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

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

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

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

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

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

If instead we look \( \pmod{2} \) we obtain

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

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

Thus the existence of solutions \( \pmod{17} \) 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 \( x \equiv 0, 1, 2, 3 \implies 2x \equiv 0, 2, 4, \not{3} \)

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.

\* \( 2x \equiv 3 \pmod{5} \)

\( x \equiv 0, 1, 2, 3, 4 \implies 2x \equiv 0, 2, 4, 1, \not{3} \)

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

Thus all integers in \([4]\) satisfy the equation.
$3x \equiv 9 \pmod 6$

$x \equiv 0, 1, 2, 3, 4, 5 \Rightarrow 3x \equiv 0 \pmod 6$

Thus there are three non-congruent solutions $x \equiv 1, 3, 5 \pmod 6$.

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

$x \equiv x_0 - \frac{M}{d}t$ where $0 \leq t \leq d - 1$

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

DEF: Any integer solution to $AX \equiv 1 \pmod{M}$ is called an inverse of $a$ modulo $M$.

Notation: Note that $AX \equiv 1 \pmod{M}$

$\Rightarrow [ax] = [1] \iff [a]^{-1} [x] = [1]$

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:

$M = 10$

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

$M = 5$

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

Corollary: Let $p$ be prime. Then all $a \neq 0 \pmod{p}$ has a unique inverse modulo $p$. 
**Lecture 10**

**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 mod $m$
which are given by

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

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 \( \alpha x - \beta y = b \) has solutions.

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

The general solution is given by

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

So the previous expression for \( x \) gives all the integers satisfying \( \alpha x \equiv b \pmod{\gamma} \).

To finish we want to count the different values of \( x \pmod{\gamma} \).

Suppose \( x_0 - \frac{\gamma}{d} t_1 \equiv x_0 - \frac{\gamma}{d} t_2 \pmod{\gamma} \)

\[\Leftrightarrow \quad \frac{\gamma}{d} (t_1 - t_2) \equiv 0 \equiv \frac{\gamma}{d} \cdot 0 \pmod{\gamma} \]

\[\Rightarrow \quad t_1 - t_2 \equiv 0 \pmod{\gamma} \]

Lemma

\[\Leftrightarrow \quad t_1 \equiv t_2 \pmod{d} \]

Because \( (\gamma, \frac{\gamma}{d}) = \frac{\gamma}{d} \) therefore taking \( t \in \{0, 1, \ldots, d-1\} \)

Gives the desired \( d \) non-congruent solutions \( \pmod{\gamma} \).\]
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

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

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

THEN \(17 \cdot 13 \equiv 1 \text{ (mod 55)}\)

THAT IS \(17 \cdot 13 \equiv 1 \text{ (mod 55)}\)

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

WE PLAYED THE SQUARING-OFF GAME!