POLYNOMIAL CONGRUENCES

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

Solve for x

$m \in \mathbb{N}$

f : polynomial with integer coefficients

Brute-force : substitute x with elements of $\mathbb{Z}_m$ one by one.

practical only when m is small

For large m, we can solve the congruence efficiently if the prime factorisation of m is known.

$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$

1. Compute roots of $f(x)$ modulo each $p_i^{e_i}$
2. Combine using CRT to find solutions modulo m.

Use Hensel Lifting

Hensel lifting : obtain solutions of $f(x) \equiv 0 \pmod{p^{u+1}}$ given solutions of $f(x) \equiv 0 \pmod{p^u}$ $(p \in \mathbb{P},\ u \in \mathbb{N})$

Computing roots of $f(x) \bmod p^e$

- Compute roots of $f(x) \bmod p$ $\rightarrow$ to be discussed later on
- Use Hensel lifting to obtain roots of $f(x) \bmod p^2$, $\bmod p^3, \ldots,$ $\bmod p^u$.

HENSEL LIFTING

Task: find roots of $f(x) \bmod p^{u+1}$; Known: roots of $f(x) \bmod p^{u}$.

z : root of $f(x) \bmod p^u$ i.e., $f(z) \equiv 0 \pmod{p^u}$

Solutions to $f(x) \equiv 0 \pmod{p^u}$: $\{z + kp^u : k \in \mathbb{Z}\}$

some of these elements continue to be roots mod p^{u+1}
which ones?

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

$$f(z+kp^u) = a_d(z+kp^u)^d + a_{d-1}(z+kp^u)^{d-1} + \dots + a_1 x + a_0$$

$$= \underline{a_d z^d + a_{d-1} z^{d-1} + \dots + a_1 z + a_0}$$

$$+ \left(a_d d z^{d-1} + a_{d-1}(d-1) z^{d-2} + \dots + a_1\right) kp^u$$

$$+ (kp^u)^2 \cdot \alpha$$

$$(z+kp^u)^i = z^i + \binom{i}{1} kp^u \cdot z^{i-1} + (kp^u)^2 \cdot \beta$$

$$= f(z) + kp^u \cdot f'(z) + \underbrace{k^2 p^{2u} \cdot \alpha}_{\text{divisible by } p^{u+1}}$$

$$\equiv f(z) + kp^u f'(z) \pmod{p^{u+1}}$$

$$f(z+kp^u) \equiv 0 \pmod{p^{u+1}}$$ solve for k.

$$f(z) + kp^u f'(z) \equiv 0 \pmod{p^{u+1}}$$

$$p^u k f'(z) / p^u \equiv -f(z) / p^u \pmod{p^{u+1} / p^u}$$

$$k f'(z) \equiv -\frac{f(z)}{p^u} \pmod{p} \quad \dots (1)$$

$f(z) \equiv 0 \pmod{p^u}$

$p^u \mid f(z)$

① will have 0, 1 or p solutions

these determine the integers that continue to be roots modulo p^{u+1}

Example

$$f(x) = 7x^3 - 26x^2 + 18 \qquad f'(x) = 21x^2 - 52x$$

$$f(x) \equiv 0 \pmod{27}$$

Solutions modulo 3 : $\boxed{0, 2}$

$$f(0) = 18 \equiv 0 \pmod 3$$

$$f(1) = -1 \equiv 2 \pmod 3$$

$$f(2) = -30 \equiv 0 \pmod 3$$

Solutions modulo 3^2 : $\boxed{0, 3, 6, 5}$

Lift 0 : $k \cdot f'(0) \equiv -\frac{f(0)}{3} \pmod 3$

$f'(0) = 0$ $\quad \frac{f(0)}{3} = \frac{18}{3} = 6$

$k \cdot 0 \equiv -6 \pmod 3$

$\equiv 0 \pmod 3$

$k = 0, 1, 2$

Roots of $f(x) \bmod 3^2$: $0, 3, 6$

$(0 + k \cdot 3)$

Lift 2 : $f(2)/3 = -\frac{30}{3} = -10$

$f'(2) = -20$

$k(-20) \equiv 10 \pmod 3$

$k \equiv 1 \pmod 3$

soln : $2 + k\,3 = 5$

Solutions modulo 3^3: $3, 5, 6, 12, 15, 21, 24$

Lift 0 : $\frac{f(0)}{3^2} = 18/9 = 2$ $\quad f'(0) = 0$

$k \cdot 0 \equiv -2 \pmod 3$ no soln.

Lift 1 : $\frac{f(3)}{3^2} = -27/9 = -3$ $\quad f'(3) = 33$

$k \cdot 33 \equiv -(-3) \pmod 3$ $\quad k = 0, 1, 2$

solns : $3, 12, 21$

Lift 6 : $\frac{f(6)}{3^2} = \frac{594}{9} = 66$ $\quad f'(6) = 444$

$k \cdot 44 \equiv -66 \pmod 3$ $\quad k = 0, 1, 2$

solns: $6, 15, 24$

Lift 5 : $f(5)/3^2 = 243/9 = 27$ $\quad f'(5) = 265$

$k \cdot 265 \equiv -27 \pmod 3$

$k \equiv 0 \pmod 3$ $\quad$ soln: 5