THE CONGURANCE 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 \( 3 \equiv 0 \pmod{3} \))

\[
z \equiv y^2 \pmod{3}
\]

Now, the possibilities for \( y \pmod{3} \) are

\[
y \equiv 0, 1, 2 \pmod{3} \implies y^2 \equiv 0, 1, 1 \pmod{3}
\]

so \( y^2 \not\equiv 2 \pmod{3} \) and we conclude

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

If instead we look mod 2 we obtain

\[
3x^2 + 2 \equiv y^2 \pmod{2} \implies x^2 \equiv y^2 \pmod{2}
\]

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

Thus the existence of solutions mod 17 says nothing about solutions in \( \mathbb{Z} \).
Example: Solve \( 4y^2 + 2x = 3 \) in \( \mathbb{Z} \)

Working \( \text{mod} \ 4 \) gives

\[ 2x \equiv 3 \pmod{4} \]

As \( y \equiv 0, 1, 2, 3 \Rightarrow 2x \equiv 0, 2, 1, 2 \equiv 3 \)

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

\[ 2x \equiv 3 \pmod{5} \]

\[ x \equiv 0, 1, 2, 3, 4 \Rightarrow 2x \equiv 0, 2, 4, 1, \not{3} \]

So \( x \equiv 4 \pmod{5} \) is a solution

Thus all integers in \([4]\) satisfy the equation
3x ≡ 9 (mod 6)

\[ x ≡ 0, 1, 2, 3, 4, 5 \Rightarrow 3x ≡ 0 (\text{mod} 6) \]

\[ 0, 3, 0, 0, 3, 0 \]

Thus there are three non-congruent solutions \( x ≡ 1, x ≡ 3, x ≡ 5 \) (mod 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 \( ax ≡ b \) (mod \( M \)) has no solutions if \( d \nmid b \).

(B) Suppose \( d | b \), then \( ax ≡ b \) (mod \( M \)) has exactly \( d \) distinct solutions modulo \( M \).

They are given by

\[ x ≡ x_0 - \frac{M}{d} t \text{ where } 0 ≤ t ≤ d-1 \]

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 \([a][x]\) and \([x]\) are inverses in \( \mathbb{Z}/m\mathbb{Z} \)

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

Examples:

\[ m = 10 \]

\[
\begin{array}{cccccccccc}
a & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\hline
\hat{a} & 1 & 1 & 7 & 7 & 3 & 3 & 9 & 9 & 1 & 1
\end{array}
\]

\[ m = 5 \]

\[
\begin{array}{cccc}
a & 0 & 1 & 2 & 3 & 4 \\
\hline
\hat{a} & 1 & 3 & 2 & 4 & 1
\end{array}
\]

Corollary: Let \( p \) be prime.

Then all \( a \neq 0 \pmod{p} \) has a unique inverse modulo \( p \).
**THM:** 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 \( \pmod{M} \) which are given by

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

where \( x_0 \) is a particular solution.

**Proof:** (A) Suppose \( ax_0 \equiv b \pmod{M} \) for some \( x_0 \in \mathbb{Z} \)

then \( ax_0 - b = My_0 \Rightarrow ax_0 + M(-y_0) = b \)

meaning that \( ax + My = b \) has the solution \( (x_0, -y_0) \). Thus \( (a, M) = d \mid b \).

By the THM for linear Diophantine equations.
(B) Suppose \( d \mid b \). Then \( aX - My = b \) has solutions

Let \( (x_0, y_0) \) be a particular solution.

The general solution is given by

\[
x = x_0 - \frac{M}{d} t, \quad y = y_0 - \frac{a}{d} t, \quad t \in \mathbb{Z}
\]

So the previous 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 \( x_0 - \frac{M}{d} t_1 \equiv x_0 - \frac{M}{d} t_2 \pmod{M} \)

\[
\iff \frac{M}{d} (t_1 - t_2) \equiv 0 \equiv \frac{M}{d} \cdot 0 \pmod{M}
\]

\[
\iff t_2 - t_1 \equiv 0 \pmod{\frac{M}{(M, \frac{M}{d})}}
\]

\[
\iff t_2 \equiv t_1 \pmod{\frac{d}{(M, \frac{M}{d})}}.
\]

\[
\uparrow \quad \text{Because} \quad \frac{M}{d} = \frac{m}{d}
\]

Therefore taking \( t \in \{0, 1, \ldots, d-1\} \)

\[
\text{gives the desired } d \text{ non-congruent solutions } \pmod{M}.
\]
Last lecture we computed inverses mod \( M \) for \( M = 5, 10 \) by trial and error. This was possible because numbers are small.

In general to compute \( a^{-1} \pmod{M} \) we need to solve the linear Diophantine equation \( ax + My = 1 \) using Euclidean algorithm.

**Example:** Compute \( 17^{-1} \pmod{55} \)

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 \( x_0 \pmod{55} \) is the inverse we are looking for because

\[
17x_0 + 55y_0 = 1 \Rightarrow 17x_0 \equiv 1 \pmod{55}
\]
Find \((17, 55)\) using 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

\[ 1 = 17 - 4 \cdot 4 = 17 - 4(55 - 17 \cdot 3) = \]
\[ = 17 - 4 \cdot 55 + 12 \cdot 17 = \]
\[ = 17 \cdot 13 - 55 \cdot 4 \]
\[ \Rightarrow x_0 = 13, \ y_0 = -4 \]

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

That is \(17 \cdot 13 \equiv 1 \pmod{55}\)

\[ \Rightarrow [17]^{-1} = [13] \text{ in } \mathbb{Z}/55 \]

We played the squaring-off game!
THE CHINESE REMAINDER THEOREM (CRT)

We have seen how to solve congruences in one variable.

How 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."

Using congruences this problem translates into finding a positive integer $x$ such that

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

This system and many others can be solved using the CRT theorem (Chinese Remainder Theorem):

Let $N_1, N_2, \ldots, N_k \in \mathbb{Z}_{>0}$ be pairwise coprime.

Let $b_1, b_2, \ldots, b_k \in \mathbb{Z}$ and consider the system

$$
\begin{align*}
   x &\equiv b_1 \pmod{N_1} \\
   x &\equiv b_2 \pmod{N_2} \\
   x &\equiv b_k \pmod{N_k}
\end{align*}
$$

Then there is a unique solution to $(*)$ mod $N_1 N_2 \ldots N_k$. 
Before the proof let's see the example

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

The first congruence gives \( x - 3 = 7k \) that is \( x = 3 + 7k \). Replacing into the second we get

\[
3 + 7k \equiv 2 \pmod{3} \Rightarrow k \equiv 2 \pmod{3}
\]

that is \( k = 2 + 3t \). Now replacing for \( k \) gives

\[
x = 3 + 7(2 + 3t) = 17 + 21t
\]

Note that 21 is the modulus predicted by CRT.

So \( x \equiv 17 \pmod{21} \) should be the solution predicted by CRT. Indeed, we check that

\[
\begin{align*}
  x = 17 + 21t &\equiv 3 + 0 \equiv 3 \pmod{7} \\
  x = 17 + 21t &\equiv 2 + 0 \equiv 2 \pmod{3}
\end{align*}
\]

This last calculation is a particular case of

Prop: Let \( a, b, n, N \in \mathbb{Z} \) with \( n > 0, N > 0 \) and \( N | n \).

If \( a \equiv b \pmod{N} \) then \( a \equiv b \pmod{N} \).

Proof: \( a - b = Nk = N(N') \Rightarrow N | a - b \iff a \equiv b \pmod{N} \).
**Proof of CRT:**

We first construct a solution.

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

Note that \( (N_i, N_j) = 1 \), 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 observe that

\[ X \equiv 0 + 0 + \ldots + b_i M_i y_i + \ldots + 0 \pmod{N_i} \]

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

We now prove the solution is unique \( \text{mod} \ M \).

Let \( X \) and \( X' \) be two solutions to \((*)\).

Then \( X \equiv b_i \equiv X' \pmod{N_i} \) \( \forall i \).

\[ \Rightarrow X - X' \text{ is divisible by } N_i \ \forall i \]

\[ \Rightarrow X - X' \text{ is divisible by } \text{lcm}(N_1, N_2, \ldots, N_k) \]

Since \( N_i \) are pairwise coprime, we have

\[ M = N_1 N_2 \ldots N_k = \text{lcm}(N_1, N_2, \ldots, N_k) \]

So \( M \mid X - X' \Rightarrow X \equiv X' \pmod{M} \).
Let us consider again

\[
\begin{align*}
\begin{cases}
X \equiv 3 \pmod{7} & N_1 = 7 \quad N_2 = 3 \\
X \equiv 2 \pmod{3} & N_1 = 3 \quad N_2 = 2
\end{cases}
\end{align*}
\]

\[M = 3 \cdot 7 = 21, \quad N_1 = \frac{N}{N_1} = 3, \quad N_2 = \frac{N}{N_2} = 7\]

we solve \( M \cdot x \equiv 1 \pmod{N_1} \):

- \( i = 1 \): \( 3 \cdot x \equiv 1 \pmod{7} \Rightarrow y_1 = 5 \pmod{7} \)
- \( i = 2 \): \( 7 \cdot x \equiv 1 \pmod{3} \Rightarrow y_2 = 1 \pmod{3} \)

Thus \( x \equiv 3 \cdot 3 \cdot 5 + 2 \cdot 7 \cdot 1 \equiv 45 + 14 \equiv 17 \pmod{21} \)

as expected.

**Corollary:** Let \( N_1, N_2, \ldots, N_k \) be positive and pairwise coprime.

Then the systems

\[
\begin{align*}
\begin{cases}
X \equiv 1 \pmod{M_1} \\
X \equiv 1 \pmod{M_2}
\end{cases}
\end{align*}
\]

\[
\begin{align*}
\begin{cases}
X \equiv -1 \pmod{N_1} \\
X \equiv -1 \pmod{N_2}
\end{cases}
\end{align*}
\]

have respectively the unique solution \( x \equiv 1 \pmod{M_1 \ldots M_k} \)

and \( x \equiv -1 \pmod{N_1 \ldots N_k} \).

**Proof:** Clearly \( x \equiv 1 \) and \( x \equiv -1 \) satisfy the systems (respectively). Then it follows from the uniqueness part of CRT that there are no other solutions \( \pmod{N_1 \ldots N_k} \).
**Example:** Find \( 17^{-1} \mod 55 \).

We have to solve \( 17x \equiv 1 \mod 55 \).

Since \( 55 = 5 \cdot 11 \) we split into the congruences:

\[
\begin{align*}
17x & \equiv 1 \mod 5 \\
17x & \equiv 1 \mod 11
\end{align*}
\]

\[
\begin{align*}
2x & \equiv 1 \mod 5 \\
x & \equiv 3 \mod 5 \\
6x & \equiv 1 \mod 11
\end{align*}
\]

Note that \( 3 \cdot 2 \equiv 1 \mod 5 \) and \( 6 \cdot 2 \equiv 1 \mod 11 \).

Thus the system is equivalent to:

\[
\begin{align*}
x & \equiv 3 \mod 5 \\
x & \equiv 2 \mod 11
\end{align*}
\]

We can now apply CRT:

\( N_1 = 5, N_2 = 11, b_1 = 3, b_2 = 2 \).

\( N = 5 \cdot 11 = 55 \), \( M_1 = \frac{N}{N_1} = 11 \), \( M_2 = \frac{N}{N_2} = 5 \).

We have to solve \( M_i x \equiv b_i \mod N_i \):

\( i = 1 \) : \( 11x \equiv 3 \mod 5 \) \( \Rightarrow y_1 = 3 \)

\( i = 2 \) : \( 5x \equiv 2 \mod 11 \) \( \Rightarrow y_2 = -2 \)

Then:

\[
x = b_1 M_1 y_1 + b_2 M_2 y_2 \equiv 3 \cdot 11 \cdot 3 + 2 \cdot 5 \cdot (-2) \equiv 33 - 20 \equiv 13 \mod 55
\]

As expected since we have seen this before using Euclidean Algorithm.
Example: Compute \( 8^{10003} \pmod{105} \)

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

We want to find an integer \( x \equiv 8^{10003} \pmod{105} \)

such that \( 0 \leq x \leq 104 \). In particular, \( x \) satisfies

\[
\begin{align*}
\begin{cases}
  x \equiv 8^{10003} \pmod{3} \\
  x \equiv 8^{10003} \pmod{5} \\
  x \equiv 8^{10003} \pmod{7}
\end{cases}
\end{align*}
\]

Therefore the CRT will give the number we need.

First note that:

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

To find \( x \), we observe

\[
(-2)^4 \equiv 16 \equiv 1 \pmod{5}
\]

Thus \( x \equiv (-2)^{10003} \equiv (-2)^3 \cdot (-2)^{2500} \equiv (-2)^3 \equiv 2 \pmod{5} \)

We conclude that we need to apply CRT to the system

\[
\begin{align*}
\begin{cases}
  x \equiv -1 \pmod{3} \\
  x \equiv 2 \pmod{5} \\
  x \equiv 1 \pmod{7}
\end{cases}
\end{align*}
\]
We have \( M_1 = 3, N_2 = 5, N_3 = 7 \)
\( b_1 = -1, b_2 = 2, b_3 = 4 \)
\( \Pi = 3 \cdot 5 \cdot 7 = 105 \), \( \frac{M_1}{N_1} = \frac{M_2}{N_2} = 35 \), \( \frac{M_3}{N_3} = 21 \), \( N_3 = 15 \)

Solving the congruences:
\[
\begin{align*}
35x &\equiv 1 \pmod{3} \\
21x &\equiv 1 \pmod{5} \\
15x &\equiv 1 \pmod{7}
\end{align*}
\]

Gives
\[
\begin{align*}
y_1 &= -1 \\
y_2 &= 4 \\
y_3 &= 1
\end{align*}
\]

Hence
\[
x \equiv b_1M_1y_1 + b_2N_2y_2 + b_3N_3y_3
\]
\[
\equiv (-1)35(-1) + 2 \cdot 21 \cdot 4 + 4 \cdot 15 \cdot 1
\]
\[
\equiv 35 + 42 + 15 \equiv 92 \pmod{105}
\]

Rem: Since \(-1 \equiv 2 \pmod{3}\) we could have grouped the congruences into:
\[
\begin{align*}
x &\equiv 2 \pmod{3} \\
x &\equiv 2 \pmod{5} \\
x &\equiv 1 \pmod{7}
\end{align*}
\]

\[
\Rightarrow \begin{align*}
x &\equiv 2 \pmod{15} \\
x &\equiv 4 \pmod{7}
\end{align*}
\]

And apply CRT to the last 2 congruences.
APPLICATIONS: DIVISIBILITY TESTS

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

Why is this true?

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

\( N \) 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 \( 10^k \equiv 1 \pmod{9} \).

Write \( N \) in base 10, that is

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

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

Therefore \( 3 \mid N \iff N \equiv 0 \pmod{3} \iff a_k + a_{k-1} + \cdots + a_1 + a_0 \equiv 0 \pmod{3} \)

And similarly for divisibility by 9. \( \Box \)
**Example:**  \( N = 4127835 \)

\[ S = \text{sum of digits} = 4 + 1 + 2 + 7 + 8 + 3 + 5 = 36 \]

**Therefore** \( 3 \mid S \) **but** \( 9 \nmid S \)

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

**Proof:** Let \( N \in \mathbb{Z}_{+} \).

\( N \) **is divisible by** \( M \) **if and only if** \( M \) **divides**

**the alternate sum of the digits of** \( N \) **(in base 10)**

\( \equiv \)

**Proof:** \( 10 \equiv -1 \pmod{11} \)

**Hence** \( 10^k \equiv (-1)^k \pmod{11} \)

**Thus**

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

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

**Thus** \( N \equiv 0 \pmod{11} \) \( \iff \) \( M \) **divides the alternate sum of the digits of** \( N \)

**Example:** \( N_1 = 323160823 \)

\[ S = 3 + 2 + 3 - 1 + 6 - 0 + 8 - 2 + 3 = 22 \quad \Rightarrow \quad M \mid N_1 \]

\( N_2 = 33678924 \)

\[ S = 3 - 3 + 6 - 7 + 8 - 9 + 2 - 4 = -4 \quad \Rightarrow \quad M \nmid N_2 \]
Prop: Let \( N, k \in \mathbb{Z}_{>0} \).

\( N \) is divisible by \( 2^k \) if and only if the integer \( N' \) obtained from the last \( k \) digits of \( N \) is divisible by \( 2^k \).

Proof: We have \( 10 \equiv 0 \pmod{2} \Rightarrow 10 \equiv 0 \pmod{2^3} \).

Write \( N = a_k 10^k + \ldots + a_1 10 + a_0 \).

Thus \( N \equiv a_0 \pmod{2} \)
\( N \equiv a_k 10 \equiv a_k \pmod{4} \)
\( N \equiv a_k 10^2 + a_1 10 + a_0 \pmod{8} \)
\( \vdots \)
\( N \equiv a_3 10^3 + \ldots + a_1 10 + a_0 \pmod{2^3} \)

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 \( 32 \mid N \).
Fast Modular Exponentiation

Given $a, k, m \in \mathbb{Z}^+$, $m \geq 2$. How to compute

Quickly $\quad a^k \pmod{m}$

**Step 1:** Write the exponent in base 2, that is

$$k = 2^{r_1} + 2^{r_2} + \ldots + 2^{r_e} \quad , \quad r_1 > r_2 > \ldots > r_e$$

**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 $\quad a^k = a^{2^{r_1}} \cdot a^{2^{r_2}} \cdot \ldots \cdot a^{2^{r_e}}$.

**Example:** Compute $7^5 \pmod{17}$

(1) $5 = 2^2 + 2^1 + 2^0 = 32 + 16 + 2 + 1$

(2) $7 \equiv 7 \pmod{17}$, $7^2 \equiv 49 \equiv 15 \equiv -2 \pmod{17}$

$$7^4 \equiv (-2)^2 \equiv 4 \pmod{17} \quad , \quad 7^8 \equiv 4^2 \equiv 16 \equiv -1 \pmod{17}$$

(3) $7^5 = 7^{4+2+16+32} = 7^5 \cdot 7^1 \cdot 7^{16} \cdot 7^{32}$

$$7^5 \equiv 7 \cdot 7 \cdot 7 \cdot 7 \equiv 7 \cdot (-2) \cdot 1 \cdot 1 \equiv -14 \equiv 3 \pmod{17}$$
WE PLACED THE SQUADRON ON THE MAP.

GIVING THE MIDTERM I BACK.
Applications: The ISBN10 code

- It is used to identify books.
- It is made of 10 digits \( a_1, a_2, \ldots, a_{10} \) such that:
  1. \( 0 \leq a_i \leq 9 \) for \( i = 1, \ldots, 9 \)
  2. \( a_{10} \) is an integer \( \text{mod} \ 10 \). We use the letter \( X \) to identify \( 10 \) \( \text{(mod} \ 11) \)

- An ISBN10 code is valid if the sum
  \[ S = \sum_{i=1}^{10} i \cdot a_i = 1 \cdot a_1 + 2a_2 + \ldots + 10a_{10} \equiv 0 \ (\text{mod} \ 11) \]

Example: Our textbook code is 0-321-50031-8

And it satisfies (as expected)

\[ 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 0 + 7 \cdot 2 + 8 \cdot 3 + 9 \cdot 1 + 10 \cdot 8 \equiv 0 + 6 + 49 + 89 \equiv 16 \ (\text{mod} \ 11) \]

Example: 1100000000 X is invalid.

Indeed, \( S = 1 \cdot 1 + 2 \cdot 0 + 10 \cdot 10 = 103 \equiv 4 \ (\text{mod} \ 11) \)
Let: We can take $a_1, \ldots, a_q$ to be arbitrary and
by taking $A_{10} \equiv \sum_{i=1}^{q} i a_i = a_1 + 2 a_2 + \ldots + q a_q$

we get a valid code. Indeed,

$S = \sum_{i=1}^{10} i a_i = a_1 + a_2 + \ldots + a_q + 10 \left( \sum_{i=1}^{q} i a_i \right) =
\left( \sum_{i=1}^{q} i a_i \right) + 10 \left( \sum_{i=1}^{q} i a_i \right) = \left( \sum_{i=1}^{q} i a_i \right) \cdot (1+10)
= 0 \pmod{11}$

The ISBN 10 code detects single errors.

Suppose $x_1, \ldots, x_{10} \xrightarrow{\text{transmission}} y_1, \ldots, y_{10}$ is received

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

$x_j = y_j \quad \forall i \neq j$ and $y_j = x_j + a, \quad -10 \leq a \leq 10, \quad a \neq 0$

We check if $y_1, \ldots, y_{10}$ is valid. Indeed

$S_y = \sum_{i=1}^{10} i y_i = \sum_{i=1}^{10} i x_i + j x_j = \sum_{i=1}^{10} i x_i + j (x_j + a)
= \sum_{i=1}^{10} i x_i + j a \equiv j a \pmod{11}$

and $j a \not\equiv 0 \pmod{11}$ since $i+j$ and $i+j$
THE ISBN 10 CODE DETECTS TRANSPOSITION ERRORS

Suppose \( X_1 \ldots X_{10} \rightarrow \bar{y}_1 \ldots \bar{y}_{10} \) where two digits were transposed. That is,

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

\[ y_j = X_k, \quad y_k = X_j, \quad y_i = X_i \quad \forall i \neq j, k \]

We check if \( \bar{y}_1 \ldots \bar{y}_{10} \) is valid. Indeed,

\[ S_y = \sum_{i=1}^{10} i \bar{y}_i = \sum_{i=1}^{10} i y_i + k X_k - k X_k + j x_j - j x_j \]

\[ = \sum_{i=1}^{10} i X_i + k y_k + j y_j - k x_k - j x_j \]

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

\[ = S_x + (k-j)(X_j - X_k) \]

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

Because \( M + k-j \) and \( M + x_j - x_k \)

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

\[ \neq 0 \]
WILSON'S THEOREM

**Theorem (Wilson):**

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

The following lemma is required to the proof, but it is important on its own.

**Lemma:** Let \( p \) be a prime. Let \( a \in \mathbb{Z} \).

Then \( a \equiv a^{-1} \pmod{p} \) if and only if \( a \equiv \pm 1 \pmod{p} \).

**Proof:** \( \iff \) Suppose \( a \equiv \pm 1 \pmod{p} \).

Since \( a \cdot 1 \equiv a \) and \( (-1)(-1) \equiv 1 \pmod{p} \), we have \( a \equiv a^{-1} \pmod{p} \).

\( \Rightarrow \) Suppose \( a \equiv a^{-1} \pmod{p} \).

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

Then \( p \mid (a-1)(a+1) \Rightarrow p \mid a-1 \) or \( p \mid a+1 \).

Then \( a \equiv 1 \pmod{p} \) or \( a \equiv -1 \pmod{p} \).

\( \because p \) being prime is necessary! Indeed,

Take \( a = 3 \) and \( p = 8 \). Then \( a^{-1} \not\equiv 3 \pmod{8} \) because \( 3 \cdot 3 = 9 \equiv 1 \pmod{8} \).
Example: Take $p = 7$. Wilson's Theorem says $(p-1)! \equiv -1 \pmod{p}$.

Indeed, $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \equiv 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \equiv 1 \cdot 6 \cdot 1 \cdot 1 \equiv -1 \pmod{7}$

Proof of Wilson's Theorem:

For $p = 2, 3$ it is true. Indeed $(2-1)! = 1 \equiv -1 \pmod{2}$

$(3-1)! = 2 \equiv -1 \pmod{3}$

Suppose $p > 3$. We have $p-1$ even.

We know that every $a \neq 0 \pmod{p}$ has an inverse $a^{-1}$.

By the lemma only $1$ and $p-1$ are their own inverses.

So $2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv (2 \cdot 2^{-1}) (3 \cdot 3^{-1}) \ldots \equiv 1 \pmod{p}$

$\Rightarrow 1 \cdot (2 \cdot 3 \cdot \ldots \cdot (p-2)) (p-1) \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}$

$\Rightarrow (p-1)!$ as needed.

Proposition: Let $N \in \mathbb{Z}^+$. If $(N-1)! \equiv -1 \pmod{N}$ then $N$ is prime.

Proof: Suppose $N = a \cdot b$. We will show that $a = 1$.

We can assume $a \leq b < N$. Note $a \mid (N-1)!$.

Now $(N-1)! \equiv -1 \pmod{N}$ implies $N \mid (N-1)! + 1$ implies $a \mid (N-1)! + 1$ implies $a \mid (N-1)! + 1 - (N-1)! = 1$ implies $a = 1$. $\square$


Lecture 15

**Fermat's Little Theorem (FLT)**

**Theorem (Wilson):** If \( p \) is a prime then \((p-1)! \equiv -1 \pmod{p}\)

**Theorem (FLT):**

Let \( p \) be a prime. Let \( a \in \mathbb{Z}^\ast \), \((a, p) = 1\).

Then \( a^{p-1} \equiv 1 \pmod{p} \)

**Proof:** Consider the sequence of integers

\[
a, 2a, 3a, \ldots, (p-1)a
\]

We **claim** that: These integers are all distinct \( \pmod{p} \) and none of them is congruent to \( 0 \) or \( \pm a \).

Therefore, \( a \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p} \) (i.e. multiplication by \( a \) is reordering then)

Thus since \( a \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a \equiv a^{p-1} \cdot (1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1)) \pmod{p} \)

We get \( a^{p-1} \cdot (p-1)! \equiv (p-1)! \)

\( \Rightarrow \) \( a^{p-1} \cdot (-1) \equiv -1 \pmod{p} \)

(Wilson's Theorem)

\( \Leftrightarrow \) \( a^{p-1} \equiv 1 \pmod{p} \), as desired
We now prove the claim:

→ Suppose \( ka \equiv k'a \pmod{p} \). Note \( a^{-1} \) exists.

Then \( (ka)^{-1} \equiv (k'a)^{-1} \pmod{p} \) \( \Rightarrow k \equiv k' \pmod{p} \)

\( \Rightarrow k = k' \) since \( 1 \leq k, k' \leq p-1 \)

→ We have \( p \nmid a \) and \( k \), so \( ka \not\equiv 0 \pmod{p} \)

\[ \square \]

Corollary: \( a^p \equiv a \pmod{p} \) \( \forall a \in \mathbb{Z} \)

Proof: \( p \mid a \) then \( a \equiv a \pmod{p} \)

If \( p \nmid a \) by FLT \( a^{p-1} \equiv 1 \pmod{p} \)

\( \Rightarrow a^p \equiv a \pmod{p} \)

\[ \square \]

Corollary: Let \( a \in \mathbb{Z} \) s.t. \( (a, p) = 1 \).

Then \( a^{p-2} \equiv a^{-1} \pmod{p} \)

Proof: FLT \( \Rightarrow a^{p-1} \equiv 1 \pmod{p} \) \( \Leftrightarrow a \cdot (a^{-1}) \equiv 1 \pmod{p} \)

Corollary: Let \( a \in \mathbb{Z} \), \( (a, p) = 1 \).

If \( d \equiv e \pmod{p-1} \) then \( a^d \equiv a^e \pmod{p} \)

Proof: If \( d = e \), it is direct. Suppose \( d > e \).

We have \( d - e = (p-1)k \), \( k \in \mathbb{Z}_{>0} \). Thus,

\[ d = e + (p-1)k \Rightarrow a^d = a^e \cdot (a^{p-1})^k \equiv a^e \cdot a^k \equiv a^e \pmod{p} \]

\[ \square \]
Example: (i) Compute $3^{20} \pmod{101}$. We have

$$3^{20} \equiv 1 \pmod{101}$$

(ii) Compute $2^{180} \pmod{87}$.

Note $p = 87$ is prime and $p-1 = 86$.

$180 \equiv 4 \pmod{86} \Rightarrow 2^{180} \equiv 2^{4} \equiv 16 \pmod{87}$

Corollary 3

**Primality Testing**

The converse of Wilson's Theorem gives a Primality Test

Proof: Let $N \in \mathbb{Z}_{>1}$.

If $(N-1)! \equiv -1 \pmod{N}$ then $N$ is prime.

Proof: Suppose $N = a \cdot k$. We will show that $a = 1$.

We can assume $1 < a < N$. Note $a \mid (N-1)!$

We have $(N-1)! \equiv -1 \pmod{N} \Rightarrow N \nmid (N-1)! + 1$

$\Rightarrow a \nmid (N-1)! + 1$ (since $a \nmid N$)

$\Rightarrow a \nmid ((N-1)! + 1 - (N-1)! = 1 \Rightarrow a = 1$)

This test is only good theoretical because computing $(N-1)! \pmod{N}$ is hard.
**Fermat's Test:** Let $1 < b < N$

If $b^{N-1} \not\equiv 1 \pmod{N} \implies N$ is composite.

**Proof:** If $N$ is prime we have $(b,N)=1$ and $b^{N-1} \equiv 1 \pmod{N}$ by FLT.

**Example:** $2^{30} \equiv 64 \pmod{91}$

Since $64 \not\equiv 1 \pmod{91}$ it follows $91$ is composite.

**Def:** If $N$ is composite but $b^{N-1} \equiv 1 \pmod{N}$ for some $1 < b < N$ we say that $N$ is a pseudoprime to the base $b$.

**Example:**

(i) $340$

\[ 2^{340} \equiv 1 \pmod{341} \text{ but } 341 = 11 \times 31 \]

\[ \Rightarrow 341 \text{ is pseudoprime for base } b = 2. \]

(ii) $3^{340} \equiv (3^{30})^{11} \times 3^{10} \equiv 3^{10} \pmod{31}$

\[ \text{Since } 3^{10} \equiv (3^3)^3 \times 3 \equiv (-4)^3 \times 3 \equiv 25 \pmod{31} \]

\[ \text{we have } 3^{340} \not\equiv 1 \pmod{31} \]

\[ \Rightarrow 3^{340} \not\equiv 1 \pmod{341} \]

Thus $341$ fools Fermat's test in base $2$.

But not in base $3$. 
DEF: We call an integer $N$ a **Carmichael Number** if it is a pseudoprime for every base $b$ such that $(N, b) = 1$.

Thus, suppose $N = p_1 \cdots p_r$ where $p_i$ are distinct primes such that $p_i - 1 \mid N - 1 \quad \forall i$.

Then $N$ is a Carmichael Number.

**Proof:** We have $N - 1 = (p_i - 1)k_i \quad \forall i, k_i \in \mathbb{Z}^+$.

Thus $b^{N-1} \equiv (b^{p_i-1})^{k_i} \equiv 1^{k_i} \equiv 1 \pmod{p_i}$ (by FLT since $(b, N) = 1 = (b, p_i)$)

Therefore, the system of congruences is satisfied

\[
\begin{align*}
1^{N-1} & \equiv 1 \pmod{p_i} \\
1^{N-1} & \equiv 1 \pmod{p_i} \quad \text{CNTR}
\end{align*}
\]

Hence $N$ is a pseudoprime for base $b$ and since $b$ is arbitrary we conclude $N$ is a CN.

**Example:** $561 = 3 \cdot 11 \cdot 17$ is a Carmichael Number because $3 - 1 = 2$; $11 - 1 = 10$, $17 - 1 = 16$.

All divide $561 - 1 = 560 = 2^4 \cdot 5 \cdot 7$. 
Miller's Test:

1. Let $N$ be an odd positive integer.

2. Suppose $N$ is a pseudoprime in base $b > 2$. That is, $b^\frac{N-1}{2} \equiv \pm 1 \pmod{N}$.

3. Let $x = b^\frac{N-1}{2} \pmod{N}$.

Recall: If $N$ is prime and $x_0^2 \equiv 1 \pmod{N}$, then $x_0 \equiv \pm 1 \pmod{N}$.

Thus, if $N$ is prime, since $x^2 = b^\frac{N-1}{2} \equiv 1 \pmod{N}$, we conclude $x \equiv \pm 1 \pmod{N}$.

Hence, if $b^\frac{N-1}{2} \not\equiv \pm 1 \pmod{N}$ then $N$ is composite.

If $N-1$ is divisible by 4 and $b^\frac{N-1}{4} \equiv 1 \pmod{N}$, we repeat with $y = b^\frac{N-1}{4}$.

Again, $y^2 \equiv b^\frac{N-1}{2} \equiv 1 \pmod{N} \Rightarrow y \equiv \pm 1 \pmod{N}$ if $N$ is prime. Thus $b^\frac{N-1}{4} \not\equiv \pm 1 \Rightarrow N$ is composite.

We can repeat while $\frac{N-1}{2^k}$ is an integer.

Example: We have seen that $N = 561$ is the smallest Carmichael number, thus $b^{560} \not\equiv 1 \pmod{561}$ whenever $\gcd(b, 561) = 1$.
Take \( b = 5 \), we have \( 5 \equiv 67 \equiv 1 \pmod{561} \).

Take \( b = 2 \), we have \( 2^{280} \equiv 1 \pmod{561} \)

But \( 2^{140} \equiv 67 \equiv 1 \pmod{561} \).

So depending on the base \( b \), we may need different number of steps in Miller's Test.

Q: Can a composite integer fool Miller's Test for every base?

Example: Let \( N = 2047 = 23 \cdot 89 \).

Then \( 2^{1023} \equiv 1 \pmod{2047} \).

So that \( N \) is a pseudoprime in base \( b = 2 \).

Moreover, \( N - 1 = 1023 \) and \( (2^{11})^{93} = 2048^{93} \equiv 1 \pmod{2047} \).

So 2047 fools Miller's Test for base \( b = 2 \).

THM: If \( N \) is positive, odd and composite then \( N \) fools Miller's Test for at most \( \frac{N-1}{q} \) bases \( b \) s.t. \( 9 \leq b \leq N-1 \).

Rabin's Probabilistic Test: Let \( N \in \mathbb{N} \), pick \( b_1, \ldots, b_k \in \mathbb{N} \)

s.t. \( 1 < b_i < N-1 \). If \( N \) is composite the probability that it passes Rabin's test for all \( b_i \) is less than \( \frac{1}{4^k} \).
THE POLLARD p-1 FACTORIZATION METHOD

Let \( N \) be a large integer.

1. Compute \( R_k \equiv 2^{k!} \pmod{N} \) recursively using fast modular exponentiation and the formula \( R_k \equiv R_{k-1}^k \pmod{N} \).

2. At each step compute \((R_{k-1}, N)\) with the Euclidean algorithm. Since \( 0 \leq R_k \leq N-1 \) we have \( R_{k-1} < N \). Hence, if \((R_{k-1}, N) > 1\) we have found a proper divisor of \( N \).

Q: Why does it work?

→ Suppose \( p \mid N \) and \( p-1 \mid k! \) for some \( k \) (always possible for \( k! \) large).

→ Thus \( k! = (p-1)q \) and we have

\[
2^{k!} = 2^{(p-1)q} = (2^{p-1})^q \equiv 1^q \equiv 1 \pmod{p}
\]

→ \( p \mid 2^{k!} - 1 \)

→ We also have \( R_k = 2^{k!} + q'N \implies R_{k-1} = (2^{k!}-1) + q'N \)

→ \( p \mid R_{k-1} \) (because \( p \mid N \) and \( p \mid 2^{k!}-1 \))

Therefore \( p \mid (R_{k-1}, N) \)
**Example:** \( N = 10403 \)

\[
\begin{align*}
L_1 &= 2^2 = 4 \quad (\text{mod } N) \\
L_2 &= 4^3 = 64 \\
L_4 &= 64^4 = 7580 \\
L_5 &= 7580^2 = 4438 \\
L_{10} &= 9798
\end{align*}
\]

\[
\begin{align*}
(N, R_{10} - 1) &= 7 \\
(N, 9798) &= 1 \\
(N, 7580) &= 1 \\
(N, 4438) &= 1 \\
(N, 9798) &= 101
\end{align*}
\]

We obtain \( 10403 = 101 \times 103 \)

**Remarks:**

(i) This method is good if we can find small \( k \) such that \( p - 1 \mid k! \) for some \( p / N \).

This is likely to happen when \( p - 1 \) has small prime factors.

\[
p = 101, \quad p - 1 = 100 = 2^2 \cdot 5^2
\]

\( 100 \mid k! \) for \( k \geq 10 \) but \( 100 \not\mid 9! \)

(ii) A large \( k \) always exists but is not practical.

(iii) We can replace 2 by any other base \( 6 \pm 2 \).

(iv) In practice, this is used after trial division by small primes and before harder methods (which are not part of this course!)
Example of \( p-1 \) Pollard Factorization Method:

\[
N = 10403 = 101 \times 103
\]

<table>
<thead>
<tr>
<th>( k )</th>
<th>( R_k \equiv R_{k-1}^2 \mod N )</th>
<th>( (R_{k-1}, N) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>( 2^2 \equiv 4 \mod N )</td>
<td>( (N, 3) = 1 )</td>
</tr>
<tr>
<td>3</td>
<td>( 4^3 \equiv 64 )</td>
<td>( (N, 64) = 1 )</td>
</tr>
<tr>
<td>4</td>
<td>( 64^4 \equiv 7580 )</td>
<td>( (N, 7579) = 1 )</td>
</tr>
<tr>
<td>5</td>
<td>( 7580^5 \equiv 4438 )</td>
<td>( (N, 4437) = 1 )</td>
</tr>
<tr>
<td>10</td>
<td>( 4438^9 \equiv 9779 )</td>
<td>( (N, 9779) = 101 )</td>
</tr>
</tbody>
</table>

**Remark:** This method is likely to succeed when \( p-1 \) has small prime factors.

For the previous example:

- \( p = 101 \), \( p-1 = 100 = 2^2 \times 5^2 \) has small factors.
- Note also \( 100 \equiv 1 \mod 101 \) for \( k = 0 \) but \( 100 \not\equiv 1 \mod 9 \).
Euler's $\phi$ Function and Euler's Theorem

**Theorem (Fermat):** Let $p$ be prime and $a \in \mathbb{Z}$ coprime to $p$.

Then $a^p \equiv a \pmod{p}$

**Q:** What if instead of $p$ we use a modulus $m$ which is not a prime?

Which power of $a^x$ is guaranteed to be congruent to $1 \pmod{m}$?

**A:** The answer is given by Euler's Theorem. Before stating it we need to introduce a very important function

**Definition:** Let $N \in \mathbb{Z}^+$. The Euler $\phi$-function is defined by $\phi(N) = \# \{ x \in \mathbb{Z} : 1 \leq x \leq N \text{ and } (x,N) = 1 \}$

That is, it counts the number of positive integers up to $N$ that are coprime to $N$

**Example:**
- $\phi(1) = 1$; $\phi(2) = 1$
- $\phi(3) = 2$ since $1, 2$ are coprime to $3$
- $\phi(6) = 2$ since from $1, 2, 3, 4, 5, 6$ only $1, 5$ are coprime to $6$
- $\phi(p) = \# \{ x \in \mathbb{Z} : 1 \leq x \leq p \text{ and } (x,p) = 1 \} = p - 1$
**Theorem (Euler):** Let $a, m \in \mathbb{Z}$ with $m > 0$ and such that $(a, m) = 1$. Then \[ a^{\phi(m)} \equiv 1 \pmod{m} \]

**Corollary:** Let $m = p$ be a prime. Then \[ \phi(p) = p - 1 \] and \[ a^{p-1} \equiv 1 \pmod{p} \]

This means that FLT is a special case of Euler's Theorem.

**Proof of Euler's Theorem:** Let $a \in \mathbb{Z}$, $(a, n) = 1$.

Let $a_1, a_2, \ldots, a_{\phi(n)}$ be the distinct positive integers $\leq n$ such that $(a_i, n) = 1$ (by def of $\phi(n)$).

**Claim:** The integers $a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\phi(n)}$ are distinct mod $n$, satisfy $(a \cdot a_i, n) = 1$ (and are not congruent to zero).

Therefore: \[ (a \cdot a_1) \cdot (a \cdot a_2) \cdots (a \cdot a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{m} \]

\[ \Leftrightarrow \quad a^{\phi(n)} (a_1 a_2 \cdots a_{\phi(n)}) \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{n} \].

Since $(a_1 a_2 \cdots a_{\phi(n)}, n) = 1$, the number $a_1 a_2 \cdots a_{\phi(n)}$ is invertible mod $n$, hence \[ a^{\phi(n)} \equiv 1 \pmod{n} \]
We now prove the claim:

\[ \rightarrow \text{Suppose } (a; a_i, n) > 1 \text{ for some } i. \text{ The } \exists p \text{ s.t. } p|a_i \text{ and } p|m \]
\[ \rightarrow (p|a \text{ and } p|m) \text{ on } (p|a_i \text{ and } p|m) \]
\[ \rightarrow (a, n) > 1 \text{ on } (a_i, n) > 0 \text{ XXX} \]

\[ \rightarrow \text{Suppose } a \cdot a_i \equiv a \cdot a_j \pmod{n}. \text{ Since } (a, n) = 1 \text{ the inverse } a_i^{-1} \text{ exists hence } a_i^{-1}(a \cdot a_i) \equiv a_i^{-1}(a \cdot a_j) \pmod{n} \]
\[ \Rightarrow a_i^{-1} \equiv a_j^{-1} \pmod{n} \text{ with } 0 \leq a_i, a_j \leq n-1 \]
\[ \Rightarrow a_i = a_j \]

**DEF:** A set of integers with \( \phi(n) \) elements which are coprime to \( n \) and no two of them are congruent modulo \( n \) is a **reduced residue system modulo \( n \)**

**Corollary (of the claim):** Let \( a \in \mathbb{Z}^*, (a, n) = 1. \)

If \( \{a_1, a_2, \ldots, a_{\phi(n)}\} \) is a reduced residue system modulo \( m \)

then \( \{a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\phi(n)}\} \) also is
**Theorem:** (Formula for \( \phi \)) Let \( N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \ a_k \geq 1. \)

Then,

\[
\phi(N) = N \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\]

**Example:** \( \phi(100) = \phi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40 \)

**Example:** Compute the last two (decimal) digits of \( 3^{50} \)

**Want:** \( 3^{50} \pmod{100} \)

**Note that** \( 40 \equiv 3 \pmod{100} \) by Euler's Theorem,

\( 3^5 = 3 \cdot 3 \equiv 9 \cdot 3 \equiv 27 \equiv (-19)^2 \cdot 3 \equiv 49 \pmod{100} \)

**Example:** Solve the equation \( \phi(N) = 8 \)

Let \( N = p_1^{a_1} \cdots p_k^{a_k}. \) Then \( \phi(N) = \prod_{j=1}^{k} \frac{p_j - 1}{p_j} \)

- \( \phi(N) = 8 \Rightarrow p_j - 1 \) otherwise \( \phi(N) > p_j - 1 > 8 \)
- \( p_j \neq 7 \) otherwise \( p_j - 1 = 6/8 \) xxx. Thus \( N = 2^2 \cdot 3 \cdot 5 \)
- \( a = 0 \) or \( a = 1 \) otherwise \( 3 \mid 8; \) similarly \( c = 0 \) or \( c = 1 \).

1. \( b = c = 0 \Rightarrow N = 2 \overset{(a=1)}{\Rightarrow} \phi(N) = 2^{a-1} = 8 \Rightarrow a = 4 \Rightarrow N = 16 \)
2. \( b = 0, c = 1 \Rightarrow N = 2 \cdot 5 \overset{(a=1)}{\Rightarrow} \phi(N) = 2 \cdot 4 = 8 \Rightarrow a = 2 \Rightarrow N = 20 \)
3. \( b = 1, c = 0 \Rightarrow N = 2 \cdot 3 \overset{(a=1)}{\Rightarrow} \phi(N) = 2^{a-1} = 8 \Rightarrow a = 3 \Rightarrow N = 24 \)
4. \( b = c = 1 \Rightarrow N = 2 \cdot 3 \cdot 5 \overset{(a=1)}{\Rightarrow} \phi(N) = 2^{a-1} = 8 \Rightarrow a = 1 \Rightarrow N = 30 \)

For \( a = 0 \) case (4) also gives \( \phi(N) = 15 \) since \( \phi(15) = 8 \) also works!
LECTURE 18

**ARITHMETIC FUNCTIONS**

**DEF:** A function whose domain is \( \mathbb{Z}_{>0} \) is called an **ARITHMETIC FUNCTION**

**Examples:**

1) \( f(n) = 1 \quad \forall n \in \mathbb{Z}_{>0} \)

2) \( f(n) = n \quad \forall n \in \mathbb{Z}_{>0} \)

3) \( \phi(n) \) "The Euler \( \phi \)-function"

4) \( \tau(n) = "Number of positive divisors of \( n"\)"

5) \( \sigma(n) = \"Sum of positive divisors of \( n\)"\)

**Example:** Take \( n = 6 \). Its positive divisors are \( \{1, 2, 3, 6\} \). Thus \( \tau(6) = 4 \),

\[ \sigma(6) = 1 + 2 + 3 + 6 = 12 \]

**DEF:** An arithmetic function \( f \) is called **MULTIPLICATIVE** if \( f(m \cdot n) = f(m) \cdot f(n) \) whenever \( (m, n) = 1 \).

The function \( f \) is called completely **MULTIPLICATIVE** if \( f(m \cdot n) = f(m) \cdot f(n) \) \( \forall m, n \).
The function $\phi(n)$ is multiplicative.

**Proof:** Let $n_1, n_2 > 0$ be coprime.

We write the positive integers up to $n_1 \cdot n_2$ in the form

\[
\begin{array}{cccc}
1 & n_1 + 1 & 2n_1 + 1 & \ldots & (n_2-1)n_1 + 1 \\
2 & n_1 + 2 & 2n_1 + 2 & \ldots & (n_2-1)n_1 + 2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
N_1 & 2n_1 & 3n_1 & \ldots & n_1 \cdot n_2
\end{array}
\]

- Suppose $1 \leq r \leq n_1$ and $(r, n_1) = d > 1$. Then all the numbers in the $r$-th row are divisible by $d$.

Thus they are not coprime to $n_1 \cdot n_2$.

- Hence there are $\phi(n_1)$ rows that may contain numbers which are coprime to $n_1 \cdot n_2$.

- Suppose $(r, n_1) = 1$. Then the numbers in the $r$-th row are coprime to $n_1$.

The $r$-th row has $n_2$ elements which are not congruent mod $n_2$ because

$$k \cdot n_1 + r = k' \cdot n_1 + r \quad (mod \quad n_2) \Rightarrow k \equiv k' \Rightarrow k = k'$$

Thus exactly $\phi(n_2)$ of them are coprime to $n_2$. Since they are also coprime to $n_1$ they are coprime to $n_1 \cdot n_2$.

Because there are $\phi(n_1)$ rows, each containing $\phi(n_2)$ integers coprime to $n_1 \cdot n_2$ we conclude $\phi(n_1 \cdot n_2) = \phi(n_1) \cdot \phi(n_2)$.
Here is a method to produce multiplicative functions.

**Theorem:** Let \( f \) be an arithmetic function. Define the arithmetic function \( F \) by
\[
F(N) = \sum_{d|N, \ d > 0} f(d) \quad \forall N \in \mathbb{Z}^+.
\]

If \( f \) is multiplicative then \( F \) is multiplicative.

**Theorem:** \( \sigma(N) \) and \( \tau(N) \) are multiplicative.

**Proof:** We can write \( \tau \) and \( \sigma \) as
\[
\tau(N) = \sum_{d|N, \ d > 0} 1, \quad \sigma(N) = \sum_{d|N, \ d > 0} d.
\]

Since \( f(N) = 1 \) and \( f(N) = N \) are multiplicative, the result now follows from previous theorem.
Proof of Theorem:

**Want:** \( F(N_1 \cdot N_2) = F(N_1) \cdot F(N_2) \)

if \((N_1, N_2) = 1\)

We have \( F(N_1 \cdot N_2) = \sum_{d \mid N_1 \cdot N_2, d > 0} f(d) \)

**Claim:** Since \((N_1, N_2) = 1\) each divisor \(d\) of \(N_1 \cdot N_2\) can be written as \(d = d_1 \cdot d_2\) where \((d_1, d_2) = 1\), \(d_1 \mid N_1\), \(d_2 \mid N_2\). Also, each such product \(d_1 \cdot d_2\) is a divisor of \(N_1 \cdot N_2\).

Thus \( F(N_1 \cdot N_2) = \sum_{d_1 \mid N_1, d_2 \mid N_2, d_1 > 0, d_2 > 0} f(d_1) \cdot f(d_2) \)

\[= \left( \sum_{d_1 \mid N_1, d_1 > 0} f(d_1) \right) \left( \sum_{d_2 \mid N_2, d_2 > 0} f(d_2) \right) \]

\[= F(N_1) \cdot F(N_2) \]

\(\square\)
Formulas For $\phi, \sigma, \tau$

Let $N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ with $p_i$ distinct.

Let $f$ be $\phi$, $\sigma$, or $\tau$. Then

$$f(N) = f(p_1^{a_1}) \cdot f(p_2^{a_2}) \cdots f(p_k^{a_k})$$

Thus to find a formula for $f$ it is enough to give a formula for $f(p_i^{a_i})$.

Lemma: $\phi(p^{a}) = p^a - p^{a-1} = p^a (1 - \frac{1}{p})$

Proof: (Note $\phi(p) = p - 1$ is a special case.)

$(N, p^a) = 1 \Rightarrow (N, p) = 1$

The multiples of $p$ which are $\leq p^a$ are the numbers of the form $k \cdot p$ for $1 \leq k \leq p^{a-1}$

Thus, $\phi(p^a) = p^a - p^{a-1}$ $\Box$

Thm: $\phi(N) = \prod_{p_i \mid N} (1 - \frac{1}{p_i}) = \frac{N}{\prod_{p_i \mid N} p_i}$

Proof: $\phi(N) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) = p_1^{a_1} (1 - \frac{1}{p_1}) \cdots p_k^{a_k} (1 - \frac{1}{p_k})$

$= p_1^{a_1} \cdots p_k^{a_k} \left( 1 - \frac{1}{p_1} \right) \cdots \left( 1 - \frac{1}{p_k} \right) = \prod_{p_i \mid N} (1 - \frac{1}{p_i})$ $\Box$
THM: \( \text{Let } N = p_1^{a_1} \cdots p_k^{a_k}, \) \( p_i \text{ distinct } a_i > 1. \)

THEN \( \begin{cases} \sigma(N) = \prod_{i=1}^{k} (a_i+1) \\ \tau(N) = \prod_{i=1}^{k} \left( \frac{p_i^{a_i+1}}{p_i - 1} \right) \end{cases} \)

Proof: It is enough to compute \( \sigma(p^a) \) and \( \tau(p^a) \).

- The positive divisors of \( p^a \) are \{1, p, p^2, ..., p^a\}.
- In particular, \( p^a \) has \( a+1 \) positive divisors so \( \tau(p^a) = a+1 \).
- \( \sigma(p^a) = 1 + p + ... + p^a = \frac{p^{a+1} - 1}{p - 1} \) by the formula for the sum of terms in a geometric progression.

\[ \square \]

Example: \( N = 100 = 2^2 \cdot 5^2 \)

\[ \begin{align*} \sigma(N) &= \frac{3}{2-1} \cdot \frac{6}{5-1} = 7.31 = 217 \\ \tau(N) &= (2+1)(2+1) = 9 \]
THM: Let \( N \in \mathbb{Z}_{>0} \). Then \( \sum_{d|N, d>0} \phi(d) = N \)

**Proof:** \( F(N) = \sum_{d|N, d>0} \phi(d) \) is multiplicative because \( \phi(n) \) is multiplicative.

Thus \( F(N) = F(p_1^{a_1}) \cdots F(p_k^{a_k}) \)

where \( N = p_1^{a_1} \cdots p_k^{a_k} \).

Note that \( F(p^a) = \sum_{0 \leq i \leq a} \phi(p^i) \)

\[ = 1 + (p-1) + (p^2 - p) + \cdots + (p^a - p^{a-1}) = p^a \]

Thus \( F(N) = p_1^{a_1} \cdots p_k^{a_k} = N \)

\[ \exists \]

**Example:** \( N = 12 \)

The positive divisors are \( \{1, 2, 3, 4, 6, 12\} \)

\( \phi(1) = \phi(2) = 1 \)

\( \phi(3) = \phi(4) = \phi(6) = 2 \)

\( \phi(12) = 4 \)

AND \( 1 + 1 + 2 + 2 + 2 + 4 = 12 = N \) as expected!
**Example:** Solve $\phi(N) = 1$

Let $N = p_1^{a_1} \cdots p_k^{a_k}$. 

$$\phi(N) = \prod_{i=1}^{k} p_i^{a_i - 1} (p_i - 1)$$

Suppose $\phi(N) = 1$. Then $p_i - 1 \mid 1 \Rightarrow p_i = 2 \ \forall p_i \mid N$

Thus if $N \neq 1$ then $N = p_1 2^{a_1}$, $a_1 \geq 1$

$$\Rightarrow \phi(N) = 2 ^ {a_1 - 1} \cdot 1 = 1 \Rightarrow a_1 = 1 \Rightarrow N = 2$$

Clearly $[N = 1]$ is also a solution.

**Example:** Solve $\phi(N) = 3$

Let $N = p_1^{a_1} \cdots p_k^{a_k}$. Then $p_i - 1 \mid 3 \ \forall p_i \mid N$

$$\Rightarrow p_i = 1 = 3 \mbox{ or } p_i - 1 = 1 \Rightarrow p_i = 4 \mbox{ or } p_i = 2$$

Note 4 is not a prime. Then $N = 2^{a_2}$, $a_2 \geq 0$.

- If $a_2 = 0$ then $N = 1$ is not a solution since $\phi(1) = 1$.
- If $a_2 \geq 1$ then $\phi(N) = 2^{a_2 - 1} \cdot (2 - 1) = 3$

Thus is impossible!

There are no solutions for $\phi(N) = 3$. 
**Perfect Numbers**

**DEF:** An integer $N > 0$ is called Perfect if $\sigma(N) = 2N$.

**Ex:** $N = 6$. Positive Divisors $\{1, 2, 3, 6\}$

$\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$

**Ex:** $N = 28$. Positive Divisors $\{1, 2, 4, 7, 14, 28\}$

$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28$

**DEF:** We call the integer $M_N = 2^N - 1$ the $N$-th Mersenne number. If $M_N$ is prime we say Mersenne Prime.

**THM:** If $M_N$ is prime then $N$ is prime.

**Proof:** Suppose $N = a \cdot b$ with $1 < a, b < N$

We have

$2^N - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + 2^{a(b-3)} + ... + 2^{a1})$

with both factors $> 1$. Thus $M_N$ is not prime.
Example:

\[2^5 - 1 = 31 \text{ is prime}\]
\[2^7 - 1 = 127 \text{ is prime}\]
\[2^{11} - 1 = 2047 = 23 \times 89 \text{ not prime}\]
There is a 1-1 correspondence between Mersenne Primes and **even** perfect numbers.

**Theorem:** Let $N \in \mathbb{Z}_{>0}$.

Then $N$ is an even perfect number if and only if $N = 2^p (2^p - 1)$ where $2^p - 1$ is a prime number.

**Proof:**

$(\Rightarrow)$ Let $2^p - 1$ be a prime number. So $p$ is also prime by the previous theorem.

Write $N = 2^{p-1} (2^p - 1)$ and compute

$$
\sigma(N) = \sigma(2^{p-1} (2^p - 1)) = \sigma(2^{p-1}) \sigma(2^p - 1) = \frac{2^p - 1}{2^p - 1} \cdot 2^p = 2(2^{p-1} (2^p - 1))
$$

Since $\sigma$ is multiplicative, $(2^{p-1}, 2^p - 1) = 1$.

$(\Leftarrow)$ By the formula for $\sigma$.

Because $2^p - 1$ is prime or also by the formula $2 \cdot N$.
Let \( N \) be an even perfect number.

Write \( N = 2^a \cdot b, \ a, b \in \mathbb{Z}_+, \ b \ odd, \ a > 1 \)

\[ \sigma(N) = \sigma(2^a) \sigma(b) = \left( \frac{2^{a+1} - 1}{2 - 1} \right) \sigma(b) = (2^{a+1} - 1) \sigma(b) \]

\( \sigma \) is multiplicative

Since \( N \) is perfect \( \sigma(N) = 2N = 2 \left( 2^a \cdot b \right) = 2^{a+1} \cdot b \)

\[ \Rightarrow \left( 2^{a+1} - 1 \right) \sigma(b) = 2^{a+1} \cdot b \hspace{1cm} (\star) \]

\[ \Rightarrow 2^{a+1} \mid \sigma(b) \Rightarrow \sigma(b) = 2^{a+1} \cdot c \hspace{1cm} (\star \star) \]

Inserting in \( (\star) \) gives \( \left( 2^{a+1} - 1 \right) 2^{a+1} \cdot c = 2^{a+1} \cdot b \)

\[ \Rightarrow \left( 2^{a+1} - 1 \right) c = b \hspace{1cm} (\Delta) \]

We will show that \( c = 1 \)

Suppose \( c > 1 \). By \( (\Delta) \) we see that \( b \) has at least three positive divisors \( a, c, b \) thus \( \sigma(b) \geq 1 + b + c \)

But \( \sigma(b) = 2^{a+1} \cdot c = (2^{a+1} - 1) c + c = b + c \). XXX

Thus \( c = 1 \). From \( (\Delta) \) we see \( b = 2^{a+1} - 1 \) and

\( (\star \star) \) gives \( \sigma(b) = 2^{a+1} = b + 1 \Rightarrow b \) is prime

Thus \( N = 2^a \cdot b = 2^a \left( 2^{a+1} - 1 \right) \) where \( 2^{a+1} - 1 \) is a prime, as desired.
**Theorem:** Let $p$ be an odd prime.

Then any divisor of $M_p = 2^p - 1$ is of the form $2^{pk} + 1$.

**Proof:** 

Since the product of two numbers $q_1, q_2 \equiv 1 \pmod{2p}$ is also $q_1q_2 \equiv 1 \pmod{2p}$, it is enough to prove the theorem for the prime factors of $M_p$.

Let $q | M_p$ be a prime. By FLT, we have

\[ 2^{q-1} \equiv 1 \pmod{q} \iff q \mid 2^{q-1} - 1 \]

\[ \implies q \mid (2^p - 1, 2^{q-1} - 1) \overset{(*)}{=} 2^{p(q-1)} - 1 \neq 1 \]

Claim: $(*) \implies (N^{q-1}, N^{q-1} - 1) = N^{q-1} - 1$ (Lemma 4.3)

\[ \implies (p, q-1) \neq 1 \implies p \mid q-1 \text{ because } p \text{ is prime} \]

Thus $q-1 = pk'$ with $k' = 2 \cdot k$ because $q$ is odd.

Since $M_p$ is odd, thus $q = 1 + 2^{pk}$.

**Example:** Is $M_{23} = 2^{23} - 1 = 8388607$ a prime?

We only need to test divisibility by primes of the form $q = 46k + 1$.

The smallest is 47 and dividing $M_{23}$ by it shows $M_{23} = 47 \cdot 178481$. 
