Polynomial Congruences

Debdeep Mukhopadhyay

Associate Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Hensel's Lifting**

Linear Congruences

Let, $d = \gcd(a, m)$. The congruence $ax \equiv b (\bmod m)$ is solvable for x iff $d \mid b$. If $d \mid b$, then all solutions are congruent to each other modulo m/d, *ie.* there is a unique solution modulo m/d.
In particular, if $\gcd(a, m) = 1$, then the congruence has a unique solution modulo m.

IIT Kharagpur

Polynomial Congruences

- **Locate all roots of a polynomial f(x) with integer coefficients modulo a m∈N.**

$$f(x) \equiv 0 (\bmod m)$$

- **Naïve method: Substitute all values of x∈**Z_m, and find which values will satisfy.
- Not good when m is large.

IIT Kharagpur

Hensel's lifting

- **When complete factors of m is available, we have an efficient method.**

Let, $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, with distinct primes $p_1, p_2, \dots, p_r$, $e_i \in N$.

If we know the roots of $f(x)$ modulo each $p_i^{e_i}$, we can combine these by CRT to obtain all the roots of $f(x)$ modulo m.

So, it is sufficient to solve:

$$f(x) \equiv 0 (\text{mod } p^e)$$

What is lifting?

- **Hensel's lifting is used to obtain all the solutions of $f(x) \equiv 0(\text{mod } p^{\epsilon+1})$ from the solutions of $f(x) \equiv 0(\text{mod } p^{\epsilon})$**
- **This ability helps us to first derive the roots modulo p, then lift it to p^2, then lift it to p^3, and so on.**

IIT Kharagpur

Lifting from p^ϵ to $p^{\epsilon+1}$

Let, w be a solution of $f(x) \equiv 0(\text{mod } p^\varepsilon)$. All integers that satisfy this equation modulo p^ε are $w + kp^\varepsilon, k \in Z$.

How many of them continue to satisfy $f(x) \equiv 0(\text{mod } p^{\varepsilon+1})$?

IIT Kharagpur

Lifting from p^ϵ to $p^{\epsilon+1}$

Let, $f(x) = a_d x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0$

Substituting, $x = w + kp^\varepsilon$,

$$f(c) =$$
$$a_d(w+kp^\varepsilon)^d + a_{d-1}(w+kp^\varepsilon)^{d-1} + \ldots + a_1(w+kp^\varepsilon) + a_0$$
$$= (a_d w^d + a_{d-1}w^{d-1} + \ldots + a_0) +$$
$$kp^\varepsilon(da_d w^{d-1} + (d-1)a_{d-1}w^{d-2} + \ldots + a_1) + p^{2\varepsilon}\alpha$$

[α is some polynomial expression in w]

$$= f(w) + kp^\varepsilon f'(w) + p^{2\varepsilon}\alpha.$$

IIT Kharagpur

Lifting from p^{ϵ} to $p^{\epsilon+1}$

Since, $\varepsilon \geq 1, 2\varepsilon \geq \varepsilon + 1$,

$[f(w) + kp^{\varepsilon} f'(w) + p^{2\varepsilon}\alpha](\text{mod } p^{\varepsilon+1})$

$= [f(w) + kp^{\varepsilon} f'(w)](\text{mod } p^{\varepsilon+1})$

We need to identify all the values of k for which

$[f(w) + kp^{\varepsilon} f'(w)](\text{mod } p^{\varepsilon+1}) = 0.$

Thus, $kp^{\varepsilon} f'(w) = -f(w)(\text{mod } p^{\varepsilon+1}).$

Clearly, $p^{\varepsilon} \mid f(w) \Rightarrow f'(w)k \equiv -\dfrac{f(w)}{p^{\varepsilon}}(\text{mod } p)$

Note this is a linear congruence with 0, 1, or p solutions.

IIT Kharagpur

Example

- **Find out all solutions for $2x^3 - 7x^2 + 189 \equiv 0(mod\ 675)$**

IIT Kharagpur

Practice Problem

Let C be a solution of:

$$f(x) \equiv 0(\mathrm{mod}\ p^{a}),$$

$$\text{and let } f'(c) \equiv 0(\mathrm{mod}\ p).$$

$$\text{Prove, } f(x) \equiv 0(\mathrm{mod}\ p^{a+t})$$

has exactly one solution correspond-ing to the solution $x = C$ *of* $(1), \forall t > 0.$

IIT Kharagpur