From previous lecture: $p=11$, $a=2$ is a prim. root;

n	0	1	2	3	4	5	6	7	8	9	10
2^n	1	2	4	8	5	10	9	7	3	6	1

Example: (a) $x^5 \equiv 10 \pmod{11}$

We have $10 \equiv 2^5 \pmod{11} \Rightarrow x \equiv 2$ is a solution

The general solution:

$x \equiv 2^1$ or 2^3 or 2^5 or 2^7 or $2^9 \pmod{11}$

$\equiv 2$ or 8 or 10 or 7 or $6 \pmod{11}$

(b) $x^5 \equiv 7 \pmod{11}$

We have $7 \equiv 2^7 \pmod{11}$ and $5 \nmid 7$

$\Rightarrow$ there are no solutions.

Consider $x^m \equiv c \pmod{p}$ where $\gcd(m, p-1) = 1$

Let a be a prim. root mod p.

Write $x \equiv a^i \pmod{p}$, $c \equiv a^k \pmod{p}$

$x^m \equiv c \pmod{p} \Leftrightarrow a^{im} \equiv a^k \pmod{p}$

$\Leftrightarrow im \equiv k \pmod{p-1} \Leftrightarrow i \equiv m^{-1}k \pmod{p-1}$

Therefore $x \equiv a^{m^{-1}k} \equiv c^{m^{-1}} \pmod{p}$

inverse of m modulo $p-1$

Example: $x^3 \equiv 6 \pmod{11}$

$x \equiv 2^i \pmod{11}$ $\quad 6 \equiv 2^9 \pmod{11}$

We can rewrite the equation to

$3i \equiv 9 \pmod{10} \Leftrightarrow i \equiv 3 \pmod{10}$

$\Rightarrow x \equiv 2^3 \equiv 8 \pmod{11}$.

§18 Polynomial interpolation in modular arithmetics.

It is used to solve the problem: How to split some secret among n people so that $\geq k$ people are needed to derive a secret?

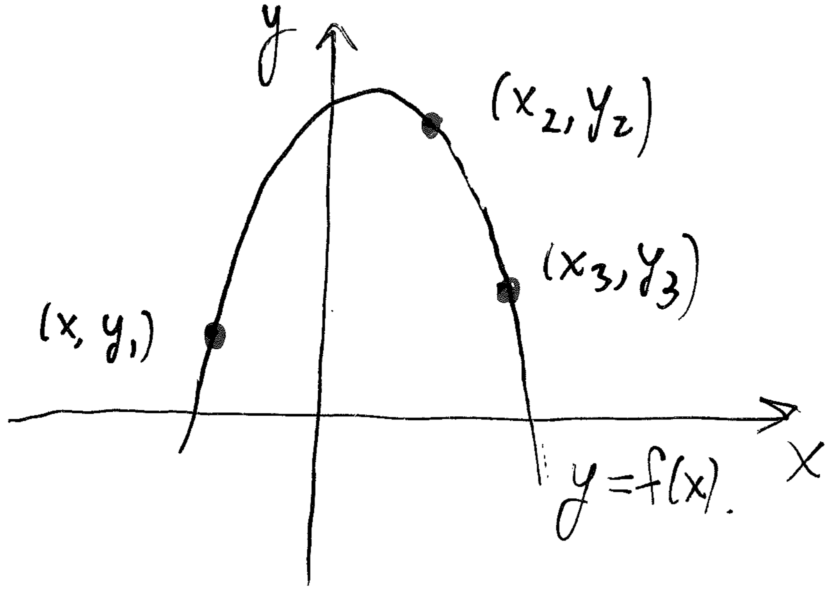
§18.1 Lagrange Interpolation Formula.

In $\mathbb{R}$ if we are given k points $(x_1, y_1), (x_2, y_2), \dots, (x_k, y_k) \in \mathbb{R}^2$ with distinct $x_1, x_2, \dots, x_k$ then there exists the unique polynomial

$$f(x) = a_{k-1}x^{k-1} + \dots + a_1 x + a_0 \text{ with } a_0, \dots, a_{k-1} \in \mathbb{R}$$

such that

$$f(x_1) = y_1$$
$$f(x_2) = y_2$$
$$\dots$$
$$f(x_k) = y_k$$



Theorem. Let p be prime, $x_1, x_2, \dots, x_k \in \mathbb{Z}$ from distinct residue classes mod p; $y_1, y_2, \dots, y_k \in \mathbb{Z}$.
Then $\exists$ unique polynomial (up to the congruence mod p) $f(x) = a_{k-1}x^{k-1} + \dots + a_1 x + a_0$ with $a_0, a_1, \dots, a_{k-1} \in \{0, 1, \dots, p-1\}$ such that

$$f(x_1) \equiv y_1 \pmod p$$
$$f(x_2) \equiv y_2 \pmod p$$
$$\dots$$
$$f(x_k) \equiv y_k \pmod p.$$

Proof: Uniqueness.
Let $f(x)$ and $g(x)$ satisfy all the conditions.
Consider $h(x) = f(x) - g(x)$.
degree of $h(x)$ is $\leq k-1$.
$h(x)$ has roots $x_1, x_2, \dots, x_k$.
By prev. Theorem (number of roots is $\leq$ degree of the polynomial) this is only possible if

$h(x) \equiv 0 \pmod{p}$. $\Rightarrow f(x) \equiv g(x) \pmod{p}$.

Existence (Lagrange Interpolation Formula):

Consider $f(x) = \sum_{i=1}^{k} y_i \frac{\prod_{j\neq i}(x-x_j)}{\prod_{j\neq i}(x_i-x_j)} = y_1 \frac{(x-x_2)(x-x_3)\cdots(x-x_k)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_k)}$

$+ y_2 \frac{(x-x_1)(x-x_3)\cdots(x-x_k)}{(x_2-x_1)(x_2-x_3)\cdots(x_2-x_k)} + \cdots + y_k \frac{(x-x_1)(x-x_2)\cdots(x-x_{k-1})}{(x_k-x_1)(x_k-x_2)\cdots(x_k-x_{k-1})}$.

We can check that it satisfies all the conditions. (Ex!) $\boxtimes$

Example. Find $f(x) = ax^2+bx+c$, $a,b,c \in \{0,1,\dots,10\}$ such that

$$f(1) \equiv 5 \pmod{11}$$
$$f(2) \equiv 2 \pmod{11}$$
$$f(4) \equiv 6 \pmod{11}$$

LIF gives

$$f(x) = 5\cdot\frac{(x-2)(x-4)}{(1-2)(1-4)} + 2\cdot\frac{(x-1)(x-4)}{(2-1)(2-4)} + 6\,\frac{(x-1)(x-2)}{(4-1)(4-2)}$$

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

$$\equiv 9(x^2-6x+8) - (x^2-5x+4) + (x^2-3x+2)$$

$$\equiv 9x^2+3x+4 \pmod{11}$$

Check: $f(1) \equiv 16 \equiv 5 \pmod{11}$
$f(2) \equiv 2 \pmod{11}$

$f(4) \equiv 160 \equiv 6 \pmod{11}$

§18.2 Splitting secret.

We have n people. Only $\geq k$ of them should be able to work out the secret.

Algorithm: (a) Take a big prime number p (at least $> n$)

(b) Randomly compute $a_0, a_1, \dots, a_{k-1} \pmod p$

(or we encode the secret as a sequence $a_0, a_1, \dots, a_{k-1} \pmod p$)

(c) Let $f(x) = a_{k-1}x^{k-1} + \dots + a_1 x + a_0$

Tell person i ($i \in \{0, \dots, n\}$) the value $f(i) \pmod p$