MEM204-Number Theory

3rd virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 03/04/2020

University of Crete

Systems of Linear Congruences

Introduction

Let $a_i, b_i \in \mathbb{Z}$ and $n_i > 1$ be fixed numbers for $i = 1, \ldots, k$. A set of congruences of the form

$$\begin{cases} a_1 x \equiv b_1 \pmod{n_1}, \\ \qquad \vdots \\ a_k x \equiv b_k \pmod{n_k}, \end{cases} \tag{1}$$

where x varies, is called a *system of linear congruences*. Some $x_0 \in \mathbb{Z}$ that satisfies all of the congruences of (1) is a *solution* of the system.

In this lecture, our aim is to characterize whether (1) is solvable or not and, in the former case, explicitly find its solutions.

Example

Take the system

$$\begin{cases} 3x \equiv -1 \pmod{10}, \\ 2x \equiv 1 \pmod{5}. \end{cases}$$

One easily checks that $x = 3$ is a solution of the system.

Some examples

Example

Take the system

$$\begin{cases} x \equiv 1 \pmod{6}, \\ x \equiv 2 \pmod{4}. \end{cases}$$

This system is impossible, since the first congruence's solutions are odd numbers and the second one's even.

Remark

Clearly a system can have a solution only if each one of its congruences is solvable. However, the inverse is not true, as the above example demonstrates.

Some definitions

Definition

We say that some $a \pmod{c}$ is a solution of a system of linear congruences, if all $x \in \bar{a}$ (where $\bar{a} \in \mathbb{Z}_c$) are solutions of that system.

Definition

Two systems of linear congruences are called equivalent (ισοδύναμα), if they both share the same set of solutions.

The main result of this lecture is the following theorem known as the *Chinese Remainder Theorem* (Κινέζικο Θεώρημα Υπολοίπων).

Theorem (Chinese Remainder Theorem)

Let $b_1, \ldots, b_k \in \mathbb{Z}$ *and* $n_1, \ldots, n_k > 1$ *be such that* $(n_i, n_j) = 1$ *for all* $i \neq j$*. Then the system*

$$\begin{cases} x \equiv b_1 \pmod{n_1}, \\ \qquad \vdots \\ x \equiv b_k \pmod{n_k}, \end{cases} \tag{2}$$

has a unique solution $\pmod{n_1 \cdots n_k}$.

Proof

The proof is comprised by 3 parts: (a) find a solution x_0, (b) show that every $x' \equiv x_0 \pmod{n_1 \cdots n_k}$ is also a solution and (c) show that every solution is also $\equiv x_0 \pmod{n_1 \cdots n_k}$.

Set $N_j := \frac{\prod_{i=1}^{k} n_i}{n_j}$. Since $n_1, \ldots, n_k$ are pairwise co-prime, we have that $(N_j, n_j) = 1$ for all j. It follows that, for every j, N_j is invertible $\pmod{n_j}$. Let $x_j \equiv N_j^{-1} \pmod{n_j}$. Now, set

$$x_0 = b_1 N_1 x_1 + \cdots + b_k N_k x_k.$$

Next, notice that, for every $i \neq j$, $n_i \mid N_j$, that is, $b_j N_j x_j \equiv 0 \pmod{n_i}$. It follows that for every i,

$$x_0 \equiv b_i N_i x_i \equiv b_i \pmod{n_i},$$

in other words x_0 is a solution of the System (2). This concludes Part (a).

Proof

Next, let $x' \equiv x_0 \pmod{n_1 \cdots n_k}$. Then, clearly, for every i, we have that $x' \equiv x_0 \equiv b_i \pmod{n_i}$. This concludes Part (b).

Finally, suppose that y is a solution of the system. Then, for every i, we have that

$$y \equiv b_i \equiv x_0 \pmod{n_i}.$$

It follows that, for every i, $n_i \mid y - x_0$. Since $n_1, \ldots, n_k$ are pairwise co-prime, this implies that $n_1 \cdots n_k \mid y - x_0$, that is, $y \equiv x_0 \pmod{n_1 \cdots n_k}$. The proof is now complete.

A method

A closer look at the proof of the Chinese Remainder Theorem reveals a method for solving this kind of systems.

For example, lets solve the system

$$\begin{cases} x \equiv 2 \pmod{5}, \\ x \equiv 3 \pmod{7}, \\ x \equiv 4 \pmod{11}. \end{cases}$$

Since $5, 7, 11$ are pairvise co-prime, the Chinese Remainder Theorem implies that the above system has a unique solution modulo $5 \cdot 7 \cdot 11 = 385$.

A method

Using the notation of the proof, we compute

$$N_1 = 7 \cdot 11 = 77,\ N_2 = 5 \cdot 11 = 55,\ N_3 = 5 \cdot 7 = 35.$$

Now, for $i = 1, 2, 3$, set $x_i \equiv N_i^{-1} \pmod{n_i}$. We compute

$$x_1 \equiv 3 \pmod{5},\ x_2 \equiv 6 \pmod{7},\ x_3 \equiv 6 \pmod{11}.$$

It follows that the solution of the system is

$$x \equiv 77 \cdot 3 \cdot 2 + 55 \cdot 6 \cdot 3 + 35 \cdot 6 \cdot 4 \equiv 2292 \equiv 367 \pmod{385}.$$

Generalizing the Chinese Remainder Theorem

The following theorem generalizes the Chinese Remainder Theorem.

Theorem

The system

$$\begin{cases} x \equiv b_1 \pmod{n_1}, \\ \vdots \\ x \equiv b_k \pmod{n_k}, \end{cases} \tag{3}$$

is solvable if and only if $(n_i, n_j) \mid b_i - b_j$*, for every* $i \neq j$*. In this case,* (3) *has a unique solution* $\pmod{[n_1, \ldots, n_k]}$.

Proof.

Omitted. $\square$

An example

Example

Solve the system

$$\begin{cases} x \equiv 1 \pmod{15}, \\ x \equiv 7 \pmod{18}. \end{cases}$$

An example

The last theorem implies that the system has a unique solution $\pmod{90}$. Let x_0 be a solution. The first congruence implies

$$x_0 = 1 + 15k,\ k \in \mathbb{Z}.$$

Now, the second congruence yields

$$\begin{aligned} & 1 + 15k \equiv 7 \pmod{18} \\ \iff & 15k \equiv 6 \pmod{18} \\ \iff & 5k \equiv 2 \pmod{6} \\ \iff & k \equiv 4 \pmod{6} \\ \iff & k = 4 + 6\ell,\ \ell \in \mathbb{Z}. \end{aligned}$$

It follows that $x_0 = 1 + 15k = 1 + 15(4 + 6\ell) = 61 + 90\ell$, $\ell \in \mathbb{Z}$. In other words $x_0 \equiv 61 \pmod{90}$.

Another example

Example

Solve the system

$$\begin{cases} 2x \equiv 4 \pmod{5}, \\ x \equiv -27 \pmod{22}, \\ 3x \equiv 30 \pmod{39}. \end{cases}$$

Another example

First, we will simplify the three congruences, in order to get an equivalent system in the form of the statement of the Chinese Remainder Theorem.

Towards this end, we solve the first congruence, using known methods, and we get

$$x \equiv 2 \pmod{5}. \tag{4}$$

The second one can be rewritten as

$$x \equiv 17 \pmod{22}. \tag{5}$$

The third one does not have a unique solution modulo 39 (in fact it has three of them). Nonetheless, it is equivalent to the congruence

$$x \equiv 10 \pmod{13}. \tag{6}$$

Another example

Now the Chinese Remainder Theorem implies that the system has a unique solution $\pmod{1430}$. Let x be a solution. Congruence (4) implies

$$x = 2 + 5a, a \in \mathbb{Z}.$$

We replace this in (5) and get

$$2 + 5a \equiv 17 \pmod{22} \iff a \equiv 3 \pmod{22}.$$

It follows that $a = 3 + 22b$, that is,

$$x = 2 + 5(3 + 22b) = 17 + 110b,\ b \in \mathbb{Z}.$$

Another example

Finally, we replace the latter in (6) and get

$$17 + 110b \equiv 10 \pmod{13} \iff b \equiv 1 \pmod{13}.$$

It follows that $b = 1 + 13c$, that is,

$$x = 17 + 110(1 + 13c) = 127 + 1430c, \; c \in \mathbb{Z}.$$

In other words, we have shown that

$$x \equiv 127 \pmod{1430}$$

is the solution of the system.

Stay home, stay safe!