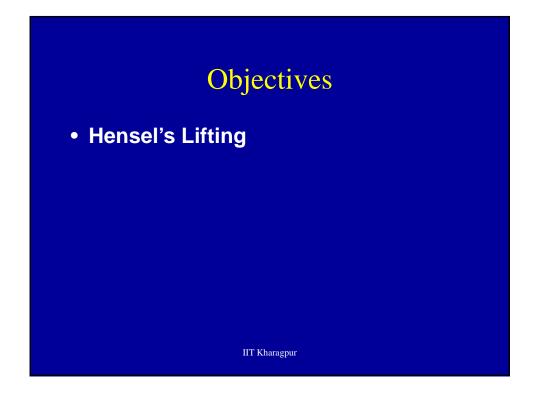
### **Polynomial Congruences**

Debdeep Mukhopadhyay

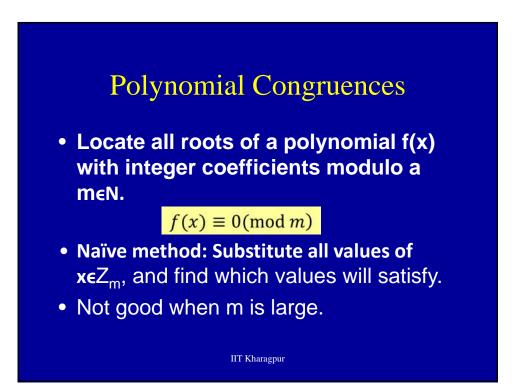
Associate Professor Department of Computer Science and Engineering Indian Institute of Technology Kharagpur INDIA -721302



## Linear Congruences

Let, d = gcd(a, m). The congruence  $ax \equiv b \pmod{m}$  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



## Hensel's lifting

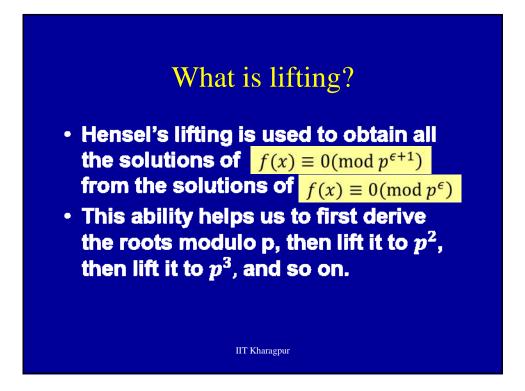
• When complete factors of m is available, we have an efficient method.

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:

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



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

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

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

#### IIT Kharagpur

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

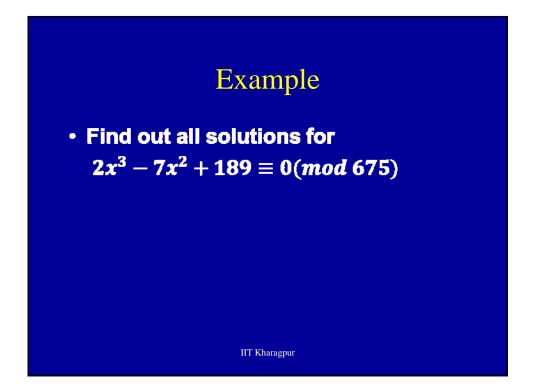
Let, 
$$f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$$
  
Substituting,  $x = w + kp^{\varepsilon}$ ,  
 $f(c) =$   
 $a_d (w + kp^{\varepsilon})^d + a_{d-1} (w + kp^{\varepsilon})^{d-1} + \dots + a_1 (w + kp^{\varepsilon}) + a_0$   
 $= (a_d w^d + a_{d-1} w^{d-1} + \dots + a_0) +$   
 $kp^{\varepsilon} (da_d w^{d-1} + (d-1)a_{d-1} w^{d-2} + \dots + a_1) + p^{2\varepsilon} \alpha$   
[ $\alpha$  is some polynomial expression in w]  
 $= f(w) + kp^{\varepsilon} f'(w) + p^{2\varepsilon} \alpha$ .

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

Since,  $\varepsilon \ge 1, 2\varepsilon \ge \varepsilon + 1$ ,  $[f(w) + kp^{\varepsilon}f'(w) + p^{2\varepsilon}\alpha] \pmod{p^{\varepsilon+1}}$   $= [f(w) + kp^{\varepsilon}f'(w)] \pmod{p^{\varepsilon+1}}$ We need to identify all the values of k for which  $[f(w) + kp^{\varepsilon}f'(w)] \pmod{p^{\varepsilon+1}} = 0.$ Thus,  $kp^{\varepsilon}f'(w) = -f(w) \pmod{p^{\varepsilon+1}}.$ 

Clearly, 
$$p^{\varepsilon} | f(w) \Rightarrow f'(w)k \equiv -\frac{f(w)}{p^{\varepsilon}} \pmod{p}$$

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



### **Practice Problem**

Let C be a solution of:  $f(x) \equiv 0 \pmod{p^a},$ and let  $f'(c) \equiv 0 \pmod{p}.$ Prove,  $f(x) \equiv 0 \pmod{p^{a+t}}$ 

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

IIT Kharagpur