Lecture 8

CONGRUENCES

DEF: Let \( a, b \in \mathbb{Z} \). Let \( \mathbb{N} \) be \( \mathbb{Z}^\geq 0 \). We say that "\( a \) is congruent to \( b \) modulo \( n \)" if and only if \( n | a - b \).

Notation:
- \( a \equiv b \pmod{n} \)
- \( a \not\equiv b \pmod{n} \)
- \( n \) is called the "modulus"

Example:
- \( 9 \equiv 3 \pmod{3} \) 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 \( 8 - 0 = 8 = 2 \cdot 4 \)
- \( \forall a, b \in \mathbb{Z} \quad 1 | a - b \iff a \equiv b \pmod{1} \)
- Let \( N = 4k + 3 \), then \( 4 | N - 3 \)
  \( \iff N \equiv 3 \pmod{4} \)
- Let \( N = 4k + 1 \), then \( 4 | N - 1 \)
  \( \iff N \equiv 1 \pmod{4} \)
We can rephrase this in the language of congruences

**Theorem**: There are infinitely many primes $p$

such that $p \equiv 3 \pmod{4}$

**Lemma**: Let $a, b \in \mathbb{Z}$ satisfy $a \equiv 1 \pmod{4}$ and $b \equiv 1 \pmod{4}$.

Then $a - b \equiv 1 \pmod{4}$

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 on $\mathbb{Z}$. More precisely,

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

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

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

In particular, the congruence relation $\pmod{M}$ 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 \( M \) \( \forall M > 0 \)

(ii) \( a - b = M k \) \( \Rightarrow b - a = M(-k) \)
\[ \Rightarrow M | b - a \iff b \equiv a \pmod{M} \]

(iii) We have \( a - b = M k_1, b - c = M k_2 \)

Then \( a - c = (a - b) + (b - c) = M k_1 + M k_2 = M(k_1 + k_2) \)
\( \iff a \equiv c \pmod{M} \)

**Example:** \( M = 4 \)

\[ [0] = \{ x \in \mathbb{Z} : x \equiv 0 \pmod{4} \} \]
\[ = \{ x \in \mathbb{Z} : x - 0 = 4k, k \in \mathbb{Z} \} \]
\[ = \{ ..., -8, -4, 0, 4, 8, ... \} \]

\[ [1] = \{ x \in \mathbb{Z} : x \equiv 1 \pmod{4} \} \]
\[ = \{ x \in \mathbb{Z} : x - 1 = 4k, k \in \mathbb{Z} \} \]
\[ = \{ x \in \mathbb{Z} : x = 4k + 1, k \in \mathbb{Z} \} \]
\[ = \{ ..., -7, -3, 1, 5, 9, ... \} \]

\[ [2] = \{ ..., -6, -2, 2, 6, ... \} \]

\[ [3] = \{ ..., -5, -1, 3, 7, 11, ... \} \]
Ex: \( M = 3 \)
\[
[0] = \{ \ldots, -6, -3, 0, 3, 6, \ldots \} \\
[1] = \{ \ldots, -5, -2, 1, 4, 7, \ldots \} \\
[2] = \{ \ldots, -4, -1, 2, 5, 8, \ldots \} 
\]

Ex: \( M = 2 \)
\[
[0] = \{ \text{EVEN INTEGERS} \} \\
[1] = \{ \text{ODD INTEGERS} \} 
\]

**Question:** Given \( a \in \mathbb{Z} \), to which class modulo \( M \) does it belong to?

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

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 \( [a] = [r] \).
Proof: \( \text{Div. Alg} \Rightarrow a = mq + r, 0 \leq r < m \)
\( \Rightarrow a - r = mq \Rightarrow m \mid (a - r) \Leftrightarrow a \equiv r \pmod{m} \)
Showing that \( a \) is congruent to some \( r \in \{0, 1, \ldots, m-1\} \).

We need to show that \( r \) is unique.

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 \( r_1 \equiv r_2 \pmod{m} \Leftrightarrow m \mid r_1 - r_2 \)
Since \( -(m-1) \leq r_1 - r_2 \leq m-1 \)
\( \Rightarrow r_1 = r_2 = 0 \) because there is no other multiple of 17 in this range. Thus \( r_1 = r_2 \) \( \blacksquare \).

Def: A set \( S \subseteq \mathbb{Z} \) such that every integer is congruent modulo \( m \) to exactly one integer in \( S \) is called "a complete residue system modulo \( m \)."

Ex: \( S = \{0, 1, \ldots, m-1\} \) is a complete residue system \( \pmod{m} \) by the previous proposition.
DEF: To the set of congruence classes modulo \( M \),
\[
\mathbb{Z}/M := \{[0], [1], \ldots, [M-1]\}
\]
we call "integers modulo \( M \)"

DEF: We can choose different representatives for example,
\[
\mathbb{Z}/3 = \{[0], [1], [2]\} = \{[3], [7], [2]\}
\]

We will see that \( \mathbb{Z}/M \) shares properties with \( \mathbb{Z} \). For example, we can add AND multiply in \( \mathbb{Z}/M \).

But there are also differences. Most importantly, there is no cancellation law! Indeed, in \( \mathbb{Z} \) we have
\[
a \cdot b = 0 \Rightarrow a = 0 \text{ or } b = 0
\]
but \( 2 \cdot 2 = 4 \equiv 0 \pmod{4} \) but \( 2 \not\equiv 0 \pmod{4} \).
THM: Let \( n \in \mathbb{N}_0 \). Suppose \( a \equiv b \pmod{n} \), \( c \equiv d \pmod{n} \).

THEN, (i) \( a + c \equiv b + d \pmod{n} \)

(ii) \( a - c \equiv b - d \pmod{n} \)

(iii) \( a \cdot c \equiv b \cdot d \pmod{n} \)

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

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

\( \iff (a + c) - (b + d) = n(-k-k') \)

\( \iff a + c \equiv b + d \pmod{n} \)

(ii) Same as (i)

(iii) \( b \cdot d = (a + kn)(c + k'n) = a \cdot c + ak'n + ckn + kk'n^2 \)

\( \iff b \cdot d - a \cdot c = n(ak' + ck + kk'n) \)

\( \iff b \cdot d \equiv a \cdot c \pmod{n} \)

Example: (i) \( n = 5 \)

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

\( 49^2 \equiv (-1)^2 \equiv 1 \pmod{5} \)
(ii) \( M = 4, \ b = d = 1. \)

Let \( a \equiv 1 \) (mod 4) and \( c \equiv 1 \) (mod 4)

Then \( a \cdot c \equiv 1 \cdot 1 \equiv 1 \) (mod 4).

Note this is what we called "Lemma 2."

REM: THE THEOREM DOES NOT HOLD FOR EXponentiation.

Indeed, \( c \equiv d \) (mod 4) \( \Rightarrow \) \( a^c \equiv a^d \) (mod 4)

because

\[ 2^3 \equiv 8 \equiv 2 \ \text{(mod 3)} \]

\[ 2^6 \equiv 2^3 \cdot 2^3 \equiv 4 \equiv 1 \ \text{(mod 3)} \]

AND \( 3 \equiv 6 \) (mod 3)
Def: Let \( [R], [S] \in \mathbb{Z}/m \). Define

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

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

(Mult by scalar) \( \lambda \cdot [R] := [\lambda R] \), \( \lambda \in \mathbb{Z} \)

Proof: The operations on \( \mathbb{Z}/m \) are well defined. That is, their output is independent of the choice of representatives.

Proof: (Addition) Let \( R' \in [R], S' \in [S] \), i.e., \( R' \equiv R \pmod{m} \) and \( S' \equiv S \pmod{m} \)

\[ R' + S' \equiv R + R' \pmod{m} \]

Then

\[ [R + S] = [R' + S'] \]

Therefore, \( [R] + [S] = [R + S] = [R' + S'] = [R'] + [S'] \)

(Multiplication follows similarly.)

Ex: Multiplication in \( \mathbb{Z}/4 \)


\[ [10] \cdot [-1] = [-10] \]
Example: Addition mod 3

\[\begin{array}{ccc}
\end{array}\]

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: \((\Leftarrow)\) Let \(d = (c, m)\). Suppose \(a \equiv b \pmod{\frac{m}{c}, m}\)

so \(a - b = \frac{m}{d} \cdot k\) \(\Rightarrow da - db = M \cdot k\)

\[\Rightarrow \frac{c}{d} (da - db) = \frac{c}{d} M k \iff ca - cb = M \left(\frac{c}{d} k\right)\]

\[\Rightarrow ca \equiv cb \pmod{m}\]

\((\Rightarrow)\) Suppose \(ca \equiv cb \pmod{m}\). Write \(d = (c, m)\).

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

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

\[\iff a \equiv b \pmod{\frac{m}{d}}\]
Example:

\[ 6a \equiv 6b \pmod{3} \quad \forall a, b \in \mathbb{Z} \]

If we cancel the 6 like we do in \( \mathbb{Z} \),
we get \( a \equiv b \pmod{3} \) \( \forall a, b \in \mathbb{Z} \),
which is false! E.g., \( 1 \not\equiv 2 \pmod{3} \).

Instead we apply the lemma

\[ 6a \equiv 6b \pmod{3} \iff a \equiv b \pmod{\frac{3}{(3,6)}} \]
\[ \iff a \equiv b \pmod{1} \quad \forall a, b \in \mathbb{Z} \]

which we know to be true!
THE CONGRUENCE METHOD

This method uses congruences to show (when it succeeds) that a Diophantine equation has no solutions.

Example: Solve \( 3x^2 + 2 = y^2 \), \( x, y \in \mathbb{Z} \).

Considering the equation modulo 3 gives:
\[ 3x^2 + 2 \equiv y^2 \pmod{3} \Rightarrow y^2 \equiv 2 \pmod{3} \]

The possible values of \( y \pmod{3} \) are:
\[ y \equiv 0, 1, 2 \pmod{3} \Rightarrow y^2 \equiv 0, 1, 1 \pmod{3} \]
So \( y^2 \not\equiv 2 \pmod{3} \).

We conclude the original equation has no solutions.

If instead we work modulo 2 we obtain:
\[ 3x^2 + 2 \equiv y^2 \pmod{2} \Rightarrow x^2 \equiv y^2 \pmod{2} \]
Which has solutions, for example take \( x = y \).

We conclude that the existence of solutions modulo \( m \) says nothing about solutions in \( \mathbb{Z} \).
Example: Solve \( 20y^2 + 2x = 3 \) in \( \mathbb{Z} \)

- Working \( \text{mod} \ 4 \) gives \( 2x \equiv 3 \pmod{4} \)
  \[ x \equiv 0, 1, 2, 3 \pmod{4} \implies 2x \equiv 0, 2, 0, 2 \neq 3 \]
  We conclude there are no solutions in \( \mathbb{Z} \).

- If instead we work \( \text{mod} \ 5 \) we get \( 2x \equiv 3 \pmod{5} \)
  \[ x \equiv 0, 1, 2, 3, 4 \pmod{5} \implies 2x \equiv 0, 2, 4, 1, 3 \pmod{5} \]
  So \( x \equiv 4 \pmod{5} \) is a solution, that is all integers in \( [4] \) satisfies \( 2x \equiv 3 \pmod{5} \)

These examples indicate that it is relevant to understand the solutions of congruences of the form \( ax \equiv b \pmod{m} \), \( a, b \in \mathbb{Z} \). These are called "linear congruences in one variable."

Example: \( 3x \equiv 9 \pmod{6} \)

\[ x \equiv 0, 1, 2, 3, 4, 5 \pmod{6} \implies 3x \equiv 0, 3, 6, 9, 0, 15 \pmod{6} \]
  \[ \equiv 0, 3, 0, 3, 0, 3 \pmod{6} \]

Thus: there are three non-congruent solutions \( x \equiv 1, 3, 5 \pmod{6} \)
Thus the behaviour of solutions can vary.
This is explained by the following theorem.

**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 $\pmod{m}$.
They are given by

$$x \equiv x_0 - \frac{m}{d}t$$

where $0 \leq t \leq d - 1$.

And $x_0$ is a particular solution.

**Corollary:** $ax \equiv 1 \pmod{m}$ has exactly one solution if and only if $(a, m) = 1$.

Def: Any integer solution to $ax \equiv 1 \pmod{m}$ is called an inverse of $a \pmod{m}$.
REMARK: 

Note that \( ax \equiv 1 \pmod{M} \)

\[ [a \times x] = [1] \iff [a] \cdot [x] = [1] \]

And we also say that \([a\bar{a}]\) and \([x\bar{x}]\)
are inverses in \(\mathbb{Z}/M\). We write \([a^{-1}] \) or \(\bar{a}^{-1}\)

**Examples:**

1. \(M = 10\)

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

2. \(M = 5\)

\[
\begin{array}{c|cccc}
\bar{a} & 0 & 1 & 2 & 3 \\
\hline
\bar{a}^{-1} & x & 1 & 3 & 2
\end{array}
\]

**Corollary:** Let \(p\) be a prime.

Then every \(a \in \mathbb{Z}/p\) not divisible by \(p\)

has a unique inverse \(\pmod{p}\).

**Proof:** \( ax \equiv 1 \pmod{p} \) has a sol if and only if \((a, p) = 1\) which is true since \(p \mid a\) is prime.
Proof of Thm:

(A) Suppose $ax_0 \equiv b \pmod{m}$, for some $x_0 \in \mathbb{Z}$.
Then $ax_0 - b = my_0 \iff ax_0 + m(-y_0) = b$.
Meaning that $ax + my = b$ has the solution $(x_0, -y_0)$.
Thus $(a, m) = d | b$ by previous Thm.

(B) Suppose $d | b$. Then $ax - my = b$ has solutions. Let $(x_0, y_0)$ be a particular solution.
The general solution is given by
$$x = x_0 - \frac{m}{d} t,$$
$$y = y_0 - \frac{a}{d} t,$$
$t \in \mathbb{Z}$.

In particular, the expression for $x$ gives all the integers satisfying $ax \equiv b \pmod{m}$.
To finish we want to count the different values of $x \pmod{m}$. 

Suppose $X_0 - \frac{M}{d} t_i \equiv X_0 - \frac{M}{d} t_2 \pmod{M}$

$\Leftrightarrow \frac{M}{d} (t_2 - t_1) \equiv 0 \equiv \frac{M}{d} \cdot 0 \pmod{M}$

$\Leftrightarrow t_2 - t_1 \equiv 0 \pmod{\frac{M}{(\frac{M}{d}, M)}}$

Lemma

$\Leftrightarrow t_1 \equiv t_2 \pmod{d}$

Because

$\text{lcm}(M, \frac{M}{d}) = \frac{M}{d}$

Therefore, taking $t \in \{0, 1, \ldots, d-1\}$ gives the desired set of \text{non-congruent solutions} mod M.
LINEAR CONGRUENCES IN ONE VARIABLE

- We studied the solutions of
  \[ ax \equiv b \pmod{m} \]
  where \( a, b, m \in \mathbb{Z} \) with \( m > 0 \).

- The case \( b = 1 \) is specially important
  **DEF:** Any integer \( x \) satisfying \( ax \equiv 1 \pmod{m} \)
  is called an inverse of \( a \) modulo \( m \).

  **REM:** Note that \( ax \equiv 1 \pmod{m} \) \(\Rightarrow\) \([ax] = [1]\)
  in \( \mathbb{Z}/m \). But \([ax] = [a][x] = [1]\)
  and we say \([a]^{-1}\) and \([x]^{-1}\) are inverses in \( \mathbb{Z}/m \).
  We write \([a]^{-1}\) or \(a^{-1}\).

<table>
<thead>
<tr>
<th>a</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>a^{-1}</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

**Corollary:** Let \( p \) be a prime. Then every \( a \in \mathbb{Z} \)
such that \( p \nmid a \) has a unique inverse modulo \( p \).
For small values of $M$ we can find the inverse of $a \mod M$ by trial and error, as we did in the table.

In general, to compute $a^{-1} \mod M$, we need to solve the equation $ax + my = 1$ using the Euclidean algorithm and back substitution.

Example: Compute $17^{-1} \mod 55$

We need to solve $17x \equiv 1 \mod 55$

which is equivalent to finding a solution $(x_0, y_0)$ to $17x + 55y = 1$. Then $x_0 \mod 55$ is the inverse $17^{-1} \mod 55$ because

$17x_0 + 55y_0 \rightarrow 17x_0 \equiv 1 \mod 55$
Find $(17, 55)$ with Euclidean Algorithm

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

so $(17, 55) = 1$

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

Using Back Substitution

\[
1 = 17 - 4 \cdot 4 = 17 - 4 \left(55 - 17 \cdot 3\right) \\
= 17 - 4 \cdot 55 + 12 \cdot 17 \\
= 17 \cdot 13 - 55 \cdot 4
\]

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

Then $17 \cdot 13 \equiv 1 \pmod{55}$

THE CHINESE REMAINDER THEOREM (CRT)

- We have studied how to solve linear congruences in one variable. What about several congruences?

- Consider the following problem:
  - Find a positive integer having remainder 2 when divided by 3, remainder 1 when divided by 4, and remainder 3 when divided by 5.

- In the language of congruences this problem is the same as finding \( x \in \mathbb{Z} \), such that

\[
\begin{align*}
  x &\equiv 2 \pmod{3} \\
  x &\equiv 1 \pmod{4} \\
  x &\equiv 3 \pmod{5}
\end{align*}
\]

This system of congruences can be solved using CRT.
**Chinese Remainder Theorem:**

Let \( N_1, N_2, \ldots, N_k \in \mathbb{Z}_{>0} \) be pairwise coprime, that is, \((N_i, N_j) = 1\) \(\forall i \neq j\).

Let \( b_1, \ldots, b_k \in \mathbb{Z} \) and consider the system

\[
\begin{aligned}
x &\equiv b_1 \pmod{N_1} \\
x &\equiv b_2 \pmod{N_2} \\
&\quad \vdots \\
x &\equiv b_k \pmod{N_k}
\end{aligned}
\]

Then there is a unique solution to (*) modulo \( N_1 N_2 \ldots N_k \).

Before giving a proof let's look into an example. Consider

\[
\begin{aligned}
x &\equiv 3 \pmod{7} \\
x &\equiv 2 \pmod{3}
\end{aligned}
\]

The first congruence gives \( x - 3 = 7k \) that is \( x = 3 + 7k \). Replacing into the second congruence gives \( 3 + 7k \equiv 2 \pmod{3} \)

\( \Rightarrow k \equiv 2 \pmod{3} \Rightarrow k = 2 + 3t \)
Now replacing for \( k \) gives
\[ x = 3 + 7(2 + 3t) = 17 + 21t \]
In particular, \( x_0 = 17 \) and \( x_1 = 38 \) are solutions.
Note that \( 21 = 7 \cdot 3 \) is the modulus predicted by CRT so \( x \equiv 17 \pmod{21} \) must be the unique solution \( \bmod 21 \).
Indeed, we can check
\[
\begin{cases}
  x = 17 + 21t & \equiv 3 + 0 \equiv 3 \pmod{7} \\
  x = 17 + 21t & \equiv 2 + 0 \equiv 2 \pmod{3}
\end{cases}
\]
This last calculation means that
\[ x \equiv 17 \pmod{21} \Rightarrow \begin{cases}
  x \equiv 3 \pmod{7} \\
  x \equiv 2 \pmod{3}
\end{cases} \]
This is a special case of
\[ \text{Prop: Let } a, b, m, n \in \mathbb{Z}, \quad m, n > 0, \quad n \mid m. \]
If \( a \equiv b \pmod{m} \) then \( a \equiv b \pmod{n} \).
\[ \text{Proof: } a - b = mk = n(n'k) \Rightarrow n \mid a - b \]
\[ \Rightarrow a \equiv b \pmod{n} \]
Lecture 12

Proof of CRT:

We first construct a solution

Let \( M = N_1 N_2 \ldots N_k \) and \( M_i = M / N_i \).

And note \((M_i, N_i) = 1\). Therefore, the congruence \( M_i x \equiv 1 \pmod{N_i} \)

has a solution \( y_i \).

Consider the integer

\[ x = b_1 M_1 y_1 + b_2 M_2 y_2 + \ldots + b_k M_k y_k \]

and note that \( N_i \mid M_i \) \( \forall i \neq i \)

so that \( x \equiv b_1 M_1 y_1 + b_2 M_2 y_2 + \ldots (\pmod{N_i}) \)

\[ \equiv b_i \pmod{N_i} \]

since \( M_i y_i \equiv 1 \pmod{N_i} \) by construction.

We conclude that \( x \) satisfies \((\ast)\).
We now prove the solution is unique mod $M$.

Let $x$ and $x'$ be two solutions to ($\star$) then $x \equiv x'$ (mod $N_i$) $\forall i$

$\Rightarrow N_i \mid x - x'$ $\forall i$

$\Rightarrow \text{LCM}(N_1, N_2, ..., N_k) \mid x - x'$

Exercise

Since $M = N_1 N_2 ... N_k$ and $(N_i, N_j) = 1 \forall i \neq j$

then $\text{LCM}(N_1, N_2, ..., N_k) = M$

therefore $M \mid x - x'$ $\Leftrightarrow x \equiv x'$ (mod $M$)

This proof is a constructive proof in the sense that it provides a recipe to obtain the solution instead of simply showing it exists.

This recipe will be used often.
LET US GO BACK TO THE EXAMPLE

\[
\begin{cases} 
  x \equiv 3 \pmod{7} \\
  x \equiv 2 \pmod{3} 
\end{cases}
\]

AND SOLVE IT FOLLOWING THE RECIPE IN CRT

WE HAVE \( N_1 = 7, \ b_1 = 3 \) AND \( N_2 = 3, \ b_2 = 7 \)

WE COMPUTE \( M = 3 \cdot 7 = 21, \ M_1 = \frac{M}{N_1} = \frac{21}{7} = 3, \ M_2 = \frac{M}{N_2} = \frac{21}{3} = 7 \)

WE SOLVE \( M_i \cdot x \equiv 1 \pmod{N_i} \)

\[
\begin{align*}
  \rightarrow i &= 1 : & 3 \cdot x &\equiv 1 \pmod{7} \Rightarrow y_1 &\equiv 5 \pmod{7} \\
  \rightarrow i &= 2 : & 7 \cdot x &\equiv 1 \pmod{3} \Rightarrow y_2 &\equiv 1 \pmod{3} 
\end{align*}
\]

Thus \( x \equiv 3 \cdot 5 + 2 \cdot 1 \equiv 45 + 14 \equiv 17 \pmod{21} \)

AS EXPECTED FROM THE PREVIOUS CALCULATION
Corollary: Let $N_1, N_2, \ldots, N_k$ be positive and pairwise coprime integers. Then the systems

$$\begin{align*}
X &\equiv 1 \pmod{N_1} \\
X &\equiv 1 \pmod{N_2} \\
& \vdots \\
X &\equiv 1 \pmod{N_k}
\end{align*}$$

and

$$\begin{align*}
X &\equiv -1 \pmod{N_1} \\
X &\equiv -1 \pmod{N_2} \\
& \vdots \\
X &\equiv -1 \pmod{N_k}
\end{align*}$$

have respectively the unique solution

$$X \equiv 1 \pmod{N_1 \cdots N_k} \quad \text{and} \quad X \equiv -1 \pmod{N_1 \cdots N_k}$$

Proof: Clearly $X = 1$ and $X = -1$ satisfy the systems (respectively). Then from the uniqueness part of CRT there are no other solutions mod $N_1 \cdots N_k$.\[\square\]
Example: Find $17^{-1} \pmod{55}$ using CRT.

We have to solve $17x \equiv 1 \pmod{55}$.

Since $55 = 5 \cdot 11$, we can split into

\[
\begin{cases} 
17x \equiv 1 \pmod{5} \\
17x \equiv 1 \pmod{11}
\end{cases} \iff 
\begin{cases} 
2x \equiv 1 \pmod{5} \\
6x \equiv 1 \pmod{11}
\end{cases}
\]

Note that $3 \cdot 2 \equiv 1 \pmod{5}$ and $6 \cdot 2 \equiv 1 \pmod{11}$.

Thus the system is equivalent to

\[
\begin{cases} 
x \equiv 3 \pmod{5} \\
x \equiv 2 \pmod{11}
\end{cases}
\]

We can now apply CRT. We have

\[N_1 = 5, \quad N_2 = 11, \quad b_1 = 3, \quad b_2 = 2 \]

\[M = 5 \cdot 11 = 55, \quad M_1 = \frac{M}{N_1} = 11, \quad M_2 = \frac{M}{N_2} = 5 \]

We solve $M_i \cdot x \equiv 1 \pmod{N_i}$

$1 \equiv 1 \pmod{5}$ \Rightarrow $\gamma_1 = 1$

$2 \equiv 1 \pmod{11}$ \Rightarrow $\gamma_2 = -2$

Then, \[x = b_1M_1\gamma_1 + b_2M_2\gamma_2 = 3 \cdot 11 \cdot 1 + 2 \cdot 5 \cdot (-2) = 33 - 20 = 13 \pmod{55}\]

As expected!
Example: Compute \( 8^{10003} \pmod{105} \)

Note that \( 105 = 3 \cdot 5 \cdot 7 \).

We want to find an integer \( x \) such that
\[
\begin{align*}
x &\equiv 8^{10003} \pmod{105}, \\
0 \leq x < 105
\end{align*}
\]

In particular, \( x \) satisfies
\[
\begin{align*}
x &\equiv 8^{10003} \pmod{3} \\
x &\equiv 8^{10003} \pmod{5} \\
x &\equiv 8^{10003} \pmod{7}
\end{align*}
\]

and we can apply CRT.

First note that
\[
\begin{align*}
&\begin{cases}
8 \equiv -1 \pmod{3} \\
8 \equiv -2 \pmod{5} \\
8 \equiv 1 \pmod{7}
\end{cases} \implies
\begin{cases}
x \equiv (-1)^{10003} \equiv -1 \pmod{3} \\
x \equiv (-2)^{10003} \equiv 7 \pmod{5} \\
x \equiv 1^{10003} \equiv 1 \pmod{7}
\end{cases}
\end{align*}
\]

To find \( 7 \), note that \((-2)^4 \equiv 16 \equiv 1 \pmod{5}\).

Thus \( x \equiv (-2)^{10003} \equiv (-2)^3 \pmod{5} \)
\[
\equiv (-2)^4 \cdot (-2) \equiv 1 \cdot (-8) \equiv 2 \pmod{5}
\]

We conclude that we need to apply CRT to
\[
\begin{align*}
x &\equiv -1 \pmod{3} \\
x &\equiv 2 \pmod{5} \\
x &\equiv 1 \pmod{7}
\end{align*}
\]
We have \( N_1 = 3, N_2 = 5, N_3 = 7 \)
\[ h_1 = -1, \; h_2 = 2, \; h_3 = 1 \]
\[ M = 3 \cdot 5 \cdot 7 = 105, \; M_1 = \frac{M}{N_1} = 35, \; M_2 = \frac{M}{N_2} = 21, \; M_3 = \frac{M}{N_3} = 15 \]

We solve \( M_i \equiv x \equiv 1 \pmod{N_i} \)

\[
\begin{align*}
& i = 1 \quad \left\{ \begin{array}{l}
35 \equiv 1 \pmod{3} \\
21 \equiv 1 \pmod{5} \\
15 \equiv 1 \pmod{7}
\end{array} \right. \quad \text{Gives} \quad \left\{ \begin{array}{l}
y_1 = -1 \\
y_2 = 1 \\
y_3 = 1
\end{array} \right.
\]

Hence \( x \equiv h_1 M_1 y_1 + h_2 M_2 y_2 + h_3 M_3 y_3 \)

\[ \equiv (-1)35(-1) + 2 \cdot 21 \cdot 1 + 1 \cdot 15 \cdot 1 \]

\[ \equiv 35 + 42 + 15 \equiv 92 \pmod{105} \]

Remark: Since \(-1 \equiv 2 \pmod{3}\) we could have grouped the congruences into

\[
\begin{align*}
& \left\{ \begin{array}{l}
x \equiv 2 \pmod{3} \\
x \equiv 2 \pmod{5} \\
x \equiv 1 \pmod{7}
\end{array} \right. \quad \iff \quad \left\{ \begin{array}{l}
x \equiv 2 \pmod{15} \\
x \equiv 1 \pmod{7}
\end{array} \right.
\]

And apply CRT to the last 2 congruences.
Given $a, k, m \in \mathbb{Z}$, $m > 2$ how do we compute $a^k \pmod{m}$ quickly?

**Step 1**: Write the exponent $k$ in base 2. That is, $k = 2^{r_1} + 2^{r_2} + \ldots + 2^{r_e}, 2^{r_1} > 2^{r_2} > \ldots > 2^{r_e}$

**Step 2**: Compute $a, a^2, a^4, \ldots, a^{2^{r_1}} \pmod{m}$ by successive squaring and reduction mod $m$.

**Step 3**: Compute $a^k = a^{2^{r_1}} a^{2^{r_2}} \ldots a^{2^{r_e}} = a \cdot a^{2^{r_1}} \cdot a^{2^{r_2}} \cdots a^{2^{r_e}} \pmod{m}$

**Example**: Compute $7^{54} \pmod{17}$

**Step 1**: $54 = 2^5 + 2^4 + 2 + 1 = 32 + 16 + 2 + 1$

**Step 2**: $7 \equiv 7 \pmod{17}$, $7^2 \equiv 49 \equiv 15 \equiv -2 \pmod{17}$

$7^4 \equiv (-2)^2 \equiv 4 \pmod{17}$

$7^8 \equiv 4^2 \equiv 16 \equiv -1 \pmod{17}$

$7^{16} \equiv (-1)^2 \equiv 1 \pmod{17}$, $7^{32} \equiv 1 \pmod{17}$
STEP 3: \[
\frac{51}{7} = 7
\]
\[
= 7 \cdot 7 \cdot 7 \cdot 7
\]
\[
= 7 \cdot (-2) \cdot 1 \cdot 4 \equiv -14 \equiv 3 \pmod{17}
\]
THE ISBN 10 CODE

1. It is used to identify books
2. It consists of 10 digits \(a_1, a_2, \ldots, a_{10}\) such that
   
   (i) \(0 \leq a_i \leq 9\) for \(i = 1, \ldots, 9\)
   
   (ii) \(a_{10}\) is an integer modulo 11.

We use the letter \(X\) to denote 10 \((\text{mod}\ 11)\).

An ISBN 10 code is valid if the sum

\[
S = \sum_{i=1}^{10} i \cdot a_i = 1a_1 + 2a_2 + \ldots + 10a_{10} \equiv 0 \pmod{11}
\]

**Example:** Our textbook ISBN 10 code is

0-321-50031-8

And it satisfies (as expected)

\[
1 \times 0 + 2 \times 3 + 3 \times 2 + 4 \times 1 + 5 \times 5 + 6 \times 0 + 7 \times 0 + 8 \times 3 + 9 \times 1 + 10 \times 8
\]

\[
\equiv 0 + 6 + 49 + 89 \equiv 5 + 5 + 1 \equiv 0 \pmod{11}
\]

**Example:** 44 000 0000 X is invalid

Because \(S \equiv 4 + 2 + 1 + 10 \times X \equiv 3 + 100 \equiv 4 \pmod{11}\)
REM: We can take $a_1, \ldots, a_q$ to be arbitrary and
by choosing $A_0 \equiv \sum_{i=1}^{q} ia_i = 1a_1 + 2a_2 + \ldots + q a_q$

We get $a_{q, q, \ldots, q, A_0}$ to be a valid code. Indeed,

\[
S \equiv \sum_{i=1}^{q} ia_i = \sum_{i=1}^{q} ia_i + 10 A_0 \equiv \sum_{i=1}^{q} ia_i + 10 \left( \sum_{i=1}^{q} ia_i \right) \\
= \sum_{i=1}^{q} ia_i \left( 1 + 10 \right) \equiv 0 \pmod{11}
\]

The 15BN10 code detects single errors.

Suppose $X_1 \ldots X_{10}$ transmission $\rightarrow Y_1 \ldots Y_{10}$ is received

with one single error. That is, $\exists j$ such that

$x_i = y_i \ \forall i \neq j \ \text{and} \ y_j = x_j + a, \ -10 \leq a \leq 10 \ \ \ a \neq 0$

We check if $Y_1 \ldots Y_{10}$ is valid. Indeed

\[
S_y = \sum_{i=1}^{10} iy_i = \sum_{i=1}^{10} ix_i + j y_j = \sum_{i=1}^{10} ix_i + j(x_j + a) \\
= \sum_{i=1}^{10} ix_i + ja \equiv ja \pmod{11} \neq 0 \pmod{11}
\]

Because 11 is prime and

$11 + j$ and $11 + a$
THE ISBN10 CODE DETECTS TRANSPOSITION ERRORS

Suppose \( X_1 \ldots X_{10} \rightarrow Y_1 \ldots Y_{10} \) when two digits were transposed, that is,

\[ \exists j, k \text{ such that } X_j \neq X_k \text{ and } \]

\[ Y_j = X_k, \quad Y_k = X_j, \quad Y_i = X_i \quad \forall i \neq j, k \]

We check if \( Y_1 \ldots Y_{10} \) is valid. Indeed,

\[ S_y = \sum_{i=1}^{10} iY_i = \sum_{i=1}^{10} iY_i + kX_k - kX_k + jX_j - jX_j \]

\[ = \sum_{i=1, i \neq k, j}^{10} iX_i + kY_k + jY_j + kX_k - kX_k + jX_j - jX_j \]

\[ = \sum_{i=1}^{10} iX_i + kX_j + jX_k - kX_k - jX_j \]

\[ = \sum_{i=1}^{10} iX_i + (k-j)(X_j - X_k) \]

\[ \equiv 0 + (k-j)(X_j - X_k) \neq 0 \quad (\text{mod} \, 11) \]

Because \( \forall \, k-j \) and \( 11 \mid X_j - X_k \)

Since \( \lvert |k-j|, \lvert X_j - X_k| \leq 10 \)

\[ \neq 0 \quad \neq 0 \]
DIVISIBILITY TESTS

"A number is divisible by 3 if the sum of its digits is divisible by 3."

Why is this true?

Prop: Let \( N \in \mathbb{Z}_{>0} \). Then, \( N \) is divisible by 3 or 9 if and only if the sum of its digits is divisible by 3 or 9.

Proof: Note \( 10 \equiv 1 \pmod{3} \) and \( 10 \equiv 1 \pmod{9} \).

Hence \( 10^k \equiv 1 \pmod{3} \) and \( 10^k \equiv 1 \pmod{9} \).

We write \( N \) in base 10, that is,

\[
N = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0, \quad a_k \neq 0
\]

\[
\equiv a_k + a_{k-1} + \ldots + a_1 + a_0 \pmod{3} \pmod{9}
\]

Therefore, \( 3 \mid N \iff N \equiv 0 \pmod{3} \)

\[
\iff a_k + a_{k-1} + \ldots + a_0 \equiv 0 \pmod{3}
\]

AND SIMILARLY FOR 9.
Example: \( N = 4127835 \)

\[ S = \text{sum of digits} = 4 + 1 + 2 + 7 + 8 + 3 + 5 = 30 \]

\[ \Rightarrow 3 \mid S \quad \text{but} \quad 9 \nmid S \]

So, \( 3 \mid N \) but \( 9 \nmid N \)

Proof: Let \( N \in \mathbb{Z}_{\geq 0} \).

\( N \) is divisible by 11 if and only if 11 divides the alternate sum of the digits of \( N \) in base 10.

Proof: \( 10 \equiv -1 \pmod{11} \) \( \Rightarrow \) \( 10^k \equiv (-1)^k \pmod{11} \)

Write \( N = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_1 10 + a_0 \)

\[ \equiv a_k (-1)^k + a_{k-1} (-1)^{k-1} + \ldots + a_1 + a_0 \pmod{11} \]

Thus \( N \equiv 0 \pmod{11} \) \( \implies 11 \mid a_k (-1)^k + \ldots + a_1 + a_0 \)

Example: \( N_1 = 723160823 \)

\[ S = 7 - 2 + 3 - 1 + 6 - 0 + 8 - 2 + 3 = 22 \implies 11 \mid N_1 \]

\[ N_2 = 33678924 \]

\[ S = 3 - 3 + 6 - 7 + 8 - 9 + 2 - 4 = -4 \implies 11 \mid N_2 \]
Prop: Let \( N, k \in \mathbb{Z}_{>0} \). Then, \( N \) is divisible by \( 2^k \) if and only if the integer obtained from the last \( k \) digits of \( N \) is divisible by \( 2^k \).

Example: \( N = 32688048 \)

\[ 2 \mid 8, 4 \mid 48, 8 \mid 048, 16 \mid 8048, 32 \mid 88048 \]

Thus \( 2, 4, 8, 16 \mid N \) and \( 32 \mid N \)

Proof: We have \( 10 \equiv 0 \pmod{2} \)

Then \( 10^j \equiv 0 \pmod{2^j} \)

Thus \( N = a_k 10^k + \ldots + a_1 10 + a_0 \) satisfies

\[ N \equiv a_0 \pmod{2} \rightarrow (a_0)_{10} \]

\[ N \equiv a_1 10 + a_0 \pmod{4} \rightarrow (a_1 a_0)_{10} \]

\[ N \equiv a_2 10^2 + a_1 10 + a_0 \pmod{8} \rightarrow (a_2 a_1 a_0)_{10} \]

\[ \vdots \]

\[ N \equiv a_{j-1} 10^{j-1} + \ldots + a_1 10 + a_0 \pmod{2^j} \rightarrow (a_{j-1} \ldots a_1 a_0)_{10} \]

So \( 2^k \mid N \iff 2^k \mid a_{k-1} \ldots a_0 \) \( \Box \)
**Wilson's Theorem**

**THM (Wilson):**

Let $p$ be a prime. Then $(p-1)! \equiv -1 \pmod{p}$

We will need the following lemma which is important on its own.

**Lemma 3:** Let $p$ be a prime. Let $a \in \mathbb{Z}$, $(a,p)=1$

Then $a \equiv a^{-1} \pmod{p}$ if and only if $a \equiv \pm 1 \pmod{p}$

**Proof:**

$\Rightarrow$ Suppose $a \equiv \pm 1 \pmod{p}$

Since $1, -1 \equiv 1$ and $(-1)(-1) \equiv 1 \pmod{p}$

Clearly, $a^{-1} \equiv a \pmod{p}$

$\Rightarrow$ Suppose $a \equiv a^{-1} \pmod{p}$

Then $a^2 \equiv 1 \pmod{p}$ \(\Rightarrow \) $a^2 - 1 = p \cdot k$, $k \in \mathbb{Z}$

\(\Rightarrow \) $(a-1)(a+1) = p \cdot k \Rightarrow p \mid a-1$ or $p \mid a+1$

\(\Rightarrow \) $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$

\(\blacksquare\)
The condition of \( p \) being prime is necessary. Indeed, take \( a = 3, p = 8 \)

then \( a^{-1} = 3 \) because \( 3 \cdot 3 = 9 \equiv 1 \ (\text{mod} \ 8) \)

but \( 3 \not\equiv \pm 1 \ (\text{mod} \ 8) \)

Example: take \( p = 7 \). Wilson's Theorem \( \Rightarrow (7-1)! = 6! \equiv -1 \ (\text{mod} \ 7) \)

Let's check: \( 6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \)

\( \equiv 1 \cdot 6 \cdot 1 \cdot 1 \equiv -1 \ (\text{mod} \ 7) \)

Proof of Wilson's Theorem:

For \( p = 2, 3 \) it holds because \( (2-1)! = 1! = 1 \equiv -1 \ (\text{mod} \ 2) \)

\( (3-1)! = 2! = 2 \equiv 2 \equiv -1 \ (\text{mod} \ 3) \)

So, suppose \( p \geq 5 \). We have \( p - 1 \) even.

We know that every \( a \not\equiv 0 \ (\text{mod} \ p) \) has an inverse because \( p \) is prime.

Lemma 3 \( \Rightarrow \) only 1 and \( p - 1 \) are their own inverses.

So \( 2 \cdot 3 \cdots (p-2) \equiv (2 \cdot 2^{-1}) (3 \cdot 3^{-1}) \cdots \equiv 1 \ (\text{mod} \ p) \)

\( \Rightarrow 1 \cdot (2 \cdot 3 \cdots (p-2)) \cdot (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \ (\text{mod} \ p) \)

\( \left( p - 1 \right)! \)