MEM204-Number Theory

6th virtual lecture

Giorgos Kapetanakis

Spring semester 2019-20 - 23/04/2020

University of Crete

Polynomial congruences modulo a prime power

The derivative

Definition

Let

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

be a polynomial. The polynomial

$$f'(x) = \sum_{i=1}^{n} i f_i x^{i-1}$$

is the (formal) derivative of f.

Example

The derivative of $f(x) = 4x^3 + 3x^2 + x + 1$ is
$f'(x) = 12x^2 + 6x + 1$.

A recursive result

Theorem

Let p be a prime, $r \geq 2$ *and* $f(x) = \sum_{i=0}^{n} f_i x^i \in \mathbb{Z}[x]$*. Moreover, assume that*

$$f(x) \equiv 0 \pmod{p^{r-1}}$$

is satisfied for some $b \in \mathbb{Z}_{p^{r-1}}$*. Then We have the following cases regarding*

$$f(x) \equiv 0 \pmod{p^r}. \tag{1}$$

A recursive result

Theorem (cont.)

- *If* $f'(b) \not\equiv 0 \pmod{p}$*, then there exists a unique solution of* (1) *corresponding to* $b \pmod{p^{r-1}}$*. This solution is* $a \equiv tp^{r-1} + b \pmod{p^r}$*, where* t *satisfies*

$$f'(b)t \equiv \left(\frac{-f(b)}{p^{r-1}}\right) \pmod{p}.$$

- *If* $f'(b) \equiv 0 \pmod{p}$*, then, we have two subcases:*
    - *If* $f(b) \equiv 0 \pmod{p^r}$*, then there are* p *solutions of* (1) *corresponding to* $b \pmod{p^{r-1}}$*, namely* $a_t \equiv tp^{r-1} + b \pmod{p^r}$*, for* $t = 0, 1, \ldots, p-1$*.*
    - *If* $f(b) \not\equiv 0 \pmod{p^r}$*, then there are no solutions of* (1) *corresponding to* $b \pmod{p^{r-1}}$*.*

Proof

Let a be a solution of (1), corresponding to $b \pmod{p^{r-1}}$, i.e., $a \equiv b \pmod{p^{r-1}}$, hence, $a = b + tp^{r-1}$ for some t. Then

$$f(a) = f(b + tp^{r-1}) = \sum_{i=0}^{n} f_i \left(\sum_{k=0}^{i} \binom{i}{k} b^k (tp^{r-1})^{i-k} \right),$$

which implies

$$f(a) = f(b) + f'(b)tp^{r-1} + Mp^{2r-2},$$

where $M \in \mathbb{Z}$. Given that $f(b) \equiv 0 \pmod{p^{r-1}}$, we have that $f(b) = sp^{r-1}$, for some s, while clearly $2r - 2 \geq r$. Hence,

$$f(a) \equiv 0 \pmod{p^r} \iff s + tf'(b) \equiv 0 \pmod{p}.$$

Proof

First, we take the case $f'(b) \not\equiv 0 \pmod p$. Then there exists $\bar{t} \in \mathbb{Z}_p$, such that $tf'(b) \equiv -s \pmod p$. It follows that $a = tp^{r-1} + b$ satisfies (1), while it is not hard to check that this number is unique $\pmod p$.

Then we focus on the case $f'(b) \equiv 0 \pmod p$. Then, if $s \not\equiv 0 \pmod p$, then $s + tf'(b) \equiv 0 \pmod p$ is impossible. On the other hand, if $s \equiv 0 \pmod p$, then it is true for every t. The proof is complete, after we observe that the numbers $a_t = tp^{r-1} + s$, $(t = 0, 1, \ldots, p-1)$ are not equivalent modulo p^r.

Consequences

- The latter provides a recursive method for solving polynomial congruences of the form

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

  as follows: (1) Solve $f(x) \equiv 0 \pmod{p}$. (2) Given the solutions of $f(x) \equiv 0 \pmod{p}$, find the solutions of $f(x) \equiv 0 \pmod{p^2}$. $\cdots$ (r) Given the solutions of $f(x) \equiv 0 \pmod{p^{r-1}}$, find the solutions of $f(x) \equiv 0 \pmod{p^r}$.
- A combination of this with previous results suggests a complete method for solving polynomial congruences over any modulus.

An elaborate example

An example

Lets solve the congruence

$$4x^4 + 4x^3 + 6x^2 + 21x + 7 \equiv 0 \pmod{252}. \tag{2}$$

Our first step is to factor the modulus into primes and split the problem into smaller ones. Here, we have that

$$252 = 2^2 3^2 7,$$

hence, if $f(x) = 4x^4 + 4x^3 + 6x^2 + 21x + 7$, it suffices to solve

$$f(x) \equiv 0 \pmod{2^2}, \tag{3}$$

$$f(x) \equiv 0 \pmod{3^2} \tag{4}$$

and

$$f(x) \equiv 0 \pmod{7}. \tag{5}$$

An example

First, we focus on (3). First we solve

$$f(x) \equiv 0 \pmod{2},$$

which is trivial to see that, 1 is its only solution $\pmod{2}$. Then, we compute

$$f'(x) = 16x^3 + 12x^2 + 12x + 21,$$

that is $f'(1) \not\equiv 0 \pmod{2}$. So, we conclude that there is a unique solution of (3), namely $x \equiv 3 \pmod{4}$.

Remark

In this case, we could also check all the elements of $\mathbb{Z}_4$ in (3) directly, since 4 is a small, manageable number.

An example

Then, we focus on (4). First, we consider $f(x) \equiv 0 \pmod{3}$. We easily check that this is equivalent to $x^2 + x + 1 \equiv 0 \pmod{3}$, that has the unique solution $1 \pmod{3}$. Again, we confirm that $f'(1) \not\equiv 0 \pmod{3}$, hence we have a unique solution for (4).

In order to find it, we compute $-f(1)/p^{2-1} = -42/3 = -14$ and $f'(1) = 61$, that is, we need to solve

$$61t \equiv -14 \pmod{3}.$$

The above is equivalent to $t \equiv 1 \pmod{3}$, so our (unique) solution is $x \equiv tp^{r-1} + b \equiv 4 \pmod{9}$.

An example

Finally, we focus on (5). One can easily see that this is equivalent to

$$2x^2(2x^2 + 2x + 3) \equiv 0 \pmod 7.$$

Since 7 is a prime, the latter yields that either $x \equiv 0 \pmod 7$, or $2x^2 + 2x + 3 \equiv 0 \pmod 7$. We explicitly check all values of $\mathbb{Z}_7$, and conclude that the second's congruence solutions are 1 and $5 \pmod 7$.

In total, we have three solutions $x \equiv 0 \pmod 7$, $x \equiv 1 \pmod 7$ and $x \equiv 5 \pmod 7$.

An example

To sum up, the solutions of the original congruence, are the solutions of the systems

$$\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{9}, \\ x \equiv 0 \pmod{7}, \end{cases} \quad \begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{9}, \\ x \equiv 1 \pmod{7}, \end{cases} \quad \text{and} \begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{9}, \\ x \equiv 5 \pmod{7}. \end{cases}$$

The solutions of the above systems are

$$x \equiv 175,\ 211 \text{ and } 103 \pmod{252}$$

respectively.

Quadratic residues (Τετραγωνικα υπολοιπα)

Introduction

A famous question in Number Theory is whether the congruence

$$x^2 \equiv a \pmod{n},$$

where $(a, n) = 1$, is solvable or not. If it is solvable (in other words if $\bar{a} \in \mathbb{Z}_n$ is a square) we call a a quadratic residue modulo n (τετραγωνικό υπόλοιπο modulo n). Otherwise, it is called a quadratic non-residue modulo n (μη-τετραγωνικό υπόλοιπο modulo n).

Unsurprisingly, as we will see in upcoming exercises in detail, this can be reduced to the same question, when n is a prime. This is why we first focus on that case.

The Legendre symbol

Definition

Let $a \in \mathbb{Z}$ and p some prime such that $p \nmid a$. The Legendre symbol (σύμβολο Legendre) of $a \pmod{p}$ is

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is quadratic residue modulo } p, \\ -1, & \text{if } a \text{ is non-quadratic residue modulo } p. \end{cases}$$

Our next aim is to describe the computation of the Legendre symbol for any a and p.

The Legendre symbol - Basic properties

From the definition of the Legendre symbol, one immediately gets the following.

- If $0 \not\equiv a \equiv b \pmod{p}$, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

- If $p \nmid a$, then

$$\left(\frac{a^2}{p}\right) = 1.$$

- For every prime p,

$$\left(\frac{1}{p}\right) = 1.$$

Stay home, stay safe!