MEM204-Number Theory

2nd virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 01/04/2020

University of Crete

Linear Congruences

Introduction

Let $a, b \in \mathbb{Z}$ and $n > 1$ be fixed numbers. A congruence of the form

$$ax \equiv b \pmod{n}, \tag{1}$$

where x varies, is called a *linear congruence*. Some x_0 that satisfies (1) is a *solution* of the congruence. Clearly, if x_0 is a solution of (1), so is every $x \in \bar{x_0}$.

In this lecture, our aim is to characterize whether (1) has a solution or not and, in the former case, how many of them are there (in $\mathbb{Z}_n$).

Some examples

Take the congruence

$$2x \equiv 3 \pmod 7.$$

We have that

- $2 \cdot 0 \equiv 0 \not\equiv 3 \pmod 7$,
- $2 \cdot 1 \equiv 2 \not\equiv 3 \pmod 7$,
- $2 \cdot 2 \equiv 4 \not\equiv 3 \pmod 7$,
- $2 \cdot 3 \equiv 6 \not\equiv 3 \pmod 7$,
- $2 \cdot 4 \equiv 1 \not\equiv 3 \pmod 7$,
- $2 \cdot 5 \equiv 3 \pmod 7$,
- $2 \cdot 6 \equiv 5 \not\equiv 3 \pmod 7$,

in other words $\bar{x} = \bar{5}$ is the only solution of the congruence.

Some examples

Take the congruence

$$2x \equiv 4 \pmod{6}.$$

We have that

- $2 \cdot 0 \equiv 0 \not\equiv 4 \pmod{6}$,
- $2 \cdot 1 \equiv 2 \not\equiv 4 \pmod{6}$,
- $2 \cdot 2 \equiv 4 \pmod{6}$,
- $2 \cdot 3 \equiv 0 \not\equiv 4 \pmod{6}$,
- $2 \cdot 4 \equiv 2 \not\equiv 4 \pmod{6}$,
- $2 \cdot 5 \equiv 4 \pmod{6}$,

in other words, here we have two solutions, $\bar{x} = \bar{2}$ and $\bar{x} = \bar{5}$.

Some examples

Take the congruence

$$2x \equiv 5 \pmod{6}.$$

We have that

- $2 \cdot 0 \equiv 0 \not\equiv 5 \pmod{6}$,
- $2 \cdot 1 \equiv 2 \not\equiv 5 \pmod{6}$,
- $2 \cdot 2 \equiv 4 \not\equiv 5 \pmod{6}$
- $2 \cdot 3 \equiv 0 \not\equiv 5 \pmod{6}$,
- $2 \cdot 4 \equiv 2 \not\equiv 5 \pmod{6}$,
- $2 \cdot 5 \equiv 4 \not\equiv 5 \pmod{6}$,

in other words, here we have no solutions at all!

One solution

From the above examples, we see that a linear congruence may have one, multiple or no solutions. The following proposition characterizes the first case.

Proposition

If $(a, n) = 1$, then the congruence $ax \equiv b \pmod{n}$ has exactly one solution.

Proof.

Since $(a, n) = 1$, we have that a is invertible modulo n. Let c be its inverse modulo n. We have that:

$$ax \equiv b \pmod{n} \Rightarrow x \equiv bc \pmod{n}.$$

□

A method

The proof of the above proposition, also suggests a method for solving these congruences, as we demonstrate below:

Example

We will solve

$$137x \equiv 4 \pmod{102}. \tag{2}$$

First, since $137 \equiv 35 \pmod{102}$, we can simplify (2) as

$$35x \equiv 4 \pmod{102}.$$

Then, with the help of the euclidean algorithm, we compute $\overline{35}^{-1} = \overline{35}$. We multiply both sides of the congruence by $\overline{35}$ and we get

$$x \equiv 4 \cdot 35 \equiv 140 \equiv 38 \pmod{102}.$$

A method

Remark

There are multiple ways for finding the inverse (in addition to the euclidean algorithm). For example, you may use

- *Euler's theorem ($\bar{a}^{-1} = \bar{a}^{\varphi(n)-1}$) or*
- *brute force.*

Example

Use Euler's theorem to solve

$$7x \equiv 8 \pmod{30}.$$

What about the case $(a, n) \neq 1$?

A complete characterization

Theorem

Let $d = (a, n)$. The congruence

$$ax \equiv b \pmod{n} \tag{3}$$

is solvable if and only if $d \mid b$. In this case, (3) has exactly d solutions and, if x_0 is one of them, then the solutions are

$$x \equiv x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d} \pmod{n}.$$

Proof

First, we focus on the existence statement.

($\Rightarrow$) Suppose that x satisfies (3). Then

$$n \mid ax - b \Rightarrow \exists\, c \ : \ ax - b = cn \overset{d|a,n}{\Longrightarrow} d \mid b.$$

($\Leftarrow$) Suppose that $d \mid b$. Then x satisfies (3) iff it satisfies

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}. \tag{4}$$

Now, since $\left(\frac{a}{d}, \frac{n}{d}\right) = 1$, from previous proposition, we get that (4) is solvable. We have now established the existence statement.

Proof

Next, we focus on the second statement. Assume that $d \mid b$, that is (3) is solvable. Then x_0 satisfies (3) iff it satisfies (4). However, (4) has a unique solution. This implies that all the solutions of (3) are of the form

$$x_0 + k\frac{n}{d},\ k \in \mathbb{Z}.$$

Further, notice that

$$\begin{aligned} x_0 + k_1\frac{n}{d} \equiv x_0 + k_2\frac{n}{d} \pmod{n} &\iff n \mid (k_1 - k_2)\frac{n}{d} \\ &\iff d \mid (k_1 - k_2) \iff k_1 \equiv k_2 \pmod{d}. \end{aligned}$$

The result follows.

An example

The congruence

$$24x \equiv 22 \pmod{33}$$

is not solvable, since $(24, 33) = 3 \nmid 22$.

Another example

We will find all the solutions of

$$2086x \equiv -1624 \pmod{1729}. \qquad (5)$$

First, note that, in $\mathbb{Z}_{1729}$, $\overline{2086} = \overline{357}$ and $\overline{-1624} = \overline{105}$, so (5) is equivalent to

$$357x \equiv 105 \pmod{1729}.$$

Next, we use the euclidean algorithm yields $(357, 1729) = 7$. However, $105 = 7 \cdot 15$. This implies that (5) has exactly 7 solutions. Our next step is to identify one solution and, based on this, find the other 6.

Another example (cont.)

Further, the euclidean algorithm yields

$$7 = 19 \cdot 1729 - 92 \cdot 357.$$

This implies

$$\begin{aligned} -92 \cdot 357 &\equiv 7 \pmod{1729} \\ \Rightarrow (-92 \cdot 15) \cdot 357 &\equiv 7 \cdot 15 \pmod{1729} \\ \Rightarrow 357 \cdot 349 &\equiv 105 \pmod{1729}. \end{aligned}$$

It follows that $\overline{349}$ is a solution of (5). If follows that all the solutions of (5) are

$$x \equiv 349, 596, 843, 1090, 1337, 1584, 102 \pmod{1729}.$$

Stay home, stay safe!