Number Theory

The study of the integers \(\mathbb{Z}\) and their arithmetic.

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

Definitions 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 \(k \in \mathbb{N}\).
- Can do a bit better.
Theorem: Fix $n \in \mathbb{N}$. Suppose $n = a \cdot b$ with $a, b \in \mathbb{N}$. Then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Proof: 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.

Solve: $-9 < \sqrt{91} < \sqrt{97} < 10$

- so only need to test prime divisors up to 9.

91: $2, 91, 3, 91, 5, 91$, but 7 divides 91

so 91 is not prime.

97: $2, 97, 3, 97, 5, 97, 7, 97$

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:** $\gcd(42,60) =$

**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:** $\{\pm 1, \pm 2, \pm 5, \pm 6\}$

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

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

(3) $\gcd(-42,60) = 6$. 
Thus: Fix $m, n \in \mathbb{Z}$ and let $d = \gcd(m, n)$. Then $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$

**Proof:** Let $a = \gcd\left(\frac{m}{d}, \frac{n}{d}\right)$
- Then $a | \left(\frac{m}{d}\right)$
  - i.e. $\exists k \in \mathbb{Z}$ s.t. $ak = \frac{m}{d}$
    - hence $(ad)k = m$
    - hence $ad | m$
  - Similarly $\exists k \in \mathbb{Z}$ s.t. $ak = \frac{n}{d}$
    - hence $a | (kd)k = n$
    - hence $a | d$
- Since $a > 1$ and $ad, d$ are common divisors 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 Euclidean Algorithm will give us an efficient way of computing gcds. Hence, we need some preliminary results.

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

(\( q \) is called the quotient of \( b \) when divided by \( a \); \( r \) is the remainder)

**PF:** Define \( S = \{ \text{the NNS of } 0 \} \)
\[ \exists k \in \mathbb{Z} \quad n = b - ak \]

Observe: \( S \neq \emptyset \)
Since \( b - ak \geq 0 \)
whenever \( k \leq \frac{b}{a} \).
(So in fact \( S \) is in \( \mathbb{R} \))

\[ \text{ex: if } b = 5, a = 2 \]
\[ S = \{ \ldots, 5 - 3, 5 - 2, 5 - 1, \ldots \} \]
\[ = \{ \ldots, 7, 5, 3, 1, \ldots \} \]
\[ = \{ 11, 3, 5, 7, \ldots \} \]
- Hence by WOP, \( S \) has a least element \( r \).
- Let \( a, b \in \mathbb{Z} \) be s.t.
  \[ b - aq = r. \]
- Then \( b = aq + r \).

Observe: \( r < a \).

\[ r \neq 0 \text{ and } r < r. \]
- Hence \( r = a + r_1 \),
- where \( r_1 > 0 \).
- Hence \( b = aq + r_1 + r \),
- \[ b = a(q+1) + r_1 \]
- \[ b = a(q+1) + r \]
- \( r_1 \in S \)
- contradiction, since \( r \) was least in \( S \).

So we have proved existence of \( q,r \) s.t. \( b = aq + r \).

Now suppose \( a', r' \in \mathbb{Z} \) with \( a', r' \) and
- \( b = aq' + r' \)

WTS: \( a = a' \) and \( r = r' \)
Observe: -either \( r \geq r' \) or \( r' \geq r \).

Assume WLOG \( r \geq r' \).

Now: \( 0 = b - b = aq + r - (a q' + r') \)
\[ = a(q - q') + (r - r') \]

Hence \( a(q - q') = r - r' \)

Hence \( a | r - r' \)

but \( 0 \leq r - r' < a \) (since \( r < a \))

Hence \( r - r' = 0 \)

i.e. \( r = r' \)

But then \( a(q - q') = 0 \)

Hence \( q = q' \)

Thus proving uniqueness.

Ex's

1. \( a = 15 \quad b = 0.7 \)
   
   Then
   \[ 0.7 = 15 \cdot 7 + 2 \]
   \[ \text{So } q = 7 \quad r = 2 \]

2. \( a = 6 \quad b = -2a \)
   
   Then
   \[ -2a = 6(-8) + 1 \]
   \[ q = -8 \quad r = 1 \]
(3) \( a = 3 \quad b = 12 \)

Then
\[
\begin{align*}
  b &= 3 \cdot 4 + 0, \\
  r &= 0
\end{align*}
\]

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:

- \( \gcd(6, 15) = 3 \)
- Thus 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.
  \[
  6 \cdot (3) + 15 \cdot (-1) = 3 \, \text{ too}
  \]
- thus also says cannot find \( \text{m} \in \mathbb{Z} \) s.t.
  \[
  6m + 15n = 2
  \]
  or \( 6m + 15n = 1 \)

\[\text{Pf. cf. thm.}\]

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

- set of (positive) linear combination of \( a \) and \( b \).

- Observe: \( S \) is not empty since \( |a| + |b| \in S \).
- Hence by WOP, \( S \) has a least \( \text{el.} \) \( \text{d} \).
- Fix \( \text{m,n} \in \mathbb{Z} \) s.t. \( d = am + bn \)
- we want to prove \( d = \gcd(a,b) \)
Claim 1: \( \text{gcd}(a, b) \)

Proof: By the division algorithm, we can write
\[
a = q \cdot d + r
\]
where \( 0 \leq r < d \) (wts \( r = 0 \))

- Hence \( r = a - q \cdot d \)
  \[
  = a - q (a_m + b_n)
  = (1 - q_m)a + (-q_n)b
  
  
- Hence \( r \) is a linear combo of \( a, b \)
- we know \( r > 0 \). If \( r > 0 \) then would have ref.
- but \( r < d \), so this would contradict minimality of \( d \).
- Hence \( r = 0 \)
- Hence \( a = q \cdot d \) i.e. \( \text{gcd}(a) \)

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

Proof: Suppose \( t \in \mathbb{N} \) and \( t\mid a \) and \( t \mid b \).
we will prove tld.

- we have \( \exists k, l \in \mathbb{Z} \) st. \( a = kt \) and \( b = kt \)

- hence \( d = am + bn \)
  \[ = lt(m + kn) \]
  \[ = t(\ell m + kn) \]

- hence \( tld, c \) claimed

- hence \( t \leq d \).

- hence \( d = \gcd(a, b) \).

**Def’n** Fix \( a, b \in \mathbb{Z} \). Then \( a, b \) are called **relatively prime** if \( \gcd(a, b) = 1 \)

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

**Corollary** if \( a, b \in \mathbb{Z} \) are relatively prime, then \( \exists m, n \in \mathbb{Z} \) such that

\[ am + bn = 1 \]

**AF:** 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

\[
7 \cdot 9 + 31 \cdot (-2) = 1.
\]

One useful application of
Bezout's theorem is:

Prop'n (Euclid's lemma)

Fix \( a, b, c \in \mathbb{Z} \). If \( \gcd(ab, c) = 1 \)
and \( a \mid bc \), then actually \( a \mid c \).
Proof: Suppose \( \gcd(ab) = 1 \) and \( a \mid bc \).

- Then \( \exists t \in \mathbb{Z} \) s.t. \( at = bc \)
- By Bezout's Identity \( \exists m, n \in \mathbb{Z} \) s.t. \( am + bn = 1 \)
- Hence
  \[
  c(am + bn) = c
  \]
- \( acm + bcn = c \)
- \( acm + aln = c \)
- \( a(cm + ln) = c \)
- \( a \mid c \)

\[ \checkmark \]

Corollary: Fix \( a, b, p \in \mathbb{Z} \) with \( p \) prime. If \( \gcd(ab) \) with \( p \) prime, then either \( a \mid p \) or \( b \mid p \).

Proof: If \( a \mid p \) we are done
- So suppose \( a \nmid p \)
- Then \( p \) and \( a \) are relatively prime

Why: Since \( p \) prime, \( \gcd(a, p) = 1 \) or \( p \)
- Hence \( p \nmid a \) \( p \nmid a \)
- 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.

\[
\exists! \quad \exists! \quad 200 = 2 \cdot 100 \\
= 2 \cdot 2 \cdot 50 \\
= 2 \cdot 2 \cdot 2 \cdot 25 \\
= 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \\
= 2^3 \cdot 5^2
\]

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 (use FTA).

Theorem: There are infinitely many primes.

Proof: - Suppose not
- then there are only finitely many primes $p_1, p_2, \ldots, p_n$

- Define $P = p_1 p_2 \cdots p_{n+1}$

- By FTA, $P$ has a prime factorization
- In particular, some prime $p$ divides $P$
- must have $p = p_j$ for some $j$
- so $P = p_j k$

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

So $p_j k = p_j M + 1$
$p_j (k - M) = 1$, hence $p_j | 1$

a contradiction
Counting divisors

Ex.: Consider

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

- If \( d \) divides \( 1800 \), then any \( p^a \) in \( d \) divides \( 1800 \).
- There are only possible factors of \( d \) are \( 2, 3, 5 \).
- And their powers cannot exceed \( 3, 2, 2 \) respectively.

i.e., if \( d \) divides \( 1800 \), then
\[ d = 2^k \cdot 3^l \cdot 5^m \quad \text{where} \quad 0 \leq k \leq 3, \quad 0 \leq l \leq 2, \quad 0 \leq m \leq 2 \]

We can use this observation to count the number of positive divisors of \( 1800 \).
- 4 possibilities for k
- 2 poss. for l
- 3 poss. for m

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

List of divisors of 1200

$2^3 \times 3 \times 5^2 = 1$
$2^4 \times 3 \times 5 = 2$
$2^1 \times 3 \times 5^2 = 6$

2. Court # of divisors of 60:

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

So if $d|60$, $d = 2^k \times 3^l \times 5^m$

- $0 \leq k \leq 2$
- $0 \leq l \leq 1$
- $0 \leq m \leq 1$

$3 \times 2 \times 2 = 12$ possibilities
\[ 2^0 \cdot 3^0 \cdot 5^0 = 1 \]
\[ 2^0 \cdot 3^1 \cdot 5^1 = 3 \]
\[ 2^0 \cdot 3^1 \cdot 5^0 = 3 \]
\[ 2^1 \cdot 3^0 \cdot 5^0 = 2 \]
\[ 2^1 \cdot 3^1 \cdot 5^0 = 6 \]
\[ 2^1 \cdot 3^1 \cdot 5^1 = 30 \]
\[ 2^2 \cdot 3^0 \cdot 5^0 = 4 \]
\[ 2^2 \cdot 3^1 \cdot 5^1 = 20 \]
\[ 2^2 \cdot 3^1 \cdot 5^0 = 12 \]
\[ 2^2 \cdot 3^1 \cdot 5^1 = 60 \]

**Modular arithmetic**

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

- This is an equivalence relation.
- Denote set of equivalence classes by \( \mathbb{Z}/n\mathbb{Z} \).

\[ \mathbb{Z}/n\mathbb{Z} = \{ CaJn | \text{ at }\mathbb{Z} \} \]

be previously fact next result
for granted.
Prop'n Fix $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$.

Then $a \equiv b \pmod{n}$ iff $a$ and $b$ have the same remainder when divided by $n$.

PR. By the division algorithm, there are unique integers $q_1, r_1, q_2, r_2 \in \mathbb{Z}$ with $0 \leq r_1, r_2 < n$ such that:

\[
a = q_1n + r_1,
\]

\[
b = q_2n + r_2.
\]

Then

\[
b - a = q_2n + r_2 - (q_1n + r_1) = (q_2 - q_1)n + r_2 - r_1
\]

(\Rightarrow) Assume $a \equiv b \pmod{n}$ then $b - a = kn$ for some $k \in \mathbb{Z}$.

Hence

\[
k = (q_2 - q_1)n + r_2 - r_1
\]

\[
\Rightarrow (k - (q_2 - q_1))n = r_2 - r_1
\]

\[
\Rightarrow n | (r_2 - r_1)
\]

But $r_2, r_1 < n$ hence $-n < r_2 - r_1 < n$.

But then $n | (r_2 - r_1) \Rightarrow r_2 - r_1 = 0$.
\( r_2 = r_1 \checkmark \)

\((\Leftarrow)\) Suppose \( r_2 = r_1 \)
- then \( b-a = (q_2 - q_1)n \)
- hence \( n \parallel b-a \)
- i.e. \( a \equiv b \pmod{n} \)

**Example**

\[ 17 \equiv 37 \pmod{4} \]

**Why:**
\[ 17 = 4 \cdot 4 + 1 \]
\[ 37 = 4 \cdot 9 + 1 \]

So in fact both \( 17 \equiv 37 \equiv 1 \pmod{4} \)

Since the only possible remainders when divided by \( n \) are 0, 1,..., \( n-1 \) they prove this property.

This fact we've been using, namely that
\[ \mathbb{Z}/n\mathbb{Z} \] has exactly \( n \) elements.

\[ \mathbb{Z}/n\mathbb{Z} = \{ [c_0], [c_1], ..., [c_{n-1}] \} \]
on hw you guys proved:

**Prop'n** 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 $ak \equiv bk \pmod{n}$

Thus can be generalized slightly:

**Theorem (Modular Arithmetic)**

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. $ak \equiv bk' \pmod{n}$

*Pt: you try.*
**Example**

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 \(x + 10 \equiv y + 7 \pmod{7}\)

**Subtraction works too:**  

\(x + (-y) \equiv y + (-y) \pmod{7}\)  

i.e. \(x - y \equiv y - y \pmod{7}\)

and since \(-y \equiv 3 \pmod{7}\)  

could also write \(x - y \equiv y + 3 \pmod{7}\)
3. 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.

\[ \text{Ex}: \text{Fix } x \equiv 2. \]
- Suppose \( 2x \equiv 1 \pmod{3} \)
- Writing \( x \equiv y_2 \pmod{7} \)
  is meaningless.

2. - Observe: \( 18 \equiv 21 \pmod{6} \)
   - If we "divide both sides by 2" we get
     \( 9 \equiv 7 \pmod{6} \)
   - 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: \( \mathbb{Z} \) has a "multiplicative inverse" in \( \mathbb{Z}/7\mathbb{Z} \) while \( \mathbb{Z}/6\mathbb{Z} \) does not have such an inverse.

(3) were on this later.

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

Pf: By induction + modular arithmetic lemma.
If \( a \equiv b \pmod{n} \)
then \( a^2 \equiv b^2 \pmod{n} \)

\[ a^k \equiv b^k \pmod{n} \]

Ex\( \text{'}s \) (1) Since \( 7 \equiv 2 \pmod{5} \)
we have \( 7^2 \equiv 2^3 \pmod{5} \)
\[ \equiv 8 \pmod{5} \]
\[ \equiv 3 \pmod{5} \]

(2) Find the last 4 digits of \( 2033 \cdot 719 + 27 \)
Sel'n: last two digits of this number is exactly the remainder when divided by 100

observe:

\[ 2033 \cdot 719 + 27 \equiv 3 \cdot 9 + 7 \pmod{100} \]
\[ \equiv 27 + 7 \pmod{100} \]
\[ \equiv 34 \pmod{100} \]
\[ \equiv 4 \pmod{10} \]

\[ \Rightarrow \text{ last digit is 4} \]

and indeed

\[ 2033 \cdot 719 + 27 = 1461754 \]

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

Sel'zh:

\[ 2 \equiv 2 \pmod{47} \]
\[ 2^2 \equiv 4 \pmod{47} \]
\[ (2^4) = (2^2)^2 \equiv 4^2 \equiv 16 \pmod{47} \]
\[ (2^8) = (2^4)^2 \equiv 16^2 \equiv 256 \]
\[ \equiv 47 \cdot 5 + 21 \]
\[ 2^{16} \equiv (28)^2 \pmod{47} \]
\[ 2^{16} \equiv 2(2) \pmod{47} \]
\[ = 441 \]
\[ 47 - 9 + 4 \]
\[ 18 \pmod{47} \]
\[ 2^{32} \equiv (2^{16})^2 \pmod{47} \]
\[ = 18^2 \pmod{47} \]
\[ = 329 \]
\[ = 6 \cdot 47 + 42 \]
\[ = 42 \pmod{47} \]
\[ \equiv -5 \pmod{47} \]

Here, \[ 2^{37} = 2^{32} \cdot 2^{4} \cdot 2 \]
\[ = (-5) \cdot (6 \cdot 2 \pmod{47}) \]
\[ = -160 \rightarrow -9 \cdot 47 + 26 \]
\[ \equiv 28 \pmod{47} \]

remainder
The multiplicative inverse in \( \mathbb{Z}/m\mathbb{Z} \)

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

We sometimes write \( b = a^{-1} \).

**Prop'n** Fix me \( N, a \in \mathbb{Z}. \) Then \( a \) has a mult. inv. in \( \mathbb{Z}/m\mathbb{Z} \) if \( a, m \) 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 solution.
- 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.

@ -5x \equiv 1 \pmod{21}$ does have a solution since $\gcd(5, 21) = 1$

- $x = 17$ works since
  
  \[ 5 \cdot 17 = 85 \equiv 1 \pmod{21} \]

- 17 is not unique solution, but
  - 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 $\{17\}_n$
  - might write:
    
    \[ \{85\}_n \cdot \{17\}_n = \{0\}_n \]

    \[ \cdots \]
  
  \[ \forall a \in \{85\}_n \forall b \in \{17\}_n \]
  
  \[ \exists c \in \{0\}_n \]

\[ a \cdot b = c \in \{0\}_n \]
3. Find all \( x \in \mathbb{Z} \) s.t. \( 4x \equiv 5 \pmod{7} \)

Solve: - 7 is prime, so any \( n \in \mathbb{Z} \) not divisible by 7 is rel. prime to 7.
- so \( y \) is rel. prime to 7.
- hence \( y \) exists in \( \mathbb{Z}/7\mathbb{Z} \).
- indeed
\[
2 \cdot y \equiv 8 \equiv 1 \pmod{7}
\]
- can treat \( y \) as "division" by \( 2 \pmod{7} \).

\[
\begin{align*}
8 & \cdot x \equiv 5 \pmod{7} \\
\Rightarrow & \ 2 \cdot 4x \equiv 2 \cdot 5 \pmod{7} \\
\Rightarrow & \ 8x \equiv 10 \pmod{7} \\
\Rightarrow & \ x \equiv 3 \pmod{7}
\end{align*}
\]

Hence set of solutions to \( 4x \equiv 5 \pmod{7} \) is
as \( x \equiv 3 \pmod{7} \)
\[
\mathbb{Z}/7\mathbb{Z} = \{ 3 \cdot 7, -43, 10, 17, \ldots \}
\]
Prop'n Fix \(a, b \in \mathbb{Z}\) and \(n \in \mathbb{N}\).

There is a solution to \(ax \equiv b \pmod{m}\)

if \(\gcd(a, n, m) \mid b\).

\[\text{Pf.:}\] \(\text{Let } d = \gcd(a, n, m)\)

\((\Rightarrow)\) Assume \(ax \equiv b \pmod{m}\) has a solution.
- \(\Rightarrow \exists t \in \mathbb{Z} : st \cdot al \equiv b \pmod{m}\)
- \(\text{Hence } m \mid b - al\)
- \(\text{Hence } \exists k \in \mathbb{Z} \text{ such that } mk = b - al\)
- \(\Rightarrow al + mk = b\)

Now: since \(dl \mid a\) and \(dl \mid m\),
we have \(a = xd, m = yd\)

\(\Rightarrow \) \(c'dl + mk = b\)

\(\Rightarrow d(c'e + m'k) = b\)

\(\Rightarrow d \mid b\)

\((\Leftarrow)\) Assume \(d \mid b\).
- Then \(b = dl\) for some \(l \in \mathbb{Z}\).

By above, \(\exists k, k' \in \mathbb{Z} \text{ s.t. }\)
\(ak + mk' = d\)

\(\Rightarrow ak + mk' = dl = b\)
\[ a + k = b - m + k \]
\[ \equiv b \pmod{m} \]

\[ \Rightarrow \ x = ek + 0 \text{ soln to } ax \equiv b \pmod{m} \]

**Case 1:**

There is a soln to
\[ 6x \equiv 4 \pmod{8} \]

Since \( \gcd(6,8) = 2 \)

and \( 2|4 \)

Check: \( x = 2 \) works

\[ 6 \cdot 2 = 12 \equiv 4 \pmod{8} \]

**Case 2:**

There is \( \text{no soln to} \)

\[ 4x \equiv 3 \pmod{8} \]

Since \( \gcd(4,8) = 4 \)

and \( 4 \not| 3 \).
Euclidean Algorithm

- Many of the above results depend on knowing \( \text{gcd}(a, b) \).
- How do we efficiently compute \( \text{gcd}(a, b) \)?

A: Euclidean Algorithm

**Lemma** Fix \( a, b, q, r \in \mathbb{Z} \).

If \( a = bq + r \)

then \( \text{gcd}(a, b) = \text{gcd}(b, r) \)

**Proof:** \( \text{Let } d = \text{gcd}(a, b) \)
\( \text{and } d' = \text{gcd}(b, r) \)

Observe: Since \( a = bq + r \) and \( d' \) divides both \( r \) and \( b \), we have \( d' \) divides \( a \).

Hence \( d' = d \). Greatest common divisor of \( a, b \).

Written by [Author Name] S.L.
\[ rm + bn = d' \]

(\( \Rightarrow \) since \( r = a - bq \) where \( (a - bq) m + bn = d' \))

\[ am - bqm + bn = d' \]

\[ am + b(n - bq) = d' \]

\( \Rightarrow \) \( d' \) is a linear combo of \( a, b \)

\( \Rightarrow \) again by Bezout that \( d \leq d' \)

\( \Rightarrow \) hence \( d = d' \)

\( \checkmark \)

Thus Lemma allows us to find \( \gcd(a, b) \) by repeatedly “dividing by remainders”

**Theorem (Euclidean Algorithm)**

Fix \( a, b \in \mathbb{N} \) with \( a > b \).

Define a finite decreasing sequence by

\[ r_0 = a \quad r_1 = b \]

\[ r_j = r_{j+1} q_{j+1} + r_{j+2} \]

where \( 0 \leq r_{j+2} < r_{j+1} \)
If \( r_n = 0 \), define \( r_n \) as the last term in the sequence.

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

**Proof:** Follows from Lemma b) (we skip and see examples).

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

\[
\begin{align*}
\text{So } \kappa_n & = 68 \quad b = 12 \\
\quad & r_0 = r_1 \\
68 & = 12 \cdot 5 + 8 \\
12 & = 8 \cdot 1 + 4 \quad r_2 \\
8 & = 4 \cdot 2 + 0 \quad r_3
\end{align*}
\]

So then says:

\[
\gcd(68, 12) = \text{last nonzero remainder} = 4
\]

Why?

By Lemma: \( \gcd(68, 12) = \gcd(12, 8) = \gcd(8, 4) = 4 \)
1.5 Find integers m, n s.t. 
\[ 68m + 12n = 4 \]

**Soln:** Bezout says m, n exist.
- Euclid gives us a way to find m, n.

\[ 4 = 12 - 8 \cdot 1 \quad \text{but} \quad 8 = 68 - 12 \cdot 5 \]
\[ = 12 - (68 - 12 \cdot 5) \cdot 1 \]
\[ = 12 - 68 \cdot 1 + 12 \cdot 5 \cdot 1 \]
\[ = 68 \cdot 1 + 12 \cdot 6 \]
\[ = 68(-1) + 12(6) \]

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.
\[ 64k + 111 \ell = 1. \]

**Soln:** For this to be possible, \( \gcd(64, 111) = 1 \)
Let's do EA:

\[ 111 = 64 \cdot 1 + 47 \]
\[ 64 = 47 \cdot 1 + 17 \]
\[ 47 = 17 \cdot 2 + 13 \]
\[ 17 = 13 \cdot 1 + 4 \]
\[ 13 = 4 \cdot 3 + 1 \]

\[ \text{gcd}(111, 64) = 1 \]
\[ 4 = 4 \cdot 1 + 0 \]

\[ 1 = 13 - 4 \cdot 3 \]
\[ \text{but } 4 = 17 - 13 \cdot 1 \]

\[ = 13 - (17 - 13 \cdot 1) \cdot 3 \]
\[ = -17 \cdot 3 + 13 + 13 \cdot 1 \cdot 3 \]
\[ = -17(3) + 13 \cdot 4 \]
\[ \text{but } 13 = 47 - 17 \cdot 2 \]
\[ = 47(3) + (47 - 17 \cdot 2) \cdot 4 \]
\[ = 47 \cdot 4 + 17(-11) \]
\[ \text{but } 17 = 64 - 4 \cdot 1 \]
\[ = 47 \cdot 4 + (64 - 4 \cdot 4 \cdot 1) \cdot (-11) \]
\[ = 64(-11) + 47 \cdot 4 + 47 \cdot 11 \]
\[ = 64(-11) + 47(15) \]
\[ \text{but } 47 = 1 \cdot 64 \]
\[ = 64(-11) + (1 \cdot 64 - 64 \cdot 1) \cdot 15 \]
\[ = 64(-11) + 64 \cdot (-11) + 64 \cdot (-15) \]
\[ = 111(15) + 64(-26) \]

So \( k = -26 \) and \( \ell = 15 \) work.