MEM204-Number Theory

5th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 10/04/2020

University of Crete

Polynomial congruences - Introduction

Glossary

Let

$$f(x) = \sum_{i=0}^{n} f_i x^i \in \mathbb{Z}[x]$$

be a polynomial over $\mathbb{Z}$. A congruence of the form

$$f(x) \equiv 0 \pmod{n},$$

where x varies, is called a polynomial congruence (πολυωνυμική ισοτιμία). The largest i, such that $f_i \not\equiv 0 \pmod{n}$ is the degree (βαθμός) of the congruence. Some $x_0 \in \mathbb{Z}_n$, satisfying $f(x_0) \equiv 0 \pmod{n}$ is a solution (λύση) of the congruence.

A few remarks

- The degree of a polynomial congruence may be smaller than the degree of the corresponding polynomial. For example, if $f(x) = 5x^2 + 2x + 1 \in \mathbb{Z}[x]$, then the degree of

$$f(x) \equiv 0 \pmod{5}$$

  is 1, while, clearly $\deg(f) = 2$.
- In the same sense, the polynomials $f = \sum_{i=0}^{n} f_i x^i \in \mathbb{Z}[x]$ and $g = \sum_{i=0}^{n} g_i x^i \in \mathbb{Z}[x]$, give rise to the same polynomial congruence $\pmod{n}$ iff $f_i \equiv g_i \pmod{n}$ for every i. For example, the polynomials $5x^2 + 2x + 1$ and $2x + 6$ define the same polynomial congruence modulo 5.

Equivalent polynomial congruences

Definition

Two polynomial congruences are equivalent (ισοδύναμες) if they have the same solutions.

Example

The congruences

$$x^2 + x \equiv 0 \pmod{7} \text{ and } x^6 + x \equiv 0 \pmod{7}$$

are equivalent, since they share $\{\bar{0}, \bar{6}\} \subseteq \mathbb{Z}_7$ as their set of solutions.

Remark

The above example demonstrates that equivalent congruences can be different.

An example

Suppose that we are looking for the solutions of

$$121x^5 + x^2 - 24x + 143 \equiv 0 \pmod{11}.$$

First, where applicable, we replace the coefficients, in order to get a simpler expression of the same congruence as follows:

$$x^2 - 2x \equiv 0 \pmod{11}.$$

Then, we check the validity of the above for all the elements of $\mathbb{Z}_{11}$ (here, it is more convenient to take $\mathbb{Z}_{11} = \{\bar{0}, \pm\bar{1}, \pm\bar{2}, \pm\bar{3}, \pm\bar{5}\}$) and easily see that the solutions are $\bar{0}$ and $\bar{2}$.

An example

Remark

The method described above is, of course, valid, universal and correct. However, if the numbers (and in particular the modulus or the powers) are large, it is problematic.

In certain cases, it is possible to split the problem into smaller, more manageable ones.

Polynomial congruences modulo a prime

An important reduction

Proposition

Let p be a prime. The polynomial congruence

$$f(x) \equiv 0 \pmod{p},$$

where

$$f(x) = \sum_{i=0}^{n} f_i x^i,$$

is equivalent to some polynomial congruence of degree $< p$.

Proof

Fermat's theorem implies that for every $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$. It follows that for very j, there exists some $0 \le \sigma(j) < p$, such that $a^j \equiv a^{\sigma(j)} \pmod{p}$, for all $a \in \mathbb{Z}$.

It follows that for every $a \in \mathbb{Z}$, we have that $f(a) \equiv g(a) \pmod{p}$, where

$$g(x) = \sum_{i=0}^{p-1} g_i x^i,$$

where, for $0 \le i \le p-1$,

$$g_i = \sum_{\substack{0 \le j \le n \\ \sigma(j) = i}} f_j.$$

The result follows.

Number of solutions of polynomial congruences modulo p

Theorem

Suppose that p is a prime and that the polynomial congruence

$$f(x) = \sum_{i=0}^{n} f_i x^i \equiv 0 \pmod{p}$$

has degree n, then is has at most n solutions modulo p.

Proof (Sketch)

We will use induction on n. The result is clear for $n = 0$. Suppose that it holds for $n = k - 1$.

Finally, let $n = k$. If the congruence has no solutions, then the result holds. Let ξ be a solution, in the case where it has one. Then, for every x,

$$\begin{aligned} f(x) &\equiv f(x) - f(\xi) \equiv \sum_{i=0}^{k} f_i x^i - \sum_{i=0}^{k} f_i \xi^i \\ &\equiv \sum_{i=1}^{k} f_i (x^i - \xi^i) \equiv (x - \xi) \sum_{i=1}^{k} f_i q_i(x) \pmod{p}, \end{aligned}$$

where $q_i(x) = \frac{x^i - \xi^i}{x - \xi}$, is a polynomial of degree $i - 1$. Now, let $g(x) = \sum_{i=1}^{k} f_i q_i(x)$. The result follows from the induction hypothesis and the fact that $\deg g = k - 1$.

An example

Take the polynomial congruence

$$f(x) = 3x^7 + 2x^6 + x^5 + 2x^3 + 6 \equiv 0 \pmod{5}.$$

Fermat's theorem states that for every $a \in \mathbb{Z}$, we have that $a^5 \equiv a \pmod{5}$. Hence

$$\begin{aligned} a^7 &\equiv a^5 a^2 \equiv a \cdot a^2 \equiv a^3 \pmod{5}, \\ a^6 &\equiv a^5 a \equiv aa \equiv a^2 \pmod{5}, \\ a^5 &\equiv a \pmod{5}. \end{aligned}$$

So, an equivalent congruence would be

$$3x^3+2x^2+x+2x^3+6 \equiv 5x^3+2x^2+x+6 \equiv 2x^2+x+1 \pmod{5}.$$

We easily check that the latter is not satisfied for $x = 0, \pm 1, \pm 2$, so we conclude that it has no solutions.

Polynomial congruences modulo a composite

A reduction technique

Proposition

If, for some $n \in \mathbb{Z}_{>0}$, $n = p_1^{n_1} \cdots p_k^{n_k}$ is its prime factorization, then the polynomial congruence

$$f(x) \equiv 0 \pmod{n},$$

where $f(x) \in \mathbb{Z}[x]$, is solvable iff, for every $1 \leq i \leq k$, the polynomial congruence

$$f(x) \equiv 0 \pmod{p_i^{n_i}}$$

is solvable. Moreover, if each of the above congruences has $L(i)$ solutions, then the original one has $L = L(1) \cdots L(k)$ solutions.

Proof - Existence

($\Rightarrow$) If, for some a, $f(a) \equiv 0 \pmod{n}$, then (given that $p_i^{n_i} \mid n$), it is immediate that $f(a) \equiv 0 \pmod{p_i^{n_i}}$, $\forall i$.

($\Leftarrow$) Suppose that, for every i, there exists some a_i, such that

$$f(a_i) \equiv 0 \pmod{p_i^{n_i}}.$$

Since $p_1^{n_1}, \ldots, p_k^{n_k}$ are pairwise co-prime, the Chinese Remainder Theorem, ensures the existence of some a, such that $a \equiv a_i \pmod{p_i^{n_i}}$, for every i. It follows that, for every i,

$$f(a) \equiv f(a_i) \equiv 0 \pmod{p_i^{n_i}},$$

which, since $p_1^{n_1}, \ldots, p_k^{n_k}$ are pairwise co-prime and $n = p_1^{n_1} \cdots p_k^{n_k}$, implies that

$$f(a) \equiv 0 \pmod{n}.$$

This completes the existence part of the statement.

Proof - Cardinality

The part of the statement regarding the cardinality of the solutions, follows from the existence one. Namely, the proof of the previous part implies that every collection of solutions $\bar{a}_1 \in \mathbb{Z}_{p_1^{n_1}}, \ldots, \bar{a}_k \in \mathbb{Z}_{p_k^{n_k}}$ corresponds to exactly one solution $\bar{a} \in \mathbb{Z}_n$. The desired result follows.

An example

We are interested in finding the solutions of

$$f(x) = 7x^7 + 16x^2 + 10 \equiv 0 \pmod{21}.$$

Since $21 = 3 \cdot 7$, we can instead study the congruences

$$f(x) \equiv 0 \pmod{3} \text{ and } f(x) \equiv 0 \pmod{7}.$$

Lets begin with the first one. After employing Fermat's theorem, it is easy to check that $f(x) \equiv 0 \pmod{3}$ is equivalent to $x^2 + x + 1 \equiv 0 \pmod{3}$. We explicitly check $x \equiv 0, \pm 1 \pmod{3}$ and we verify that $x \equiv 1 \pmod{3}$ is the unique solution.

An example

Now, we turn our attention to the second one. It is easy to check that $f(x) \equiv 0 \pmod 7$ is equal to $2x^2 + 3 \equiv 0 \pmod 7$. We explicitly check $x \equiv 0, \pm 1, \pm 2, \pm 3 \pmod 7$ and we verify that we have the solutions $x \equiv \pm 3 \pmod 7$.

It follows that the solutions of the original congruence are exactly the solutions of the following systems

$$\begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 3 \pmod 7, \end{cases} \quad \text{and} \quad \begin{cases} x \equiv 1 \pmod 3, \\ x \equiv 4 \pmod 7. \end{cases}$$

An example

Notice that the Chinese Remainder Theorem ensures that both systems have a unique solution modulo 21. We explicitly solve both of them (using any method) and attain the solutions

$$x \equiv 10 \pmod{21} \text{ and } x \equiv 4 \pmod{21}.$$

Stay home, stay safe!