MODULE 3

Prime Power Moduli

→ Discuss congruences modulo p^i, $i \geq 1$ (p: prime)

→ Because of fundamental theorem of arithmetic any integer $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ $e_i \geq 1$

Any congruence modulo m can be written as a set of congruences modulo $p_i^{e_i}$ $i = 1..k$.

Simplest Case ($i=1$)

→ Integer polynomial: $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$

a_i's are integers.

Solutions of congruences

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

Eg: $5x^2 + 3x + 7 \equiv 0 \pmod 5$

→ $\underline{\underline{x = 1}}$

→ Definition: The no of solns. of $f(x) \equiv 0 \pmod p$ is the number of elements in any CRS which satisfy the congruence.

→ Degree of a polynomial $f(x) = \sum_{i=0}^{d} a_i x^i$

- $f(x)$ has degree d if $a_d \not\equiv 0 \pmod p$
  - degree is the largest integer j such that $a_j \not\equiv 0 \pmod p$
  - degree is not defined if $a_j \equiv 0 \bmod p \ \forall j = 1..d$

Eg: $p = 5$ $4x^6 + 3x^2 + 2$ degree $= 6$

$a_d = 4$

$\underline{\underline{5x^6}} + \underline{\underline{3x^2}} + 2$ degree $= 2$

Consider polynomials with degree $d \le (P-1)$

$\checkmark\ \underbrace{5x^6 + 10x + 15}_{\text{invariably } 0 \bmod 5}$ degree not defined

Theorem: Any polynomial $f(x) = a_d x^d + \cdots + a_0$, which has at least one coefficient $a_j \not\equiv 0 \pmod p$ then $f(x)$ has at most d solutions.

Eg: $5x^2 + 3x + 2 \equiv 0 \pmod{17}$ at most 2 solns. mod 17.

PROOF: Prove it by mathematical induction:

Base Case $d = 1$ $\quad ax - b \equiv 0 \pmod p \implies ax \equiv b \pmod p$

This has solution if and only if $(a,p) \mid b$.

If $(a,p) = 1$, consider two solutions x_1 & x_2.

$ax_1 \equiv b \pmod p$ & $ax_2 \equiv b \pmod p$. This implies that $ax_1 \equiv ax_2 \pmod p$ or $p \mid a(x_2 - x_1)$. This inturn means that $x_1 \equiv x_2 \pmod p$.

If $(a,p) = P$ then b is also $0 \bmod p$. Hence $ax - b$ does not degree defined and the theorem is not applicable.

Induction Hypothesis: Assume the theorem holds for all polynomials of degree $\le (d-1)$

Consider $f(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0$.

If $f(x)$ does not have any soln: then the theorem is proved.

Otherwise there at least one solution, say a. That $f(a) \equiv 0 \pmod p$.

Now $f(x) - f(a) = \sum_{i=1}^{d} a_i x^i - \sum_{i=1}^{d} a_i a^i$

$$x^k - a^k = (x-a)(\underbrace{x^{k-1} + x^{k-2} + \cdots}_{k-1})$$

$$= \sum_{i=1}^{d} a_i (x^i - a^i)$$

$$= \sum_{i=1}^{d} a_i (x-a)(\text{Poly: of degree } i-1)$$

$$= (x-a)\Big[\underbrace{\sum_{i=1}^{d} a_i x (\text{Poly: degree } i-1)}_{g(x)}\Big]$$

$g(x)$ has degree $\le (d-1)$ and hence by Ind. Hyp: has at most $(d-1)$ solutions mod p.

$f(x) - f(a) = (x-a)\, g(x)$.

There is at least one coefficient in $g(x)$ which is not zero. (Suppose all coefficients are zeroes then all the coefficients of $f(x)$ will also be 0.

$g(x) = \sum_{i=1}^{d-1} c_i x^i$. $\quad (x-a)\, g(x) = (x-a)\left(\sum_i c_i x^i\right)$

$= \underbrace{x\left(\sum_i c_i x^i\right) - a\left(\sum_i c_i x^i\right)}$

$= h(x)$.

coefficient of x^i in $h(x) = \begin{cases} c_{d-1} & \text{if } i = d \\ c_{i-1} - a c_i & 1 \le i \le d-1 \\ -a c_0 & \text{if } i = 0 \end{cases}$

See all the coeffs are 0s.

Hence $= (x-a)\, g(x) + f(a)$ will also have all the coeffts zero.)

$f(x) = f(a) + (x-a)\, g(x) \equiv (x-a)\, g(x) \pmod p$

Hence every solution of $g(x) \equiv 0 \pmod p$ is also a solution of $f(x)$. The total nos of solutions hence is $\le \underbrace{d-1}_{\text{solns. of } g(x)} + \underbrace{1}_{a} = d$. ∎

Why didn't we consider terms with powers $\ge p$?

Consider x^k : $k \ge p$. Since p is prime $x^{p-1} \equiv 1 \bmod p$ if $(x,p) = 1$ otherwise $x^p \equiv x \pmod p$. Therefore in both cases $p \mid (x^p - x)$

i.e. $x^p \equiv x \pmod p$ $\forall\, x \in \mathbb{Z}$.

Hence $x^k \equiv x^{pl+r} = \underbrace{x^{pl}} \cdot x^r \equiv x^l \cdot x^r = x^{l+r}$

$x^{pl} = (x^p)^l$

Eg.

$p = 5$

$\downarrow$

$x^5 \equiv x \pmod 5$

$x^{16} \Rightarrow x^{15} \cdot x$.

$\Rightarrow (x^5)^3 \cdot x \Rightarrow x^3 \cdot x = x^4$

Solving Congruences Modulo p^e, $e>1$

Solve Congruence of the form $f(x)\equiv 0 \pmod{p^e}$

$p^3 \mid f(\hat{x}) \Rightarrow p^2 \mid f(\hat{x})$

$5^2 \nmid \alpha \Rightarrow 5 \mid \alpha$

Procedure

$p^2 \mid f(\hat{x}) \Rightarrow p \mid f(\hat{x})$.

1. Start with $f(x)\equiv 0 \pmod{p}$
2. Generate solutions for $f(x)\equiv 0 \pmod{p^2}$
3. Generate solutions for $f(x)\equiv 0 \pmod{p^3}$ ...

⋮

[The logic behind the stepwise procedure is that every solution of $f(x)\equiv 0 \pmod{p^{i+1}}$ is also a Solution of $f(x)\equiv 0 \pmod{p^i}$. Therefore we first solve the Simpler problem $f(x)\equiv 0 \pmod{p^i}$ and then check which of those solutions Satisfy $f(x)\equiv 0 \pmod{p^{i+1}}$]

Each solution of $f(x)\equiv 0 \pmod{p^i}$ may generate solutions $\pmod{p^{i+1}}$.

Say t satisfies $f(x)\equiv 0 \pmod{p^i}$ ie $f(t)\equiv 0 \pmod{p^i}$.

t generates further candidates $t+kp^i$ $k=0,1,2$

We will figure out k for which $t+kp^i$ is a solution $\bmod p^{i+1}$.

This translates to the Congruence

$$f(t+kp^i)\equiv 0 \pmod{p^{i+1}} \quad \text{(Solve for } k\text{)}$$

Taylor Series Expansion [Assume that f is degree d]

$$f(t+kp^i) = f(t) + kp^i f'(t) + \underbrace{\frac{(kp^i)^2}{2} f''(t) + \cdots + \frac{(kp^i)^d}{d!} f^{(d)}(t)}_{\text{are multiples of } p^{i+1} \text{ (and hence congruent to 0 mod } p^{i+1})}$$

$$\equiv \left[f(t) + kp^i f'(t)\right] \pmod{p^{i+1}}$$

We need to find k s.t

$$\left[f(t) + kp^i f'(t)\right] \equiv 0 \pmod{p^{i+1}}$$

OR

$$f(t) \equiv -kp^i f'(t) \pmod{p^{i+1}} \longrightarrow \boxed{A}$$

Now

$$p^i \mid f(t) \text{ and also } p^i \mid -kp^i f'(t)$$

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

p^{i+1}

Congruence $\boxed{A}$ therefore is equivalent to

$$\boxed{\frac{f(t)}{p^i} \equiv -k f'(t) \pmod{p}}.$$

$f(t)$ $f'(t)$

Solve this Congruence.

$$\boxed{\frac{f(t)}{p^i}} \equiv -k\boxed{f'(t)} \pmod{p}$$

$\boxed{t+kp^i}$

If t happens to satisfy $f(t) \equiv 0 \pmod{p^{i+1}}$ also then $-kp^i f'(t) \equiv 0 \pmod{p^{i+1}}$. If $f'(t) \equiv 0 \pmod{p}$ then $t+kp^i$ is a Soln: of $f(x) \equiv 0 \pmod{p^{i+1}}$ $\forall k = \{0 \ldots (p-1)\}$. Otherwise k has to be a multiple of p^{i+1} and hence $t+kp^i$ is congruent to $t \pmod{p^{i+1}}$ [and hence not a different Solution].

Ex: $f(x) = 2x+3$ $p=5$

$\{0, 1, 2, 3, 4, 5, 6 \dots 11 \dots 24\}$

$\boxed{1}$ $\boxed{6}$ $\boxed{11}$ $\boxed{16}$ $\boxed{21}$

Solve $2x+3 \equiv 0 \pmod{5^2}$

→ Solution: • First solve $2x+3 \equiv 0 \pmod 5$

$t=1$ is the only solution.

• $f(t) = 5$ $f'(t) = 2$ $2x+3 \Rightarrow 2$

$\boxed{f(t) \not\equiv 0 \pmod{25}}$

$\frac{f(t)}{p} = 1 \equiv -k \cdot 2 \pmod 5$.

$k=2$ is a solution.

Therefore $t+k.p = 1+2\cdot5 = 11$ is a solution.

$[2\cdot 11+3 = 25 \equiv 0 \mod 25]$

→ Therefore the only solution is 11

Eg: $f(x) \equiv 0 \mod (7^3)$

$f(x) = x^2+x+47$

① $x^2+x+47 \equiv 0 \pmod 7$

Solutions $= \{1, 5\}$

$1 \to t_1$ $5 \to t_2$

Solutions mod 7^2 from $t_1 = 1$

$1, 50, 99, 148, 197, 246, 295, 344$

$f(t_1) = 49 \equiv 0 \pmod{7^2}$ $f'(t_1) = 2x+1 = 3$

Hence t_1 generates no solns. mod 7^2, other than itself

Solutions mod 7^2 from $t_2 = 5$

$f(5) = 77 \not\equiv 0 \mod 7^2$ $f'(5) = 2x+1 = 11$

$\frac{f(t_2)}{p} = \frac{f(t_2)}{7} = 11$

$$11 \equiv -11k \pmod 7$$

$k = 6$ is a solution.

Solution generated by $t_2 = t_2 + k \cdot p^i$ $\quad i=1$

$$= 5 + 6 \times 7 = \underline{\underline{47}}$$

Therefore solns mod 7^2 are

$$\{1, 47\}$$

Solutions mod 7^3 generated by $\{1, 47\}$

Solutions from $t_1 = 1$

$$f(t_1) = 49 \not\equiv 0 \pmod{343} \qquad f'(t_1) = 2x + 1 = \underline{\underline{3}}.$$

$$\frac{f(t_1)}{p^2} \equiv -k \cdot 3 \pmod 7$$

$$1 \equiv -k \cdot 3 \pmod 7 \qquad \underline{\underline{k = 2}}$$

$$t_1 + k \cdot p^2 = 1 + 2 \cdot 49 = \underline{\underline{99}}$$

Soln. from $t_2 = 47$

$$f(47) = 47^2 + 47 + 47$$

$$= 47 \times 49 = \underline{\underline{2303}} \not\equiv 0 \bmod (343)$$

$$\begin{array}{r} 47 \\ 5 \\ \hline 275 \\ \hline 2350 \\ -47 \\ \hline 2303 \end{array}$$

Primality Test using Fermat's theorem

→ Consider the congruence $a^n \equiv a \pmod n$

→ We already know from Fermats' little theorem that if n is prime, the congruence is valid.

$$a^n - a = a(a^{n-1} - 1)$$

Therefore if $(a,n)=1$ then $(a^{n-1}-1)$ is a multiple of n, otherwise $(a,n)=n$ and hence $n \mid a(a^{n-1}-1)$

→ For $n \in \mathbb{N}$, if for some a, $a^n \not\equiv a \pmod n$ then we can be sure that n is not prime

(This gives a primality check algorithm).

* But you will have to try all a's from 0 to $(n-1)$ making the algorithm inefficient.

Therefore the test was done for $a=2$ alone

(Probably this started with Chinese)

PRIMALITY TEST

$$2^n \equiv 2 \pmod n \begin{cases} \xrightarrow{\text{yes}} n \text{ is prime} \\ \xrightarrow{\text{no}} n \text{ is composite} \end{cases}$$

Pseudo prime

* There are composite numbers which satisfy the congruence $2^n \equiv 2 \pmod n$

→ Smallest Pseudo-prime is 341 $(= 11 \cdot 31)$

Pseudo-prime → ∞

THEOREM : There are infinitely many pseudo primes

PROOF : We claim that if n is a pseudo-prime, so is $2^n - 1$. [This precludes the no. of pseudo-primes being finite]

Suppose n is a pseudo-prime. Then

$2^n \equiv 2 \pmod n$ or equivalently $2^n = nk + 2$. Therefore

$$2^{(2^n-1)} = 2^{nk+1} = 2 \cdot \underbrace{2^{nk}}_{1 \pmod{2^n-1}} \equiv 2 \bmod (2^n - 1)$$ since $2^n \equiv 1 \pmod{2^n-1}$ ∎

SUMMARY

→ Primality Testing : $2^n \equiv 2 \pmod n$ → yes ⇒ Prime; → no ⇒ Composite.

→ Yes part is not true

→ such composite n's which satisfy the test are Pseudo primes

→ There are infinitely many Pseudo-primes