$$\begin{tikzcd}[row sep=small] & x^2 \equiv 1 \pmod{9} \\ x^2 \equiv 1 \pmod{36} \arrow[ur] \arrow[dr] & \\ & x^2 \equiv 1 \pmod{4} \end{tikzcd}$$

We should try to understand $\mathbb{Z}_{p^\alpha}$ to understand $\mathbb{Z}_n$ in general. We begin with the case of $\alpha = 1$, $\mathbb{Z}_p$.

$$\mathbb{Z}_p = \{ [0], [1], [2], \dots, [p-1] \}$$

Congruences modulo p

Linear congruences : $ax \equiv b \pmod{p}$

- Case I : $(p, a) = p$, i.e. $p \mid a$ (or $a \equiv 0 \pmod{p}$)
  Solution x exist $\iff$ $b \equiv 0 \pmod{p}$

- Case II : $(p, a) = 1$ $\Rightarrow$ There is a unique solution x in $\mathbb{Z}_{\frac{p}{(p,a)}} = \mathbb{Z}_p$.

  - In particular, a^{-1} always exist $\pmod{p}$ unless $a \equiv 0 \pmod{p}$

Let's rewrite this congruence as $f(x) \equiv 0 \pmod{p}$ where $f(x) = ax - b$.

Note that $f(x) = 3x - 5$ and $g(x) = 10x + 2$ are essentially the same modulo 7 (always $f(x) \equiv g(x) \pmod{7}$) because $3 \equiv 10 \pmod{7}$ and $-5 \equiv 2 \pmod{7}$. So, we can always replace the coefficients with any representative of the same congruence class.

In $\mathbb{R}$, $\mathbb{C}$ a non-zero polynomial of degree d has at most d roots. Can we say the same thing for the roots in $\mathbb{Z}_p$?

- $d = 0$: trivial
- $d = 1$: shown above

<u>Theorem:</u> (Lagrange) $f(x) = a_d x^d + a_{d-1} x^{d-1} + \dots + a_1 x + a_0$ is a polynomial with integer coefficients such that $a_i \not\equiv 0 \pmod{p}$ for at least one i. Then, $f(x) \equiv 0 \pmod{p}$ has at most d solutions in $\mathbb{Z}_p$.

- Could be less than d roots: $px^2 + 2x + 3$ has degree 2 but can be reduced to $2x + 3$ which can have at most 1 root in mod p.

($px^2 \equiv 0 \pmod{p} \Rightarrow px^2 + 2x + 3 \equiv 2x + 3 \pmod{p}$)

- Could be less than d roots even if $a_d \not\equiv 0 \pmod p$. For example $x^2+1 \pmod 3$.

- If $d \geqslant p \Rightarrow$ trivial.

Proof: Induction on d.

Base cases $d=0$, $d=1$ are already done.

Assume true for $d-1$, prove for d.

- If $f(x) \equiv 0 \pmod p$ has no root, then we are done as $0 \leqslant d$.

- Suppose a is a root, i.e. $f(a) \equiv 0 \pmod p$

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

- $x^i - a^i = (x-a)(x^{i-1} + ax^{i-2} + a^2x^{i-3} + \dots + a^{i-2}x + a^{i-1})$

Taking out the common factor $x-a$, we can write $f(x) - f(a) = (x-a)\cdot g(x)$ for some polynomial $g(x)$ with integer coefficient (and $\deg g(x) = d-1$)

$$\Rightarrow f(x) = f(a) + (x-a)\cdot g(x)$$

$$f(x) \equiv 0 \pmod p \iff f(a) + (x-a)g(x) \equiv 0 \pmod p$$

$$\iff (x-a)g(x) \equiv 0 \pmod p$$

$$\iff x \equiv a \pmod p \quad \text{or} \quad g(x) \equiv 0 \pmod p$$

$\Rightarrow$ At most $1 + (d-1) = d$ solutions.

<u>Remark</u>: $f(a) \equiv 0 \pmod p \Rightarrow f(x) \equiv (x-a)\,g(x) \pmod p$

<u>Corollary</u>: If $f(x) \equiv a_d x^d + \dots + a_0 \equiv 0 \pmod p$ has more than d roots, then $a_i \equiv 0 \pmod p$ for all i.

<u>Examples</u>:

1. $f(x) = x^2 - 10x + 4$ in mod 5.

$f(x) \equiv x^2 + 4 \equiv x^2 - 1 \pmod 5$ roots: $1, 4$ in $\mathbb{Z}_p$.

2. $f(x) = 8x^3 + 4x^2 - 5x$ in mod 7

$f(x) = x \cdot (8x^2 + 4x - 5)$

- $8x^2 + 4x - 5 \equiv 0 \pmod 7$

  Try $0, 1, 2, 3, 4, 5, 6 \Rightarrow x \equiv 1,\ x \equiv 2 \pmod 7$

$8x^2 + 4x - 5 \equiv c \cdot (x-1)(x-2) \pmod 7$

$8x^2 + 4x - 5 \equiv cx^2 - 3cx + 2c \pmod 7$

$c \equiv 1 \pmod 7 \Rightarrow f(x) = x \cdot (x-1)(x-2) \pmod 7$

3. $f(x) = x^3 + 2x^2 + 3x - 1$ in mod 5

$f(1) = 5 \equiv 0 \pmod{5}$

$f(x) \equiv (x-1)(x^2 + 3x + 1)$

$g(x) = x^2 + 3x + 1 \Rightarrow g(1) \equiv 0 \pmod{5}$

$g(x) = (x-1)(x+4)$

$\Rightarrow f(x) \equiv (x-1)^2 \cdot (x+4) \equiv (x-1)^3 \pmod{5}$

Solving polynomial congruences (mod p), we can reduce the coefficients (mod p) and the next theorem will allow us to reduce the degree of the polynomial as well.

Theorem: (Fermat) For $a \not\equiv 0 \pmod{p}$, then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: Observe that the sets $\{1, 2, \ldots, p-1\}$ and $\{a, 2\cdot a, 3\cdot a, \ldots, (p-1)\cdot a\}$ are the same mod p.

For each $b \in \{1, 2, \ldots, p-1\}$, we have $ax \equiv b \pmod{p}$ for a unique x.

Then, the product of the elements of these sets must also be the same:

$1 \cdot 2 \cdot 3 \cdot \dots (p-1) \equiv a \cdot (2a) \cdot (3a) \cdot \dots ((p-1)a) \pmod p$

$\Rightarrow (p-1)! \equiv (p-1)! \cdot a^{p-1} \pmod p$ $\quad ((p-1)!, p) = 1$.

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

- $f(x) = x^{p-1} - 1$ and $g(x) = (x-1)(x-2) \cdot \dots \cdot (x-(p-1))$.

  $\Rightarrow$ $f(x)$ and $g(x)$ have the same coefficients modulo p.

  Proof: Define $h(x) = f(x) - g(x)$

  $\deg h \leq p-2$ and $1, 2, \dots, p-1$ are roots of h in $\mathbb{Z}_p$ (more than $\deg h$ roots)

  $\Rightarrow$ h has all coefficients 0 mod p

  $\Rightarrow$ f and g have the same coefficients mod p.

- For all a, we have $a^p \equiv a \pmod p$

- $x^p - x$ and $x \cdot (x-1)(x-2) \cdot \dots \cdot (x-(p-1))$ have the same coefficients modulo p.

Some Applications of Fermat's Theorem

① Compute $2^{1003} \pmod{11}$

$2^{1003} \equiv (2^{10})^{100} \cdot 2^3 \equiv 1^{100} \cdot 2^3 \equiv 8 \pmod{11}$

② Prove that $n^{25}-n$ is divisible by 30 for all n.

- 5 divides $n^{25}-n$:

  - If $n \equiv 0 \pmod 5$, then $n^{25}-n \equiv 0 \pmod 5$

  - If $n \not\equiv 0 \pmod 5$, then

  $n^{25}-n \equiv (n^4)^6 \cdot n - n \equiv 1^6 \cdot n - n \equiv 0 \pmod 5$

- 3 divides $n^{25}-n$:

  - If $n \equiv 0 \pmod 3$, then $n^{25}-n \equiv 0 \pmod 3$

  - If $n \not\equiv 0 \pmod 3$, then

  $n^{25} - n \equiv (n^2)^{12} \cdot n - n \equiv 1^{12} \cdot n - n \equiv 0 \pmod 3$

- 2 divides $n^{25}-n$:

  "similar"

$\Rightarrow$ $[2,3,5] = 30$ divides $n^{25}-n$.

③ Solve $x^{17} + 6x^{14} + 2x^5 + 1 \equiv 0 \pmod 5$

- If $x \equiv 0 \pmod 5$, then "not a solution"

  $x^{17} + 6x^{14} + 2x^5 + 1 \not\equiv 0 \pmod 5$.

- If $x \not\equiv 0 \pmod 5$

$$x^{17} + 6x^{14} + 2x^5 + 1 \equiv (x^4)^4 \cdot x + (x^4)^3 \cdot x^2 + 2x^4 \cdot x + 1$$

$$\equiv x + x^2 + 2x + 1$$

$$\equiv x^2 + 3x + 1.$$

$\Rightarrow x^2 + 3x + 1 \equiv 0 \pmod 5$

$\Rightarrow x^2 - 2x + 1 \equiv 0 \pmod 5$

$\Rightarrow (x-1)^2 \equiv 0 \pmod 5$

$\Rightarrow x \equiv 1 \pmod 5$.