§14 Polynomial equations in modular arithmetics.

We consider

$$a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0 \equiv 0 \pmod{m}$$

x is unknown

$a_0, a_1, \ldots, a_d \in \mathbb{Z}$, $a_d \not\equiv 0 \pmod{m}$

$m \in \mathbb{Z}^+$ is a modulus.

Before we considered the case $d=1$:

$$ax \equiv c \pmod{m}$$

Principle 1: We can replace a_i by a_i' where $a_i \equiv a_i' \pmod{m}$ without changing the set of solutions.

Principle 2: If ~~f~~ x is a solution and $y \equiv x \pmod{m}$ then y is a solution too.

I.e. the solution set is a union of congruence classes modulo m.

Examples: (1) $x^3 + 4x + 4 \equiv 0 \pmod{5}$

By principle 1 we can rewrite the equation:

$$x^3 - x - 1 \equiv 0 \pmod{5}$$

By principle 2 it is enough to look for solutions ~~f~~ inside some complete set of residues mod 5.

x	0	1	2	3	4
$x^3-x-1 \pmod 5$	4	4	0	3	4

solution is $x \equiv 2 \pmod 5$.

(2) $x^2 \equiv 1 \pmod 8$

Notice: x is odd.

$1^2 \equiv 1$, $3^2 \equiv 1$, $5^2 \equiv 1$, $7^2 \equiv 1 \pmod 8$

So the solution is $x \equiv 1$ or 3 or 5 or $7 \pmod 8$

or $x \equiv 1 \pmod 2$.

If p is prime then the only solutions of $x^2 \equiv 1 \pmod p$ are

$x \equiv 1$ or $x \equiv -1 \pmod p$.

($p \mid x^2-1 \Rightarrow p \mid (x-1)(x+1) \Rightarrow$ [p is prime]

$\Rightarrow p \mid x-1$ or $p \mid x+1$)

Example (3) $x^2 \equiv -1 \pmod 5$

Notice: $-1 \equiv 4 \equiv 2^2 \pmod 5$

Then $x^2 \equiv 4 \pmod 5$ gives two solutions:

$x \equiv 2$ or $x \equiv -2 \equiv 3 \pmod 5$

(This is because ~~for~~ $a^2 \equiv b^2 \pmod p$ implies

$a \equiv b$ or $a \equiv -b \pmod p$ for prime p - Ex)

Example (4): $x^2 \equiv -1 \pmod 7$

x	0	1	2	3	4	5	6
$x^2 \pmod 7$	0	1	4	2	2	4	1

No -1's (or 6's) $\Rightarrow$ no solutions.

Proposition: Let p be prime, $p \equiv 3 \pmod 4$. Then $x^2 \equiv -1 \pmod p$ does not have solutions.

Proof: Assume x is a solution.

FLT $\Rightarrow x^{p-1} \equiv 1 \pmod p$

$$1 \equiv x^{p-1} \equiv (x^2)^{\frac{p-1}{2}} \equiv (-1)^{\overset{\uparrow}{\frac{p-1}{2}}} \equiv -1 \pmod p$$

odd

Contradiction. $\boxtimes$

Proposition: Let p be prime and $p \equiv 1 \pmod 4$. Then $x^2 \equiv -1 \pmod p$ has (two congruence classes of) solutions.

Proof.

$$(p-1)! = \underbrace{1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots}_{\left(\frac{p-1}{2}\right)!} \cdot \underbrace{(p-3)(p-2)(p-1)}_{(-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!}$$

$$(p-3) \equiv -3, \quad (p-2) \equiv -2, \quad (p-1) \equiv -1$$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot \left(\left(\tfrac{p-1}{2}\right)!\right)^2 \equiv \left(\left(\tfrac{p-1}{2}\right)!\right)^2 \pmod p.$$

Split the set $\{1,2,3,\dots,p-1\}$ into pairs $(a, a^{-1} (\text{mod } p))$.

Numbers a without pair satisfy

$a \equiv a^{-1} \pmod p \Rightarrow a^2 \equiv 1 \pmod p$

$\Rightarrow a \equiv 1$ or $a \equiv -1 \pmod p$.

Rewrite $(p-1)! \equiv 1 \cdot (-1) \cdot \underbrace{(2 \cdot 2^{-1})}_{1} \cdot \underbrace{(3 \cdot 3^{-1})}_{1} \cdot \dots$

$\equiv -1 \pmod p$

Finally: $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \pmod p$ and $\left(\frac{p-1}{2}\right)!$ is a solution. $\boxtimes$

Theorem. Let p be prime,

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

$a_i \in \mathbb{Z}$, $a_d \not\equiv 0 \pmod p$.

Then the solution of the equation $f(x) \equiv 0 \pmod p$ ~~is~~ is the union of at most d congruence classes modulo p.

Proof: By induction.

$d = 1$: $a_1 x + a_0 \equiv 0 \pmod p$. Gives one solution $x \equiv -a_0 a_1^{-1} \pmod p$.

Assume the statement is true for $d-1$ and prove it for d.

If there are no solutions – nothing to prove.
Otherwise let c be a solution

$$f(c) \equiv 0 \pmod p$$

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

$$= (x-c)\Big(a_d(x^{d-1} + x^{d-2}c + \dots + c^{d-1}) + a_{d-1}(\dots)$$

$$+ \dots + a_1\Big) = (x-c)g(x) \pmod p$$

$g(x)$ is a polynomial of degree $d-1$

$$f(x) \equiv 0 \pmod p \Rightarrow f(x) - f(c) \equiv 0 \pmod p$$

$\Rightarrow p \mid f(x) - f(c) \Rightarrow p \mid (x-c)g(x)$

$\Rightarrow p \mid x - c$ or $p \mid g(x)$.

In other words,

$x - c \equiv 0 \pmod p \leftarrow$ one solution

or $g(x) \equiv 0 \pmod p \leftarrow \leq d-1$ solutions $\boxtimes$