z}$ with $x \equiv y \pmod 7$

Then $x + 3 \equiv y + 3 \pmod 7$

and $x + 10 \equiv y + 3 \pmod 7$

④ subtraction works too!

$x + (-4) \equiv y + (-4) \pmod 7$

i.e. $x - 4 \equiv y - 4 \pmod 7$

and since $-4 \equiv 3 \pmod 7$

could also write

$x - 4 \equiv y + 3 \pmod 7$

(8) if $x \equiv 3 \pmod 7$

then $10x \equiv 30 \pmod 7$

$\equiv 2 \pmod 7$

on the other hand, division on both sides is not allowed in general.

ex: (1) Fix $x \in \mathbb{Z}$.

- Suppose $2x \equiv 1 \pmod 3$
- writing $x \equiv 1/2 \pmod 3$

is meaningless.

(2) - Observe: $15 \equiv 21 \pmod 6$

- if we "divide both sides by 3" we get

$5 \equiv 7 \pmod 6$

which is false.

(3) - Observe: $8 \equiv 22 \pmod 7$

- if we divide both sides by 2 we get

$4 \equiv 11 \pmod 7$

which is true

what gives?

turns out: 2 has a "multiplicative inverse" in $\mathbb{Z}/7\mathbb{Z}$, while 3 does not have such an inverse in $\mathbb{Z}/6\mathbb{Z}$.
↳ more on this later

Prop'n Fix $a, b \in \mathbb{Z}$ and $k, n \in \mathbb{N}$.
if $a \equiv b \pmod{n}$
then $a^k \equiv b^k \pmod{n}$

Pf: use induction + modular arithmetic lemma.
if $a \equiv b \pmod{n}$
then $a^2 \equiv b^2 \pmod{n}$
$\vdots$
$a^k \equiv b^k \pmod{n}$

ex's ① Since $7 \equiv 2 \pmod{5}$
we have
$$7^3 \equiv 2^3 \pmod{5}$$
$$\equiv 8 \pmod{5}$$
$$\equiv 3 \pmod{5}$$

② Find the last ~~two~~ digits of $2033 \cdot 719 + 27$

28

Sol'n: last ~~two~~ digit of this number is exactly the remainder when divided by 10

Observe:

$$2033 \cdot 719 + 27 \equiv 3 \cdot 9 + 7 \pmod{10}$$
$$\equiv 27 + 7 \pmod{10}$$
$$\equiv 34 \pmod{10}$$
$$\equiv 4 \pmod{10}$$

$\Rightarrow$ last digit is 4

and indeed

$$2033 \cdot 719 + 27 = 1{,}461{,}754$$

③ Find the remainder of 2^{57} when divided by 47.

Sol'n:

$$2 \equiv 2 \pmod{47}$$
$$2^2 \equiv 4 \pmod{47}$$
$$(2^4) = (2^2)^2$$
$$\equiv 4^2$$
$$\equiv 16 \pmod{47}$$
$$(2^8) = (2^4)^2$$
$$= 16^2$$
$$\equiv 256$$

$47 \cdot 5 + 21$

$$\equiv 21 \pmod{47}$$

$$2^{16} = (2^8)^2$$
$$\equiv 21^2 \pmod{47}$$
$$= 441$$
$$47 \cdot 9 + 18$$
$$\equiv 18 \pmod{47}$$

$$2^{32} = (2^{16})^2$$
$$\equiv 18^2 \pmod{47}$$
$$= 329$$
$$6 \cdot 47 + 42$$
$$\equiv 42 \pmod{47}$$
$$\equiv -5 \pmod{47}$$

here $2^{37} = 2^{32} \cdot 2^4 \cdot 2^1$
$$\equiv (-5) \cdot 16 \cdot 2 \pmod{47}$$
$$= -160 \rightarrow -4 \cdot 47 + 28$$
$$\equiv 28 \pmod{47}$$

remainder

Multiplicative inverses in $\mathbb{Z}/m\mathbb{Z}$

Def'n Fix $m \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then a is said to have a multiplicative inverse in $\mathbb{Z}/m\mathbb{Z}$ iff $\exists b \in \mathbb{Z}$ s.t.
$$ab \equiv 1 \pmod{m}$$

We sometimes write $b = a^{-1}$ ← not unique but unique up to $\equiv$-class

Prop'n Fix $m \in \mathbb{N}$, $a \in \mathbb{Z}$. Then a has a mult. inv. in $\mathbb{Z}/m\mathbb{Z}$ iff a, m are relatively prime

Pf ($\Rightarrow$) - Assume $\exists b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{m}$.
- Then $m \mid 1 - ab$
- i.e. $\exists k \in \mathbb{Z}$ s.t. $mk = 1 - ab$
- hence $ab + mk = 1$
- Since 1 is a linear combo of a, m must have $\gcd(a, m) = 1$

($\Leftarrow$) - Assume $\gcd(a, m) = 1$
- then $\exists b, k \in \mathbb{Z}$ s.t.
  $ab + mk = 1$
  $\Rightarrow mk = 1 - ab$
  $\Rightarrow m \mid 1 - ab$
  $\Rightarrow ab \equiv 1 \pmod{m}$ $\Rightarrow b = a^{-1}$.

Ex ① - The congruence $6x \equiv 1 \pmod{21}$ has no sol'n.

- such an x would be mult. inv. of 6 in $\mathbb{Z}/21\mathbb{Z}$,
- but $\gcd(6,21) = 3 \neq 1$ so no such x exists

② - $5x \equiv 1 \pmod{21}$ does have a sol'n since $\gcd(5,21) = 1$

- $x = 17$ works since

$$5 \cdot 17 = 85 = 4 \cdot 21 + 1 \equiv 1 \pmod{21}$$

- 17 is not unique solution, but is unique up to equiv. class
- e.g. $-4 \equiv 17 \pmod{21}$

and $5 \cdot (-4) = -20 = (-1) \cdot 20 + 1 \equiv 1 \pmod{21}$

- set of solutions to $5x \equiv 1 \pmod{21}$ is exactly $[17]_{21}$
- might write:

$$[5]_{21} \cdot [17]_{21} \text{ "}=\text{" } [1]_{21}$$

i.e.

$$\forall a \in [5]_{21} \ \forall b \in [17]_{21}$$

we have $a \cdot b \in [1]_{21}$

3. Find all $x \in \mathbb{Z}$ s.t.
$$4x \equiv 5 \pmod 7$$

Sol'n: - 7 is prime, so any $n \in \mathbb{Z}$ not divisible by 7 is rel. prime to 7

- so 4 is rel. prime to 7.
- hence 4^{-1} exists in $\mathbb{Z}/7\mathbb{Z}$.
- indeed
$$2 \cdot 4 \equiv 8 \equiv 1 \pmod 7$$
- can treat multiplication by 2 as "division" by 4 mod 7.

So:
$$4x \equiv 5 \pmod 7$$
$$\Rightarrow 2 \cdot 4x \equiv 2 \cdot 5 \pmod 7$$
$$\Rightarrow 8x \equiv 10 \pmod 7$$
$$\Rightarrow x \equiv 3 \pmod 7$$

hence set of solutions to $4x \equiv 5 \pmod 7$ is exactly
$$[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$$

Prop'n Fix $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. There is a solution to $ax \equiv b \pmod{m}$ iff $\gcd(a,m) \mid b$.

Pf: Let $d = \gcd(a, m)$

($\Rightarrow$) - Assume $ax \equiv b \pmod{m}$ has a sol'n.

- i.e. $\exists \ell \in \mathbb{Z}$ s.t. $a\ell \equiv b \pmod{m}$
- hence $m \mid b - a\ell$
- hence $\exists k \in \mathbb{Z}$ $mk = b - a\ell$

$\Rightarrow a\ell + mk = b$

Now: since $d \mid a$ and $d \mid m$ we have $a = a'd$ $m = m'd$

$\Rightarrow a'd\ell + m'dk = b$

$\Rightarrow d(a'\ell + m'k) = b$

$\Rightarrow d \mid b$ ✓

($\Leftarrow$) Assume $d \mid b$

- then $b = d\ell$ for some $\ell \in \mathbb{Z}$

By Bezout, $\exists k, k' \in \mathbb{Z}$ s.t.

$ak + mk' = d$

$\Rightarrow a\ell k + m\ell k' = d\ell = b$

$\Rightarrow a\ell k = b - m\ell k$
$\equiv b \pmod{m}$

$\Rightarrow x = \ell k$ is a sol'n to $ax \equiv b \pmod{m}$

Ex's ① There is a sol'n to
$6x \equiv 4 \pmod{8}$
since $\gcd(6,8) = 2$
and $2 \mid 4$
check: $x = 2$ works
$6 \cdot 2 = 12 \equiv 4 \pmod{8}$

② There is no sol'n to
$4x \equiv 3 \pmod{8}$
since $\gcd(4,8) = 4$
and $4 \nmid 3$.

Euclidean Algorithm

- Many of the above results depend on knowing $\gcd(a,b)$
- how do we efficiently compute $\gcd(a,b)$?

A: Euclidean Algorithm

Lemma Fix $a,b,q,r \in \mathbb{Z}$.
If $a = bq + r$
then $\gcd(a,b) = \gcd(b,r)$

Pf: Let $d = \gcd(a,b)$
$d' = \gcd(b,r)$

Observe: - Since $a = bq + r$ and $d' | r$ and $d' | b$ we have $d' | a$.
- hence $d' \leq d$ ← greatest common divisor of a,b

OTOH By Bezout $\exists m,n \in \mathbb{Z}$ s.t.

$\cancel{am + bn = d}$

$\cancel{\Rightarrow (bq+r)m + bn = d}$

$\cancel{\Rightarrow rm + bqm + bn = d}$

$\cancel{\Rightarrow rm + b(qm+n) = d}$

~~$\Rightarrow d$ is a linear combination of r and b.~~

$rm + bn = d'$

$\Rightarrow$ since $r = a - bq$ we have

$(a-bq)m + bn = d'$
$\Rightarrow am - bqm + bn = d'$
$\Rightarrow am + b(n - mq) = d'$

$\Rightarrow d'$ is a linear combo of a, b

$\Rightarrow$ again by Bezout that $d \le d'$

$\Rightarrow$ hence $d = d'$ ✓

- This lemma allows us to find $\gcd(a,b)$ by repeatedly "reducing by remainders"

<u>Thm</u> (Euclidean Algorithm)
Fix $a, b \in \mathbb{N}$ with $a \geq b$. Define a finite decreasing sequence by

$$r_0 = a \qquad r_1 = b$$
$$r_j = r_{j+1} q_{j+1} + r_{j+2}$$

where $0 \le r_{j+2} < r_{j+1}$

If $r_n = 0$, define r_n as the last term in the sequence

Then: $r_{n-1} = \gcd(a,b)$.

Pf: follows from lemma, but let's skip and see examples.

Ex 1 Find $\gcd(68, 12)$

Sol'n $a = 68$ $b = 12$

$$\begin{array}{cc} a = 68 & b = 12 \\ \| & \| \\ r_0 & r_1 \end{array}$$

$$\begin{aligned} \overset{r_0}{68} &= \overset{r_1}{12} \cdot 5 + \overset{r_2}{8} \\ 12 &= 8 \cdot 1 + 4 \leftarrow r_3 \\ 8 &= 4 \cdot 2 + 0 \leftarrow r_4 \end{aligned}$$

So thm says:

$\gcd(68, 12)$ = last nonzero remainder $= 4$

Why?

By lemma: $\gcd(68, 12)$
$= \gcd(12, 8)$
$= \gcd(8, 4) = 4$ ✓

1.b Find integers m, n s.t.
$68m + 12n = 4$

Sol'n: - Bezout says m, n exist
- Euclid gives us a way to find them

$$4 = 12 - 8 \cdot 1 \qquad \text{but } 8 = 68 - 12 \cdot 5$$
$$= 12 - (68 - 12 \cdot 5) \cdot 1$$
$$= 12 - 68 \cdot 1 + 12 \cdot 5 \cdot 1$$
$$= -68 \cdot 1 + 12 \cdot 6$$
$$= 68(-1) + 12(6)$$

so $m = -1$ $n = 6$ works

↳ this method of "back substitution" to find m, n is called extended Euclidean algorithm

② Find $k, \ell \in \mathbb{Z}$ s.t.
$64k + 111\ell = 1.$

Sol'n For this to be possible must be that $\gcd(64, 111) \stackrel{?}{=} 1$

Let's do EA:

$$
\begin{aligned}
111 &= 64\cdot 1 + 47\\
64 &= 47\cdot 1 + 17\\
47 &= 17\cdot 2 + 13\\
17 &= 13\cdot 1 + 4\\
13 &= 4\cdot 3 + 1 \quad \leftarrow 1 = \gcd(111, 64)\\
4 &= 4\cdot 1 + 0
\end{aligned}
$$

$$
\begin{aligned}
1 &= 13 - 4\cdot 3 \qquad \text{but } 4 = 17 - 13\cdot 1\\
&= 13 - (17 - 13\cdot 1)\cdot 3\\
&= -17\cdot 3 + 13 + 13\cdot 1\cdot 3\\
&= 17(-3) + 13\cdot 4 \qquad \text{but } 13 = 47 - 17\cdot 2\\
&= 17(-3) + (47 - 17\cdot 2)\cdot 4\\
&= 47\cdot 4 + 17(-11) \qquad \text{but } 17 = 64 - 47\cdot 1\\
&= 47\cdot 4 + (64 - 47\cdot 1)(-11)\\
&= 64(-11) + 47\cdot 4 + 47\cdot 11\\
&= 64(-11) + 47(15) \qquad \text{but } 47 = 111 - 64\cdot 1\\
&= 64(-11) + (111 - 64\cdot 1)(15)\\
&= 111\cdot 15 + 64\cdot(-11) + 64\cdot(-15)\\
&= 111(15) + 64(-26)
\end{aligned}
$$

So $k = -26$ $\ell = 15$ works ✓