- linear congruences.

$$ax \equiv b \pmod m$$

Theorem 6.3

$$d = \gcd(a, m)$$

sols exist iff $d \mid b$

if so they're given by

$$x \equiv t + i\frac{m}{d}, \quad i = 0, \dots, d-1$$

where t is the unique solution to reduced congruence

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\mod \frac{m}{d}\right)$$

- Chinese Remainder Theorem.

  ↳ allow us to solve $f(x) \equiv 0 \pmod m$ by solving the sub-congruences.

$$f(x) \equiv 0 \pmod{p_i^{a_i}} \quad i = 1, \dots, r$$

where $m = \prod_{i=1}^{r} p_i^{a_i}$

So we need more understanding of solutions of $f(x) \equiv 0 \pmod{p^a}$

First, case when $a = 1$.

Theorem (Lagrange)

For a poly. congruence, p prime

$$f(x) \equiv 0 \pmod p \quad (*)$$

$(n \geq 1)$

if it has degree n, ie.

$$f = \sum_{i=0}^{n} a_i x^i \quad , \text{ where } a_n \not\equiv 0 \pmod p$$

ie. $p \nmid a_n$.

then $(*)$ has at most n solutions.

Proof: (nice substantial argument, using induction and proof by contradiction)

We perform induction on the degree of the polynomial

Base case $n=1$ ie. linear polynomials

$$a_1 x + a_0 \equiv 0 \pmod p$$

Well we understand these from yesterday

we're assuming $p \nmid a_1$, so $\gcd(a_1, p) = 1$

ie. there is a single unique solution to this $x \equiv -a_1^{-1} a_0 \pmod p$.

So 1 sol for a degree 1 poly. So the theorem is true when $n=1$

So now we assume theorem is true for all polynomials of degree $n = k$, for some

$k \geq 1$. Now we will deduce the theorem for $n = k+1$.

To do this we'll use proof by contradiction. So we assume the theorem is false for $n = k+1$, ie. there exists at least one "bad" polynomial.

say $g(x) = \sum_{i=0}^{k+1} a_i x^i \equiv 0 \pmod{p}$

where $p \nmid a_{k+1}$, with at least $\underline{k+2}$ solutions. which are

$x \equiv x_0, x_1, \ldots, x_{k+1} \pmod{p}$

We will obtain from g, a poly h that violates our assumption that theorem is true for polys of degree k.

Construct another poly G.

$$\boxed{G(x) := g(x) - g(x_0)}$$

$$= \sum_{i=0}^{k+1} a_i x^i - \sum_{i=0}^{k+1} a_i x_0^i$$

$$= \sum_{i=0}^{k+1} a_i (x^i - x_0^i)$$

$$\left(\begin{array}{l} \text{Remember } c^i - d^i \text{ always factorises as} \\ c^i - d^i = (c-d)\left(c^{i-1} + c^{i-2}d + c^{i-3}d^2 + \dots + cd^{i-2} + d^{i-1}\right) \end{array} \right)$$

So $\boxed{G(x) = (x - x_0)\,h(x)}$

where h is a poly. with integer coefficients.

with degree k, and leading coefficient.

a_{k+1}, and remember $p \nmid a_{k+1}$

Consider the other solutions

$x_1, \dots, x_{k+1} \pmod p$ of g.

$$G(x_j) = g(x_j) - g(x_0) \equiv 0 \pmod p$$

$$= (x_j - x_0)\,h(x_j)$$

i.e. $p \mid (x_j - x_0)\,h(x_j)$

But x_0, x_j are <u>distinct</u> modulo p

i.e. $p \nmid x_j - x_0$

$\implies p \mid h(x_j)$, from Euclid's lemma on primes.

i.e. $h(x_j) \equiv 0 \pmod{p}$

$p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

So summarizing we've constructed h, a poly. of degree k, with too many sols, $x_1, \ldots, x_{k+1}$

$\llcorner$ this contradicts our induction assumption above.

So the assumption, ie that g exists, that lead to h, must itself be false.

Therefore no such 'bad' poly g can exists

So in other words, if theorem is true for polys of degree k, it is also true for polys of degree $k+1$.

So by induction theorem is true for polys of any degree $n \geq 1$

i.e. true for all polys.

What about

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

for $a>1$? Theorem 7.2 tells if and how solutions to $f(x) \equiv 0 \pmod{p^{a-1}}$ "lift" to corresponding sols mod p^a.

(derivative f' of f appears here due to using finite Taylor expansion of f. in proof of 7.2).

$81 = 3^4$.

Example 7.1.

Find all solutions to

$$f(x) = x^2 + 3x - 16 \equiv 0 \mod 81$$

We'll apply the theorem repeatedly, once we have solutions to $f(x) \equiv 0 \mod 3$

$$\iff x^2 + 3x - 16 \equiv 0 \pmod 3$$

$$\iff x^2 - 1 \equiv 0 \pmod 3$$

$$\iff x^2 \equiv 1 \pmod 3$$

$$\iff x \equiv -1, 1 \pmod 3$$

$$\iff x \equiv 1, 2 \pmod 3$$

$f(1)$
$= 1 + 3 - 16$
$= -12$

So lets call $\underline{\underline{r = 1}}$

$f'(x) = 2x + 3$, $f'(r) = f'(1) = 5 \not\equiv 0 \mod 3$

so $r=1$ will lift uniquely to a solution

$s = 1 + t3$ where t is the

unique solution to

$$5t - \frac{12}{3} \equiv 0 \pmod 3$$

$$\Leftrightarrow \quad 2t - 1 \equiv 0 \pmod 3$$

$$\Leftrightarrow \quad 2t \equiv 1 \pmod 3$$

$$\Leftrightarrow \quad t \equiv 2^{-1} \pmod 3$$

$$\equiv 2 \pmod 3$$

So this is the new solution

$$s = 1 + 2 \cdot 3 = 7.$$

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

$$f(7) = 7^2 + 3 \cdot 7 - 16 = 54.$$

Attempt to lift again! Now set $r = 7$

$f'(7) = 2 \cdot 7 + 3 \equiv 17 \not\equiv 0 \pmod 3$ so again this will lift to a unique solution s

$$s = 7 + t \cdot 3^2$$

where t is the sol. to the associated linear congruence

$$17t + \frac{54}{3^2} \equiv 0 \pmod 3$$

$$\Leftrightarrow \quad 2t + 6 \equiv 0$$

$$\Leftrightarrow \quad 2t \equiv 0 \pmod 3$$

$$\Leftrightarrow \quad t \equiv 0 \pmod 3$$

So the new solution is 7 to $f(x) \equiv 0 \mod 27$ ($3^3 = 27$)

So start lifting again with $r = 7$,

$f'(7) = 17 \not\equiv 0 \pmod 3$ so again a unique lift to a solution s to $f(x) \equiv 0 \pmod{81}$

$$s = 7 + 27 \cdot t$$

where t is the sol. to

$$17t + \frac{54}{27} \equiv 0 \pmod{3}$$

$$\iff 2t + 2 \equiv 0 \pmod{3}$$

$$\iff 2t \equiv 1 \pmod{3}$$

$$\iff t \equiv 2 \pmod{3}.$$

So $s = 7 + 27 \cdot 2$
$\quad = 61.$

So we have our first solution $x \equiv 61 \bmod 81$ to $f(x) \equiv 0 \pmod{81}$

Now return to our second solution
$r = 2 \pmod{3}$ and lift this.

$f'(x) = 2x + 3$, $f'(2) = 7 \not\equiv \pmod{3}$

so a unique lift to

$s = 2 + 3 \cdot t$, where t is the sol to

$$7t + \frac{-6}{3} \equiv 0 \pmod{3}$$

$\iff t \equiv 2 \pmod 3$

$$f(2) = 2^2 + 3\cdot 2 - 16 = 4 + 6 - 16 = -6$$

So the new sol is

$$s = 2 + 3\cdot 2 = 8 \pmod 9$$

So lift $r = 8 \pmod 9$

$f'(8) = 2\cdot 8 + 3 = 19 \not\equiv 0 \bmod 3.$

So unique lift to

$s = 8 + 9t$ where t is the sol to

$$19t + \frac{72}{9} \equiv 0 \pmod 3$$

$$f(8) = 8^2 + 3\cdot 8 - 16 = 72.$$

$\iff t + 2 \equiv 0 \pmod 3$

$\iff t \equiv 1 \pmod 3$

So the new sol is

$$s = 8 + 9 = 17 \pmod{27}$$

So lift for the last time with

$$r = 17 \pmod{3^3}$$

$f'(17) = 2\cdot 17 + 3 = 37 \not\equiv 0 \pmod 3$

So unique lift to

$s = 17 + 27\cdot t$ where t is the sol

$$37t + \frac{324}{27} \equiv 0 \pmod 3$$

$\Longleftrightarrow \quad t + 12 \equiv 0 \pmod 3 \qquad f(17) = 324$

$\Longleftrightarrow \quad t \equiv 0 \pmod 3$

So the new solution is $x \equiv 17 \pmod{81}$ to $f(x) \equiv 0 \pmod{81}$.