INTRODUCTION TO NUMBER THEORY

INSTRUCTOR: NUNO FERITAS (nuno@math.ubc.ca)
CLASS: MON WED FRI 11:00 - 12:00 (460 LSK)
OFFICE HOURS: MON WED 12:30 - 14:00
WEB: www.math.ubc.ca/~nuno/math312w16.html

GRADING SCHEME:
- 40% for best 2 out of 3 midterms
- 60% for final exam
- 20% of problems are from problem sets

DATES FOR MIDTERMS: 30th September, 28th of October and 15th of November
Q: What do we study in number theory?

- We will focus on the study of the
  integer numbers \( \mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots \} \)

- Divisibility / Prime Numbers
- Congruences
- Applications (ex: Cryptography)

**Fact:** The integers \( \mathbb{Z} \) satisfy the Well Ordering Principle (WOP), that is
  "Every non-empty subset \( S \subseteq \mathbb{Z}^+ \) of positive integers contains a smallest element"

  Ex: 2 is the smallest even number.

- The WOP is equivalent to induction
- The WOP does not hold for other sets of numbers like \( \mathbb{Q} \) or \( \mathbb{R} \).

  Consider, for example \( S = \{ \frac{1}{n} : n \in \mathbb{Z}_{>0} \} \)
Divisibility

Definition: Let \( a, b \in \mathbb{Z} \). We say that 
\( a \) divides \( b \) if there exists an integer 
\( c \in \mathbb{Z} \) such that \( b = a \cdot c \)

Notation: \( a \mid b \), \( a \nmid b \)

\( a \) is a factor of \( b \)
\( b \) is a multiple of \( a \)

Example:
- \( 3 \mid 6 \) since \( 6 = 3 \cdot 2 \) with \( c = 2 \)
- \( 3 \nmid 5 \) since \( 5 = 3 \cdot \frac{5}{3} \) with \( c = \frac{5}{3} \notin \mathbb{Z} \)
- \( a = 1 \cdot a = (-1)(-a) \Rightarrow \pm 1, \pm a \) divide \( a \)
- \( 0 = a \cdot 0 \Rightarrow a \mid 0 \ \forall a \in \mathbb{Z} \)
- \( b = 0 \cdot c \Rightarrow b = 0 \) i.e. only \( 0 \) is divisible by \( 0 \)

Remark: \( 0 \mid 0 \) but \( \frac{0}{0} \) makes no sense

Be careful!
**Proposition:** If \( a \mid b \) and \( c \mid d \) then \( a \mid c \)

**Proof:** We have \( b = a \cdot b_0 \) and \( d = c \cdot d_0 \)

\[
\begin{align*}
c &= b \cdot c_0 = (a \cdot b_0) \cdot c_0 = a \cdot (b_0 \cdot c_0) \\
\Rightarrow a \mid c
\end{align*}
\]

\[\square\]

**Proof:** Let \( a, b, c, m, n \in \mathbb{Z} \)

If \( c \mid a \) and \( c \mid b \) then \( c \mid ma + nb \)

**Proof:** We have \( a = c \cdot a_0 \) and \( b = c \cdot b_0 \)

\[
\begin{align*}
ma + nb &= m(c \cdot a_0) + n(c \cdot b_0) \\
&= c(ma_0 + nb_0) \\
\Rightarrow c \mid ma + nb
\end{align*}
\]

\[\square\]

**Notation:** An expression of the form \( ma + nb \)

is called a (integral) linear combination of \( a \) and \( b \)

**Corollary:** \( c \mid a \), \( c \mid b \) \( \Rightarrow \ c \mid a + b \) and \( c \mid a - b \)
THEOREM (DIVISION ALGORITHM / DIVISION WITH REMINDER)

Let \( n, a \in \mathbb{Z} \) with \( a > 0 \),

then there are \underline{unique} \( q, r \in \mathbb{Z} \) such that
\[
    n = q \cdot a + r, \quad 0 \leq r < a
\]

\textbf{Notation:} \( q \) is \text{the quotient}, \( r \) is \text{the remainder}

\textbf{Dem:} \( a \mid n \iff r = 0 \)

\textbf{Example:}

- \( 6 = 2 \cdot 3 + 0 \), \( n = 6 \), \( a = 3 \), \( q = 2 \), \( r = 0 \)
- \( n = 30 \), \( a = 7 \)
  \[
  30 = 4 \cdot 7 + 2, \quad q = 4, \quad r = 2
  \]

\textbf{Proof:} Let \( n \in \mathbb{Z} \) and \( a \in \mathbb{Z}_{>0} \).

\textbf{Existence}.

Consider \( T = \{ n \in \mathbb{Z}_{>0} \mid \exists k \in \mathbb{Z}: n = n - ka \} \)

the set of non-negative numbers that differ from \( n \) by a multiple of \( a \).

\( T \neq \emptyset \) by taking \( k \) negative enough since \( a > 0 \)
Let $b = \min \mathcal{T}$ which exists by WOP.

We have $0 \leq b = n - qa$ for some $q \in \mathbb{Z}$.

By the definition of $\mathcal{T}$.

Thus we have found candidates for $b$ and $q$.

Suppose $b > a$. Then $b - a = n - (q + 1)a \geq 0$.

$\Rightarrow b - a \in \mathcal{T}$ and $0 \leq b - a < b$ (since $a > 0$).

Which is a contradiction with minimality of $b$.

Thus $b < a$ as desired.

**Uniqueness**

Suppose $n = q \cdot a + b = q' \cdot a + b'$

with $0 \leq b, b' < a$.

Suppose $b = b'$. Then $(q - q')a = 0 \Rightarrow q = q'$.

We will show $b = b'$.

Suppose $b' > b$. Then $b' - b = (q' - q)a > 0$.

$\Rightarrow b' - b > a$ but $a > b' > b' - b > a$, a contradiction!

By symmetry, we get a contradiction to $b > b'$.

Thus $b = b'$ as desired.

\[\square\]
**Greatest Common Divisor**

**Def.** Let \( a, b \in \mathbb{Z} \), with at least one not zero. The GCD of \( a \) and \( b \) is the largest positive integer \( d \) such that \( d \mid a \) and \( d \mid b \).

**Notation.** \((a, b) = \text{GCD}(a, b)\)

If \((a, b) = 1\) we say \( a, b \) are **coprime**

**Defn:** \((-a, b) = (a, -b) = (-a, -b)\) so we can restrict the discussion to non-negative \(a, b\).

**Ex:** \(a = 12, b = 18\) have common positive divisors \(\{1, 2, 3, 6\}\) \(\Rightarrow (12, 18) = \text{GCD}(12, 18) = 6\)

**Thm:** Let \(a > 0\), then \((a, 0) = a\)

**Thm:** Let \(a, b \in \mathbb{Z}\), not both zero. Then \((a, b)\) is the smallest positive integer of the form \(ax + by\) with \(x, y \in \mathbb{Z}\).

**Cor:** If \((a, b) = 1\) then

\[1 = ax + by\] for some \(x, y \in \mathbb{Z}\)
Ex.: \((5,7) = 1\) AND \(1 = 10 \cdot 5 + (-7) \cdot 7\)

\((3,15) = 3\) AND \(3 = 3 \cdot 6 + (-1) \cdot 15\)

But also \(3 = 3 \cdot 1 + 0 \cdot 15\)

**Proof:** Let \(a, b \in \mathbb{N}_{\geq 0}\) not both zero.

Consider \(I = \{ax + by \mid x, y \in \mathbb{Z}\}\)

the set of all integral linear combinations of \(a, b\).

- **Note:** \(I\) is closed for addition and scalar multiplication

\[
\begin{align*}
(ax_0 + by_0) + (ax_1 + by_1) &= a(x_0 + x_1) + b(y_0 + y_1) \\
\alpha(ax_0 + by_0) &= a(\alpha x_0) + b(\alpha y_0) \quad , \alpha \in \mathbb{Z}
\end{align*}
\]

- \(\pm a, \pm b \in I \Rightarrow I\) contain positive integers

- Let \(d = ax_0 + by_0\) for the smallest positive integer \(d\) in \(I\) by the WOP

\[
\text{Want: } d = \text{GCD}(a, b)
\]

- Let \(N\) be a common divisor of \(a\) and \(b\)

Then \(N \mid ax + by \forall x, y \in \mathbb{Z}\).

In particular \(N \mid d\).

Thus \((a, b) \mid d\) hence \((a, b) \leq d\)
We will show that $d$ divides all the elements of $I$.

We conclude $d | a$, $d | b$ hence $d \leq (a, b)$

Thus $d = (a, b)$ by the other inequality.

$\Rightarrow$ Let $n \in I$. Dividing $n$ by $d$ we get

$$n = q \cdot d + r, \quad 0 \leq r < d, \quad q \in \mathbb{Z}$$

Then $r = n - q \cdot d \in I$ because $I$ is closed

Thus $r = 0$ otherwise $I$ would contain a positive number smaller than $d$.

$\Rightarrow d | n \Rightarrow d | a$, $d | b$, and $d \leq (a, b)$}

Corollary: Every common divisor of $a$, $b$ divides $(a, b)$

Proof: Let $d_0 \mid a$ and $d_0 \mid b$.

Then $(a, b) = ax + by = d_0(a'x) + d_0(b'y) = d_0(a'x + b'y) \Rightarrow d_0 \mid (a, b)$
Rem: Computing \((a, b)\) by listing all the common divisors is a bad algorithm.

We will learn the "Euclidean Algorithm" for this.

Def: Let \(a_1, a_2, \ldots, a_n \in \mathbb{Z}\) not all zero.

The \(\text{GCD}(a_1, \ldots, a_n)\) is the largest positive integer dividing all \(a_i\).

If \((a_i, a_j) = 1\) \(\forall i \neq j\), we say that the \(a_i\) are pairwise coprime.

Ex: \((24, 60, 49) = 1\) (they are coprime)

But \((24, 60) = 12\) so they are not pairwise coprime.
REPRESENTATION OF INTEGERS

100 = 10^2 + 0 \cdot 10^1 + 0 \cdot 10^0

37465 = 3 \cdot 10^4 + 7 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0

**THM:** Let \( b \in \mathbb{Z}_{\geq 2} \). Every positive integer \( N \in \mathbb{N}_{>0} \) can be uniquely written in "base \( b \)". That is,

\[ N = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \ldots + a_1 \cdot b + a_0 \]

where \( a_k \neq 0 \) and \( 0 \leq a_i \leq b-1 \).
REPRESENTATION OF INTEGERS

- We normally work in "base 10", for example $100 = 10^2$.
  
  $37465 = 3 \cdot 10^4 + 7 \cdot 10^3 + 4 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$

- Computers often use "base 2" but other bases can be used.

**Theorem:** Let $b \in \mathbb{Z}_+$. Every positive integer $N$ can be uniquely written in "base $b". That is,

$N = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$

where $a_k \neq 0$ and $0 \leq a_i \leq b-1$

**Proof (Strong Induction):** We first prove existence.

**Base:** $N \leq b-1$; take $k=0$ and $a_0 = N$

**Step:** Suppose $N > b$. The Division Algorithm gives $N = b \cdot q + a_0$ with $0 \leq a_0 \leq b-1$.

Note that $1 \leq q < N$ hence by Induction Hypothesis $q = c_k b^k + c_{k-1} b^{k-1} + \ldots + c_0$

with $c_k \neq 0$ and $0 \leq c_i \leq b-1$. 

\[
N = \lambda \cdot q + a_0 \\
= \lambda (C_k \lambda^k + C_{k-1} \lambda^{k-1} + \ldots + C_0) + a_0 \\
= C_k \lambda^{k+1} + \ldots + C_0 \lambda + a_0
\]

We can take \( K = \lambda + 1 \) and \( a_i = C_{i-1} \) for \( i = 1, \ldots, K \).

**Uniqueness**

Suppose \( N = a_k \lambda^k + \ldots + a_1 \lambda + a_0 = a_k' \lambda^k + \ldots + a_1' \lambda + a_0' \)

where \( a_k, a_k' \neq 0 \) and \( 0 \leq a_i, a_i' \leq \lambda - 1 \).

1. If \( N \leq \lambda - 1 \) then \( K = k = 0 \) and \( a_0' = a_0 = N \).
2. Suppose \( N \geq \lambda \). Then \( a_0 = a_0' \) by the division algorithm since both are the remainders of \( N \) divided by \( \lambda \).

We have

\[
N - a_0 = a_k \lambda^{k-1} + \ldots + a_2 \lambda + a_1 = a_k' \lambda^{k-1} + \ldots + a_2' \lambda + a_1'
\]

and by induction hypothesis we have

\( a_k = a_k', \ldots, a_1 = a_1' \).

**Notation:** \( N = a_k \lambda^k + \ldots + a_1 \lambda + a_0 \) is denoted \( (a_k a_{k-1} \ldots a_0)^N \).

**Ex:** \( N = 67 \)

\( \lambda = 10 \rightarrow 67 = 6 \cdot 10 + 7 \cdot 10^0 \rightarrow (67)_{10} \)

\( \lambda = 5 \rightarrow 67 = 2 \cdot 5^2 + 3 \cdot 5 + 2 \rightarrow (232)_{5} \)

\( \lambda = 3 \rightarrow 67 = 2 \cdot 3^2 + 2 \cdot 3 + 1 \rightarrow (221)_{3} \)
THE EUCLIDEAN ALGORITHM

- The method we know so far to compute \( \text{GCD}(a, b) \) consists of finding all the common divisors of \( a, b \).

**Ex:** \( a = 30, b = 18 \)

\[
\text{DIV}(30) = \{9, 2, 3, 5, 6, 10, 15, 30\}
\]

\[
\text{DIV}(18) = \{1, 2, 3, 6, 9, 18\}
\]

Common divisors \( \{1, 2, 3, 6\} \Rightarrow (30, 18) = 6 \)

- This method is very inefficient, we will learn the Euclidean Algorithm which is much better.

But first we need the following auxiliary lemma

**Lemma:** Let \( a, b \in \mathbb{Z}^+ \) with \( a \geq b > 0 \).

Suppose \( a = q \cdot b + R \) with \( q, R \in \mathbb{Z}^+ \)

Then \( (a, b) = (b, R) \)

**Proof:** Let \( c \mid a \text{ and } c \mid b \)

We have \( R = a - q \cdot b \Rightarrow c \mid R \)

Thus \( c \) is a common divisor of \( b \) and \( R \)
Let \( c \mid R \) and \( c \mid b \).

Then \( c \) divides \( a = bq + R \) thus it is a common divisor of \( a, b \). We conclude that \( a, b \) have the same set of common divisors of \( b, R \).

In particular \( (a, b) = (b, R) \) \( \Box \)

**The Euclidean Algorithm:**

Let \( a, b \in \mathbb{Z} \) with \( a > b > 0 \). By the division algorithm, there exist \( q_1, R_1 \in \mathbb{Z} \) such that

\[
a = bq_1 + R_1,
\]

\( 0 \leq R_1 < b \).

If \( R_1 > 0 \) there exists (again by the Div. Alg.) \( q_2, R_2 \in \mathbb{Z} \) such that

\[
b = R_1 q_2 + R_2,
\]

\( 0 \leq R_2 < R_1 \).

If \( R_2 > 0 \), there exist \( q_3, R_3 \in \mathbb{Z} \) such that

\[
R_1 = R_2 q_3 + R_3,
\]

\( 0 \leq R_3 < R_2 \).

Continue this process. Then \( R_N = 0 \) for some \( N \).

If \( N > 1 \) then \( (a, b) = R_{N-1} \).

If \( N = 1 \) then \( (a, b) = b \).
Proof: Note that \( R_1 > R_2 > R_3 > \ldots \) and \( R_1 > 0 \)

If \( R_n = 0 \ \forall n \) then we obtain a

strictly decreasing sequence of positive

integers which is impossible.

Thus \( R_n = 0 \) for some \( n \geq 1 \).

If \( n > 1 \) repeated applications of the

Lemma gives

\[
(a, b) = (b, R_1) = (R_1, R_2) = \ldots = (R_{n-1}, R_n) = (R_{n-1}, 0) = R_{n-1}, \quad \text{as desired}
\]

If \( n = 1 \) then \( R_1 = 0 \) and \( b \mid a \)

Thus \( (a, b) = b \)

\[
\]

Example: \( a = 30, \ b = 18 \)

Step 1) \( 30 = 1 \cdot 18 + 12 \Rightarrow (30, 18) = (18, 12) \)

Step 2) \( 18 = 1 \cdot 12 + 6 \Rightarrow (18, 12) = (12, 6) \)

Step 3) \( 12 = 2 \cdot 6 + 0 \Rightarrow (12, 6) = (6, 0) = 6 \)

Thus \( (30, 18) = 6 \)
Example: Compute \((803, 154)\)

1) \(803 = 154 \cdot 5 + 33 \rightarrow (803, 154) = (154, 33)\)

2) \(154 = 33 \cdot 4 + 22 \rightarrow (154, 33) = (33, 22)\)

3) \(33 = 22 \cdot 1 + 11 \rightarrow (33, 22) = (22, 11)\)

4) \(22 = 11 \cdot 2 + 0 \rightarrow (22, 11) = (11, 0) = \n\)

Thus \((803, 154) = 11\)
Euclidean Algorithm Continued

Example: Compute \((803, 154)\)

1) \(803 = 154 \cdot 5 + 33 \Rightarrow (803, 154) = (154, 33)\)

2) \(154 = 33 \cdot 4 + 22 \Rightarrow (154, 33) = (33, 22)\)

3) \(33 = 22 \cdot 1 + 11 \Rightarrow (33, 22) = (22, 11)\)

4) \(22 = 11 \cdot 2 + 0 \Rightarrow (22, 11) = (11, 0) = 11\)

Thus \((803, 154) = 11\)

Recall: \((a, b)\) is the smallest positive integer of the form \(ax_0 + by_0\) with \(x_0, y_0 \in \mathbb{Z}\).

Question: Is there a method to find \(x_0, y_0\)?

Yes! We use **back substitution**

Ex: \((803, 154) = 11\)

\[= 33 - 22 = 33 - (154 - 33 \cdot 4) =\]

\[= 33 \cdot 5 - 154 = (803 - 154 \cdot 5) \cdot 5 - 154\]

\[= 803 \cdot 5 - 154 \cdot 26 = 803 \cdot 5 + 154 (-26)\]
We conclude
\[(a, b) = 14, \quad a = 803, \quad b = 154\]
\[x_0 = 5 \quad \text{AND} \quad y_0 = -26\]

**Example:** Compute \((154, 35)\) and \(x_0, y_0\)

First apply the EA

1) \(154 = 4 \cdot 35 + 14 \Rightarrow (154, 35) = (35, 14)\)

2) \(35 = 2 \cdot 14 + 7 \Rightarrow (35, 14) = (14, 7)\)

3) \(14 = 2 \cdot 7 + 0 \Rightarrow (14, 7) = (7, 0) = 7\)

Now back substitution

\[7 = 35 - 2 \cdot 14 = 35 - 2(154 - 4 \cdot 35)\]

\[= 35 \cdot 9 + 154 \cdot (-2) = 154 \cdot (-2) + 35 \cdot 9\]

So

\[x_0 = -2 \quad \text{AND} \quad y_0 = 9\]
Prime Numbers

We have learned division but there are numbers that cannot be divided. They work as "building blocks".

Def: Let \( p \in \mathbb{Z}^+ \). Then \( p \) is a prime if its only positive divisors are 1 and \( p \).

A number \( n > 1 \) which is not prime is composite.

Ex: 2, 3, 5, 7 are primes.

\[ 6 = 2 \cdot 3 \] is composite.

Here is a great theorem.

Thm (Euclid):

There are infinitely many primes.

For its proof we need the following lemma.

Lemma: Every integer \( n > 1 \) has a prime divisor.

Proof: Suppose \( n > 1 \) is the smallest integer without prime divisors.

Since \( N/N \) we know \( n \) is not prime. Thus \( n \) is composite and

\[ N = a \cdot b \text{ with } 1 < a, b < N \]

Minimal of \( N \Rightarrow \exists p | a \Rightarrow p | N \), a contradiction.
Proof (Euclid): Suppose there are only finitely many primes \( p_1, \ldots, p_n \).

Consider the number \( N = p_1 p_2 \cdots p_n + 1 \).

By the lemma \( N \) has a prime divisor \( p \).

Hence \( p = p_i \) for some \( i \).

Thus \( p \mid N - p_1 p_2 \cdots p_n = 1 \), impossible.

Question: How are primes distributed?

**THM (Prime Number Theorem):**

Let \( \pi(x) \) be the function giving the number of primes \( \leq x \). Then \( \pi(x) \sim \frac{x}{\log x} \) as \( x \to \infty \).

**THM (Dirichlet Density THM):**

Let \( a, b \in \mathbb{Z} \) satisfy \( (a, b) = 1 \).

Then there are infinitely many primes in the arithmetic progression \( a + kb \).
Question: How can we decide if a given number is prime?

Proposition: Let \( N \) be composite. Then \( N \) has a prime divisor \( p \leq \sqrt{N} \).

Proof: We have \( N = a \cdot b \), \( 1 < a, b < N \).

WLOG suppose \( b \geq a \).

Suppose \( a > \sqrt{N} \). Then \( N = a \cdot b > \sqrt{N} \cdot \sqrt{N} = N \).

Thus \( a \leq \sqrt{N} \) and all prime factors of \( a \) are factors of \( N \leq \sqrt{N} \).

So to decide if \( N \) is prime/composite we have to test divisibility by primes up to \( \sqrt{N} \).

This is not efficient. We will see better later.

The following is why primes are building blocks.

THM (Fundamental Theorem of Arithmetic): Every \( N \in \mathbb{Z} \), \( N \neq 0, 1 \) can be written as \( N = \pm p_1^{e_1} \cdots p_k^{e_k} \) in a unique way, where \( p_i \) are different primes and \( e_i \geq 1 \).

(THIS IS UP TO REORDERING \( p_i \)).
Remark: We may be very familiar with this thing, but it is a non-trivial statement that requires proof.

It is not true in different "systems of numbers". For example, if we consider the universe of even numbers we have that 6, 10, 30, 50 are "primes" (i.e., cannot be decomposed further) and

\[ 300 = 10 \cdot 30 = 6 \cdot 50 \text{ so the decomposition is not unique!} \]

We need the following lemma for the proof of FTA:

Lemma: Let \( a, b \in \mathbb{Z}^+ \) satisfy \( (a, b) = 1 \) and \( a \mid bc \). Then \( a \mid c \).

Proof: Since \( (a, b) = 1 \) we have

\[ a = ax + by \text{ for some } x, y \in \mathbb{Z} \]

\[ c = cax + (cb)y = a(cx) + (a)(by) \]

\[ = a(cx + ky) \implies a \mid c \]
**Theorem (FTA):**

Every $N \in \mathbb{Z}$, $N \neq 0, 1$ can be written as

$$N = \pm p_1^{e_1} \cdots p_k^{e_k}$$

in a unique way

where $p_i$ are distinct primes and $e_i > 1$.

(Up to reordering)

---

**Lemma:** Let $a, b \in \mathbb{Z}_{>0}$ satisfy $(a, b) = 1$, $a \mid b \cdot c$.

Then $a \mid c$.

**Proof:** Since $(a, b) = 1$ we have

$$1 = ax + by \quad \text{for some } x, y \in \mathbb{Z}$$

$$\Rightarrow c = cax + cby = a(cx) + (ak)y$$

$$= a(\text{ex} + \text{ky}) \Rightarrow a \mid c$$

---

**Remark:** The condition $(a, b) = 1$ is necessary.

Take $a = 6$, $b = 3$, $c = 4$.

Then $6 \mid 3 \cdot 4 = 12$ but $6 \nmid 4$. 

---
Corollary: Suppose $p | a_1 \ldots a_n$. Then $p | a_i$ for some $i$.

Proof: Induction on $N$

$N=1$: $p | a_1$ \implies $p | a_1$ \checkmark

$N+1$: Suppose $p | a_1 \ldots a_n a_{n+1}$

Then $p | (a_1 \ldots a_n) \cdot a_{n+1}$ and by the lemma

$p | a_1 \ldots a_n$ or $p | a_{n+1}$

[Note that if $(p, a_1 \ldots a_n) \neq 1$ then $p | a_1 \ldots a_n$]

In the second case we are done.

In the first case by induction we see $p | a_i$ for some $i = 1, \ldots, N$. \qed
Proof of ETA: Let \( N \in \mathbb{Z}_+ \).

**Existence**

1. Suppose \( N \) is prime.

   Take \( P_1 = N, \ e_1 = 1 \) and we are done.

2. Suppose \( N \) is composite.

   Assume \( N \) is the smallest integer without a prime decomposition. We have

   \[ N = a \cdot b, \ 1 < a, b < N \]

   and \( a = p_1 \cdots p_k, \ b = q_1 \cdots q_k \) (repetitions allowed) by minimality of \( N \).

   Thus \( N = a \cdot b = p_1 \cdots p_k \cdot q_1 \cdots q_k \) is a prime decomposition, contradiction!
**Uniqueness**

Suppose \( N = p_1 \cdots p_k = q_1 \cdots q_l \) are two prime decompositions. After cancelling common factors and relabeling, we get

\[ p_1 \cdots p_k = q_1 \cdots q_l, \]

where \( p_i \neq q_j \quad \forall i, j \)

By the corollary \( p_i | q_j \) for some \( j \)

which contradicts \( p_i \neq q_j \).

We conclude there are no prime factors left after the cancellation so the decompositions are equal. \( \square \)
Ex: \[ 756 = 2 \cdot 378 = 2 \cdot 2 \cdot 189 \]
\[ = 2 \cdot 2 \cdot 3 \cdot 6 \cdot 3 = 2 \cdot 3 \cdot 7 \cdot 3 \cdot 3 = 2^2 \cdot 3^2 \cdot 7 \]

Def: Let \( a, b \in \mathbb{Z}_{>0} \). The least common multiple of \( a \) and \( b \) is the smallest integer which is a multiple of \( a \) and \( b \). We write \( \text{LCM}(a, b) \).

Rem: Note that \( a \cdot b \) is a common multiple of \( a \) and \( b \). Thus \( \text{LCM}(a, b) \) exists by WOP.

Ex:
\[ \text{LCM}(2, 3) = 6 = 2 \cdot 3 \]
\[ \{2, 4, 6, 8, \ldots\} \quad \{3, 6, 9, \ldots\} \]
\[ \text{LCM}(6, 9) = 18 \neq 6 \cdot 9 \]
\[ \{6, 12, 18, \ldots\} \quad \{9, 18, 27, \ldots\} \]

Prop: Let \( a, b \in \mathbb{Z}_{>0} \). Have prime decompositions
\[ a = p_1^{a_1} \cdots p_N^{a_N} \quad b = p_1^{b_1} \cdots p_N^{b_N} \quad a_i, b_i > 0 \]
where \( p_i \) are distinct. Then

(i) \((a, b) = p_1^{\min(a_1, b_1)} \cdots p_N^{\min(a_N, b_N)}

(ii) \( \text{LCM}(a, b) = p_1^{\max(a_1, b_1)} \cdots p_N^{\max(a_N, b_N)}

(iii) \( a \cdot b = (a, b) \cdot \text{LCM}(a, b) \)
REM: We can use (i), (ii) to compute \((a, b)\) and \(\text{LCM}(a, b)\).

But factoring integers is hard.

Instead we use Euclidean algorithm to compute \((a, b)\) and (iii) to find \(\text{LCM}(a, b)\).

Example: \(2205 = \text{compute } (756, 2205), \text{LCM}(756, 2205)\)

We have
\[
756 = 2^2 \cdot 3^3 \cdot 5^0 \cdot 7^1
\]
\[
2205 = 2^0 \cdot 3^2 \cdot 5^1 \cdot 7^2
\]

Then
\[
\begin{cases}
(756, 2205) = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 = 63 \\
\text{LCM}(756, 2205) = 2^2 \cdot 3^3 \cdot 5^1 \cdot 7^2 = 26460
\end{cases}
\]

More on Primes

Theorem: There are infinitely many primes of the form \(4k + 3\), \(k \in \mathbb{Z}\).

Ex: \(k = 0 \rightarrow p = 3\) ✓
\(k = 1 \rightarrow p = 7\) ✓

\(k = 2 \rightarrow p = 11\)

\(k = 3 \rightarrow p = 15\) Not prime

REM: Note: this is a special case of Dirichlet density thm.
We need two auxiliary results.

**Lemma 1:** Let \( n \in \mathbb{Z} \).

(i) Then \( n \) is of the form \( 4k, 4k+1, 4k+2 \) or \( 4k+3 \).

(ii) If \( n \) is odd then it is of the form \( 4k+1 \) or \( 4k+3 \).

**Proof:**

(i) We divide \( n \) by 4 to obtain

\[ n = 4q + r, \quad 0 \leq r < 4 \]

Thus \( r = 0 \Rightarrow n = 4k \), \( r = 1 \Rightarrow n = 4q+1 \); ... 

(ii) Suppose \( n = 4k \) or \( 4k+2 \). Then \( 2 \mid n \)

Hence it is even.

**Lemma 2:** If \( a, b \in \mathbb{Z} \) are of the form \( 4k+1 \)

then \( a \cdot b \) is of the same form.

**Proof:** Write \( a = 4k_a + 1 \), \( b = 4k_b + 1 \).

\[ a \cdot b = (4k_a + 1)(4k_b + 1) = 16k_a k_b + 4k_a + 4k_b + 1 = 4(4k_a k_b + k_a + k_b) + 1 \]
Proof of Theorem:

Suppose there are finitely many primes of the form \(4k+3\).

Denote them \(p_0 = 3, p_1, p_2, \ldots, p_r\).

Consider \(Q = 4p_1p_2\ldots p_r + 3\).

There is a prime \(p|Q\), which is odd, since \(2|Q\).

From Lemma 1, part (ii) we have

\[ p = 4k + 1 \quad \text{or} \quad p = 4k + 3 \]

If all the primes dividing \(Q\) are of the form \(4k+3\),

Lemma 2 \(\Rightarrow\) \(Q\) is also of this form. Since \(Q\) is visibly not of the form \(4k+1\), we conclude there must be a \(p|Q\) of the form \(4k+3\).

Thus \(p = p_i\) for some \(i\).

If \(p = 3 \Rightarrow 3 | Q - 3 = 4p_1p_2\ldots p_r\) XXX

If \(p = p_i \neq 3 \Rightarrow p | Q - 4p_1\ldots p_r = 3\) XXX.

\[\Box\]
Primes Continued

**THM:** There are infinitely many primes of the form $4k + 3$

**Lemma:** Let $N \in \mathbb{Z}$.

(i) Then $N$ is of the form $4k$, $4k + 1$, $4k + 2$ or $4k + 3$

(ii) If $N$ is odd then $N$ is of the form $4k + 1$ or $4k + 3$

**Lemma:** If $a, b \in \mathbb{Z}$ are of the form $4k + 1$ then $a \cdot b$ is of the same form

**Proof of THM:**

- Suppose there are finitely many primes of the form $4k + 3$.
- Denote them $p_0 = 3, p_1, p_2, \ldots, p_r$
- Consider $Q = 4p_1p_2\ldots p_r + 3$
- There is a prime $p \mid Q$.
- $p$ is odd because $2 \nmid Q$
From Lemma 1 part (ii) we have

\[ p = 4k + 1 \quad \text{or} \quad p = 4k + 3 \]

If all the primes dividing \( Q \) are of the form \( 4k + 1 \) by Lemma 2 we conclude that \( Q \) is also of the form \( 4k + 1 \).

\( \Phi \) is clearly not of the form \( 4k + 1 \) so we must have a prime \( p | Q \) of the form \( 4k + 3 \).

Thus \( p = p_i \) for some \( i \).

If \( p = 3 \) \( \Rightarrow \) \( 3 | Q - 3 = 4p_1 \ldots p_r \) xxx

If \( p = p_i \neq 3 \) \( \Rightarrow \) \( p | Q - 4p_1 \ldots p_r = 3 \) xxx

We have a contradiction in both cases so the conclusion follows.
LINEAR DIOPHANTINE EQUATIONS

Def: Any equation with one or more variables to be solved in the integers is called a Diophantine equation.

Ex: \( 3x = 1 \), \( 2x + 2y = 3 \), \( x^2 + z^2 = y^2 \)

are Diophantine equations when we care only for solutions in \( \mathbb{Z} \).

Def: Let \( a_1, \ldots, a_n \in \mathbb{Z} \) \( \neq 0 \). A Diophantine equation of the form

\[
\sum_{i=1}^{n} a_i x_i = b, \quad b \in \mathbb{Z}
\]

is said to be a linear Diophantine equation in \( n \) variables \( x_i \).

Ex: \( 3x = 1 \) and \( 2x + 7y = 3 \) are linear.

\( x^2 + y^2 = z^2 \) and \( 2xy = 3 \) are non-linear.

Our objective is to focus on the case of 2 variables.

Thm (1 variable case): Let \( a, b \in \mathbb{Z} \), \( a \neq 0 \).

The equation \( ax = b \) has solutions if and only if \( a | b \).

When it does the solution is unique given by \( x = \frac{b}{a} \).
THM (Z VARIABLES CASE). Let $a, b, c \in \mathbb{Z}$ with $a, b \neq 0$.

Consider the equation $ax + by = c$ (*)

(A) The equation (*) has an integer solution $(x_0, y_0)$ if and only if $(a, b) \mid c$.

(B) Let $d = (a, b)$. Suppose $d \mid c$ so that there is a solution $(x_0, y_0)$ by part (A).

Then all solutions to (*) are given by

$$x = x_0 + \frac{b}{d} t, \quad y = y_0 - \frac{a}{d} t, \quad t \in \mathbb{Z}.$$ 

Proof of (A):

$\Rightarrow$ Suppose there is a solution $(x_0, y_0)$. Write $d = (a, b)$.

$$ax_0 + by_0 = c \iff (da')x_0 + (db')y_0 = d(a'x_0 + b'y_0) = c \Rightarrow d \mid c.$$

$\Leftarrow$ Suppose $d \mid c$. That is $c = dt$ with $t \in \mathbb{Z}$.

We know there exist $x_1, y_1 \in \mathbb{Z}$ such that

$$ax_1 + by_1 = d \Rightarrow a(tx_1) + b(ty_1) = d t = c \text{ multiply by } t$$

That is $x_0 = tx_1$, $y_0 = ty_1$ is a solution to (*).
Proof of (b):

1. Suppose \( d \mid c \) and \((x_0, y_0)\) is a solution to (\(*\)).

Let \( t \in \mathbb{Z} \). We compute

\[
a(x_0 + \frac{b}{d} t) + b(y_0 - \frac{a}{d} t) =
\]

\[
= ax_0 + \frac{ab}{d} t + by_0 - \frac{a^2}{d} t
\]

\[
= ax_0 + by_0 = c
\]

This shows that the formula in the statement produces solutions to (\(*\)).

2. To finish we have to show that all solutions to (\(*\)) are of the previous form.

Suppose \((x_0, y_0)\) and \((x_1, y_1)\) are 2 solutions.

Consider \( t_x = x_1 - x_0 \) and \( t_y = y_1 - y_0 \)

Compute

\[
a t_x + b t_y = ax_1 - ax_0 + by_1 - by_0
\]

\[
= (ax_1 + by_1) - (ax_0 + by_0) = c - c = 0
\]
Hence  \( b' ty = -a' t_x \)

\[ \frac{d}{d} \left( \frac{b'}{d} \right) t_y = -d \left( \frac{b'}{d} \right) t_x \], where \( d = (a, b) \)

\[ \Rightarrow b' ty = -a' t_x \], where \( a' = \frac{a}{d} \) , \( b' = \frac{b}{d} \)

Since \( (a', b') = 1 \) The lemma from previous class \( \Rightarrow b' t_x \)

That is \( t_x = b' t \) for some \( t \in \mathbb{R} \).

Then \( b' ty = -a' b' t \Rightarrow ty = -a't \)

Therefore:

\[
\begin{align*}
\begin{cases}
x_1 = x_0 + t_x = x_0 + b' t = x_0 + \frac{b}{d} t \\
y_1 = y_0 + ty = y_0 + a' b' t = y_0 + \frac{a}{d} t
\end{cases}
\end{align*}
\]
THM: Let \( a, b, c \in \mathbb{Z} \), \( a, b \neq 0 \).

Consider the equation \( ax + by = c \) (*)

(A) The equation (*) has an integer solution \( (x_0, y_0) \) if and only if \( (a, b) \mid c \).

(B) Let \( d = (a, b) \). Suppose \( d \mid c \) so that there is a solution \( (x_0, y_0) \) by (A).

Then all solutions to (*) are given by
\[
x = x_0 + \frac{b}{d} t, \quad y = y_0 - \frac{a}{d} t, \quad t \in \mathbb{Z}
\]

Example: \( 154x + 35y = 7 \)

We have seen that \( d = (154, 35) = 7 \).

Since \( 7 \mid 7 \) there are solutions.

We have also computed the particular solution
\[
(x_0, y_0) = (-2, 9)
\]

Therefore the general solution is given by
\[
x = -2 + 5t, \quad y = 9 - 22t
\]

And taking \( t = 1 \) (for example) gives the solution
\[
x_1 = 3, \quad y_1 = -13
\]
Example: $154x + 35y = 24$

Since $d = (154, 35) = 7 \n 24$

There are no solutions

Example: $154x + 35y = 21$

Since $d = (154, 35) = 7 \mid 21$ There are solutions

We know that

$154x + 35y = 7$ has solution $x_1 = -2, \ y_1 = 9$

Thus

$154x + 35y = 21$ has solution $x_0 = -6, \ y_0 = 27$

We conclude that the general solution $\mathbb{R}$ is

Given by

$x = -6 + 5t, \ y = 27 - 22t$
CONGRUENCES

DEF: Let $a, b \in \mathbb{Z}$. Let $M \in \mathbb{Z}_{>0}$.

We say that "$a$ is congruent to $b$ modulo $M"$ if and only if $M \mid a-b$.

Notation: $a \equiv b \pmod{M}$

$a \not\equiv b \pmod{M}$

$M$ is called the "modulus".

Examples:
- $9 \equiv 3 \pmod{3}$ since $9 - 3 = 6 = 3 \cdot 2$
- $7 \equiv 1 \pmod{2}$ since $7 - 1 = 6 = 2 \cdot 3$
- $8 \equiv 0 \pmod{2}$ since $8 - 0 = 8 = 2 \cdot 4$

- $\forall a, b \in \mathbb{Z} \quad M \mid a-b \iff a \equiv b \pmod{M}$
- Let $N = 4k + 3$. Then $4 \mid N-3$ \iff $N \equiv 3 \pmod{4}$
- Let $N = 4k + 1$. Then $4 \mid N-1$ \iff $N \equiv 1 \pmod{4}$
We can rephrase past this using congruences

There are infinitely many primes \( p \) such that \( p \equiv 3 \pmod{4} \)

Lemma 2: Let \( a, b \in \mathbb{Z} \) satisfy \( a \equiv 1 \pmod{4} \) and \( b \equiv 1 \pmod{4} \).

Then \( a \cdot b \equiv 1 \pmod{4} \)

We will soon see that Lemma 2 is a particular case of a general property of congruences.

Prop: Congruences modulo \( M \) is an equivalence relation.

More precisely:

(i) \( a \equiv a \pmod{M} \)

(ii) \( a \equiv b \pmod{M} \) \( \Rightarrow \) \( b \equiv a \pmod{M} \)

(iii) \( a \equiv b \pmod{M} \), \( b \equiv c \pmod{M} \) \( \Rightarrow \) \( a \equiv c \pmod{M} \)

Therefore the congruence relation modulo \( M \) divides the integers into disjoint congruence classes \( \pmod{M} \).

Notation: We write \( [a] \) for the congruence class of \( a \in \mathbb{Z} \pmod{M} \).
Proof: (i) \( a - a = 0 \) is divisible by \( M \) \( \forall n \)

(ii) \( a - b = Mk \Rightarrow b - a = M(-k) \)

\[ \Rightarrow b \equiv a \text{ (mod } M) \]

(iii) We have \( a - b = Mk_1, b - c = Mk_2 \) then

\[ a - c = (a - b) + (b - c) = Mk_1 + Mk_2 = M(k_1 + k_2) \]

\[ \Rightarrow a \equiv c \text{ (mod } M) \]

Example: \( M = 4 \)

\[ \mathbb{Z}_0 = \{ x \in \mathbb{Z}^n : x \equiv 0 \text{ (mod } 4) \} = \{ x \in \mathbb{Z}^n : x - 0 = 4k, k \in \mathbb{Z} \} \]

\[ = \{ \ldots, -8, -4, 0, 4, 8, \ldots \} \]

\[ \mathbb{Z}_1 = \{ x \in \mathbb{Z}^n : x \equiv 1 \text{ (mod } 4) \} = \{ x \in \mathbb{Z}^n : x - 1 = 4k, k \in \mathbb{Z} \} \]

\[ = \{ x \in \mathbb{Z}^n : x = 1 + 4k, k \in \mathbb{Z} \} = \{ \ldots, -7, -3, 1, 5, 9, \ldots \} \]

\[ \mathbb{Z}_2 = \{ \ldots, -6, -2, 2, 6, \ldots \} \]

\[ \mathbb{Z}_3 = \{ \ldots, -5, -1, 1, 3, 7, 11, \ldots \} \]

Ex: \( M = 3 \)

\[ \mathbb{Z}_0 = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \]

\[ \mathbb{Z}_1 = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \]

\[ \mathbb{Z}_2 = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} \]
**Question:** Given $a \in \mathbb{Z}$ to which class modulo $M$ does it belong?

**Prop:** Let $a \in \mathbb{Z}$. Let $M > 0$.

Then $a$ is congruent mod $M$ to exactly one of the integers $\{0, 1, 2, \ldots, M-1\}$

**Proof:** We divide $a$ by $M > 0$ to get

$$a = M \cdot q + r, \quad 0 \leq r < M$$

$$\Rightarrow a - r = M \cdot q \iff a \equiv r \pmod{M}$$

with $r \in \{0, 1, 2, \ldots, M-1\}$

- Suppose $a \equiv r_1 \pmod{M}$ and $a \equiv r_2 \pmod{M}$

with $r_1, r_2 \in \{0, 1, \ldots, M-1\}$

Then $r_1 \equiv r_2 \pmod{M} \iff M \mid r_1 - r_2$

Since $-(M-1) \leq r_1 - r_2 \leq M-1$ we have $r_1 - r_2 = 0 \Rightarrow r_1 = r_2$

**Def:** A set of integers such that every integer is congruent mod $M$ to exactly one integer in it is called a "complete residue system mod $M$"

Ex: $\{0, 1, \ldots, M-1\}$
Question: Given \( a \in \mathbb{Z} \) to which class modulo \( M \) does \( a \) belong?

**Proof:** Let \( a, n \in \mathbb{Z} \), \( M > 0 \).

Then \( a \equiv R \pmod{M} \) where \( R \) is the remainder of the division of \( a \) by \( M \). In particular, \( a \) is congruent to exactly one of the integers in \( \{0, 1, 2, \ldots, M-1\} \) and \( [a] = [R] \).

**Def:** A set of integers such that every integer is congruent mod \( M \) to exactly one integer in it is called "A complete residue system mod \( M \)."

**Example:** \( \{0, 1, \ldots, M-1\} \)

**Def:** To the set of congruence classes mod \( M \)

\[ \mathbb{Z}/M := \{ [0], [1], \ldots, [M-1] \} \]

We call the "integers modulo \( M \)."

**Def:** We can choose different representatives, for example, \( M = 3 \); \( \mathbb{Z}/3 = \{[0], [1], [2]\} = \{[3], [7], [10]\} \).
We shall see that \( \mathbb{Z}_M \) has many properties resembling the integers but also differences (e.g. there is no cancellation law).

**Theorem:** Let \( n \in \mathbb{Z}_M \). Suppose \( a \equiv b \pmod{M} \) and \( c \equiv d \pmod{M} \).

Then we have:

1. \( a + c \equiv b + d \pmod{M} \)
2. \( a - c \equiv b - d \pmod{M} \)
3. \( ac \equiv bd \pmod{M} \)

**Proof:** We have \( d = a + kn \), \( d = c + k'k \)

1. \( a + c + (k + k')n = b + d \)

\( \Rightarrow (a + c) - (b + d) = n(-k - k') \Rightarrow a + c \equiv b + d \pmod{M} \)

2. Same as (i)

3. \( b \cdot d = (a + kn)(c + k'n) = ac + ak'n + ckn + kk'n^2 = b \cdot c + ckn + ckn + kk'n^2 \Rightarrow b \cdot d - ac = n(ak' + ck + kk'n) \Rightarrow b \cdot d \equiv ac \pmod{M} \)
Examples: (i) \( n = 5 \)

- \( 49^2 \equiv 4^2 \equiv 16 \equiv 1 \pmod{5} \) OR
- \( 49^2 \equiv (-1)^2 \equiv 1 \pmod{5} \)

(ii) Take \( n = 4 \), \( a = d = 1 \).

Let \( a \equiv 1 \pmod{4} \) and \( c \equiv 1 \pmod{4} \)

Then \( a \cdot c \equiv 1 \cdot 1 \equiv 1 \pmod{4} \).

Note this is what we called "Lemma 2". You should look into the similarities of the proofs.

Rem: The theorem does not hold for exponentiation.

That is: \( c \equiv d \pmod{m} \) \( \not\Rightarrow \) \( a^c \equiv a^d \pmod{m} \)

Indeed, \( 2^3 \equiv 8 \equiv 2 \pmod{3} \)

\( 2^6 \equiv 2 \cdot 2^3 \equiv 4 \equiv 1 \pmod{3} \)

And \( 3 \equiv 6 \pmod{3} \)

Def: Let \( [R], [S] \in \mathbb{Z}/m \). We define

(Addition) \( [R] + [S] := [R + S] \)

(Multiplication) \( [R] \cdot [S] = [R \cdot S] \)

(Mult by scalar) \( \lambda \cdot [R] := [\lambda R] \), \( \lambda \in \mathbb{Z} \)
Prop: The operations are well defined, that is their output is independent of the choice of representatives.

Proof: (Addition) Let \( R \in \mathbb{Z}_7 \) and \( S \in \mathbb{Z}_7 \). This means \( R \equiv R' \pmod{7} \) and \( S \equiv S' \pmod{7} \). Therefore, \( R + S \equiv R' + S' \pmod{7} \). But then \( [R] + [S] = [R+S] = [R'] + [S'] = [R'] + [S'] \).

(Multiplication) Similar argument.

Example: Addition Modulo 3

<table>
<thead>
<tr>
<th></th>
<th>[0]</th>
<th>[1]</th>
<th>[2]</th>
</tr>
</thead>
<tbody>
<tr>
<td>[0]</td>
<td>[0]</td>
<td>[1]</td>
<td>[2]</td>
</tr>
<tr>
<td>[1]</td>
<td>[1]</td>
<td>[2]</td>
<td>[0]</td>
</tr>
<tr>
<td>[2]</td>
<td>[2]</td>
<td>[0]</td>
<td>[1]</td>
</tr>
</tbody>
</table>

Example: Multiplication Mod 7

\( H = 7 \): \([3^3] \cdot [6] = [18] = [4] = [-10]\)
\([10] \cdot [-1] = [-10]\)
Here is a difference compared to the integers.

**Lemma:** Let $a, b, c \in \mathbb{Z}$. Then

$c \cdot a \equiv c \cdot b \pmod{M} \iff a \equiv b \pmod{\frac{M}{(c, M)}}$

**Proof:** ($\Rightarrow$) Let $d = (c, M)$. Suppose $a \equiv b \pmod{\frac{M}{d}}$.

So $a - b = \frac{M}{d} \cdot k \Rightarrow da - db = M \cdot k$

$\Rightarrow \frac{c}{d} (da - db) = \frac{c}{d} M \cdot k \Rightarrow ca - cb = M \left(\frac{ck}{d}\right)$

$\Rightarrow ca \equiv cb \pmod{M}$.

($\Leftarrow$) Suppose $ca \equiv cb \pmod{M}$, write $d = (c, M)$.

We have $ca - cb = M \cdot k \Rightarrow \frac{c}{d} (a - b) = \frac{M}{d} \cdot k$

Since $\left(\frac{c}{d}, \frac{M}{d}\right) = 1$ we have $\frac{M}{d} \mid a - b$

$\Rightarrow a \equiv b \pmod{\frac{M}{d}}$.

\[\square\]
Example:

- \(6a \equiv 6b \pmod{3} \quad \forall a, b\)

  since \(0 \equiv 0 \pmod{3}\)

- If we just cancel the 6 like we do in \(\mathbb{Z}\), we get \(a \equiv b \pmod{3} \quad \forall a, b\)

  which is FALSE!! (E.g., \(1 \not\equiv 2 \pmod{3}\))

- Instead we apply the lemma:

  \(6a \equiv 6b \pmod{3} \iff a \equiv b \pmod{\frac{3}{(3,6)}}\)

  \(\iff a \equiv b \pmod{1} \quad \forall a, b\)

  This we know to be TRUE!
THE CONGRUENCE METHOD

THIS SOMETIMES ALLOWS TO SHOW THAT CERTAIN DIOPHANTINE EQUATIONS IN \( \mathbb{Z} \) HAVE NO SOLUTIONS.

**Example:** Find \( x, y \in \mathbb{Z} \) such that
\[
3x^2 + 2 = y^2
\]

Reducing modulo 3 we get (since \( 3 \equiv 0 (\text{mod} \ 3) \))
\[
2 \equiv y^2 \ (\text{mod} \ 3)
\]

Now, the possibilities for \( y \ (\text{mod} \ 3) \) are
\[
y \equiv 0, 1, 2 \ (\text{mod} \ 3) \Rightarrow y^2 \equiv 0, 1, 1 \ (\text{mod} \ 3)
\]
so \( y^2 \not\equiv 2 \ (\text{mod} \ 3) \) and we conclude

**There are no solutions in the integers to the original equation.**

If instead we look \( \text{mod} \ 2 \) we obtain
\[
3x^2 + 2 \equiv y^2 \ (\text{mod} \ 2) \Rightarrow x^2 \equiv y^2 \ (\text{mod} \ 2)
\]

which has solutions (take \( x = y \)).

Thus the existence of solutions \( \text{mod} \ M \) says nothing about solutions in \( \mathbb{Z} \).
Example: Solve $4y^2 + 2x = 3$ in $\mathbb{Z}$

Working mod 4 gives

$2x \equiv 3 \pmod{4}$

As: $x \equiv 0, 1, 2, 3 \Rightarrow 2x \equiv 0, 2, 0, 2 \not\equiv 3$

We conclude there are no solutions.

This example indicates it is important to understand solutions of equations of the form $ax \equiv b \pmod{m}$

which are called "linear congruences in one variable".

Ex: We have seen that $2x \equiv 3 \pmod{4}$ has no solutions.

- $2x \equiv 3 \pmod{5}$

$x \equiv 0, 1, 2, 3, 4 \Rightarrow 2x \equiv 0, 2, 4, 0, 3$

so $x \equiv 4 \pmod{5}$ is a solution.

Thus all integers in $[4]$ satisfy the equation.
3x ≡ 9 \pmod{6} \\
\Rightarrow 3x ≡ 0, 3, 6, 9, 0, 3 \pmod{6}

Thus there are three non-congruent solutions \( x \equiv 1, x \equiv 3, x \equiv 5 \pmod{6} \)

These examples show that the behaviour of solutions can vary. The following theorem explains it.

**Theorem:** Let \( a, b, m \in \mathbb{Z}^* \), \( m > 0 \).

Write \( d = (a, m) \)

(A) The congruence \( ax \equiv b \pmod{m} \) has no solutions if \( d \nmid b \)

(B) Suppose \( d \mid b \). Then \( ax \equiv b \pmod{m} \) has exactly \( d \) distinct solutions modulo \( m \).

They are given by

\[ x \equiv x_0 - \frac{m}{d}t \quad \text{where} \quad 0 \leq t \leq d-1 \]

and \( x_0 \) is a particular solution.
Corollary: \( ax \equiv 1 \pmod{m} \) has exactly one solution modulo \( m \) if and only if \((a,m)=1\).

**Definition:** Any integer solution to \( ax \equiv 1 \pmod{m} \) is called an inverse of \( a \) modulo \( m \).

**Notation:** Note that \( ax \equiv 1 \pmod{m} \)

\[ \Rightarrow [ax] = [1] \iff [a][x] = [1] \]

We also say that \([a]^{-1}\) and \([x]\) are inverses in \( \mathbb{Z}/m\mathbb{Z} \)

and we write \([a]^{-1} \) or \( a^{-1} \).

**Examples:** M = 10

\[
\begin{array}{c|cccccccccc}
  a & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
  \hline
  a^{-1} & x & 1 & x & 7 & x & x & x & x & 3 & x \end{array}
\]

M = 5

\[
\begin{array}{c|cccc}
  a & 0 & 1 & 2 & 3 \\
  \hline
  a^{-1} & x & 1 & 3 & 2 \end{array}
\]
Corollary: Let \( p \) be a prime
then all \( a \neq 0 \pmod{p} \) has a unique inverse modulo \( p \).

In the previous examples for \( n = 5, 10 \) to find inverses we can try all possibilities because the numbers are small.
In general, to compute \( a^{-1} \pmod{n} \) we need to solve the linear Diophantine equation \( ax + ny = 1 \) using the methods we already know.

Example: Compute \( 47^{-1} \pmod{55} \)

We want to solve \( 17x \equiv 1 \pmod{55} \)

which is equivalent to find a solution \((x_0, y_0)\) to \( 17x + 55y = 1 \) and then \( x_0 \pmod{55} \) will be the inverse.

We are looking for, because
\[ 17x_0 + 55y_0 = 1 \Rightarrow 17x_0 \equiv 1 \pmod{55} \]
o Find \((17, 55)\) using Euclidean Algorithm

\[55 = 17 \times 3 + 4\]
\[17 = 4 \times 4 + 1\]
\[4 = 1 \times 4 + 0\]

so \((17, 55) = 1\)

o Find \((x_0, y_0)\) satisfying \(17x + 55y = 1\)

using back substitution

\[1 = 17 - 4 \times 4 = 17 - 4(55 - 17 \times 3) =\]
\[= 17 - 4 \times 55 + 12 \times 17 = 17 \times 13 - 55 \times 4\]

\[\Rightarrow x_0 = 13, \quad y_0 = -4\]

Then \(17 \times 13 \equiv 1 \pmod{55}\)

That is \([17]^{-1} \equiv [13] \text{ in } \mathbb{Z}_{55}\)