$P(x) = \underline{2}x^3 + \underline{3}x^2 - \underline{6}x + \underline{4} \pmod{11}$

Nontrivial

* Polynomial of degree d has at most d roots.

$\pmod m$ m prime. $+, -, \times, \div$ non-zero.

$a \pmod m$ Does $a^{-1} \bmod m$ exist?

$a^{-1} = b$.

if and only if $a \cdot b \equiv 1 \pmod m$

$\gcd(a, m) = 1$.

$5^{-1} \pmod{12} = 5$.

~~$7^{-1} \pmod{12}$~~

~~$7x \neq 1 \pmod{12}$~~

$5x = 1 \pmod{12}$

$5x = 1 + \underline{k \cdot 12}$.

$7^{-1} \pmod{15} = 13$.

$12 \cdot 2 + 1 = 25$.

$x = \frac{25}{5} = \underline{5}$

$15+1, 30+1, 45+1, 60+1, 75+1,$

$\frac{90+1}{7} = \boxed{13}$

$\gcd(82, 67) = 1.$

$82x + 67y = 1$

$67^{-1} \bmod 82$

$67y = 1 \pmod{82}$

$82 = 67 \times 1 + 15 \quad \gcd(82, 67)$

$67 = 15 \times 4 + 7 \quad \gcd(67, 15)$

$15 = 7 \times 2 + 1 \quad \gcd(15, 7) = 1$

$7 = 1 \times 7 + 0$

$15x' + 7y' = 1$

$15 \times 1 + 7 \times (-2) = 1.$

$67x'' + 15y'' = 1.$

substitute $7 = 67 - 15 \times 4$

$15 \times 1 + (67 - 15 \times 4) \times (-2) = 1.$

$15 \times 9 - 67 \times 2 = 1.$

substitute $15 = 82 - 67 \times 1.$

$(82 - 67 \times 1) \times 9 - 67 \times 2 = 1.$

$82 \times 9 - 67 \times 11 = 1.$

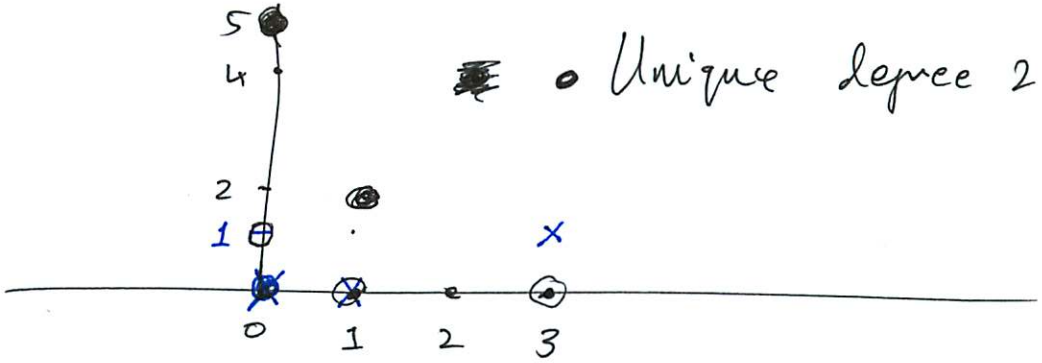
$\mod 82.$

$-11 = 71 \pmod{82}$

$67^{-1} \pmod{82}$

$67 \times -11 = 1 \pmod{82}$

✓ * Polynomial of degree d has at most d roots.



• Unique degree 2 polynomial. (mod 11)

$(0,5)$, $(1,2)$, $(3,4)$

$P(x)$ degree d. (x_1,y_1), (x_2,y_2), ---, (x_{d+1}, y_{d+1})

Suppose not unique: $Q(x) \neq P(x)$ $\underbrace{P(x)-Q(x)}_{d}$ Contradiction.

Lagrange Interpolation.

zero at $x=1$ & $x=3$.

$\Delta_3(x) = \frac{2X(X-1)}{\cancel{X}}$ $(X-1)(x-3)$.

$3 \times 2 = 6$.

$6^{-1} \bmod 11$.

$6 \cdot \boxed{2} = 1 \bmod 11$

$P(0) = 5$

$P(1) = 2$

$P(3) = 4$

$\Delta_0(x) = \frac{4(x-1)(x-3)}{\cancel{3}}$ $x=0 \leftrightarrow 3$.

$3 \cdot 4 = 1 \pmod{11}$

$\Delta_1(x) = \frac{5x(x-3)}{-2}$ $(-2)(-6) = 1 \bmod 11$

11

5

$$P(x) = 5\Delta_0(x) + 2\Delta_1(x) + 4\Delta_3(x).$$

$$P(0) = 5\Delta_0(0) + 2\Delta_1(0) + 4\Delta_3(0).$$

$$= 5$$

$$P(1) = 5\Delta_0(1) + 2\Delta_1(1) + 4\Delta_3(1).$$

$$= 2 \times 1 = 2.$$

$$P(x) = 5 \cdot 4(x-1)(x-3) + 2 \cdot 5 x(x-3) + 4 \cdot 2 x(x-1)$$

$$= -2(x-1)(x-3) - x(x-3) + 8x(x-1).$$

$$= -2(x^2 - 4x + 3) - x^2 + 3x + 8x^2 - 8x.$$

$$= 5x^2 - 3x + 5$$

$$= 5x^2 + 3x + 5.$$

$P(0) = 5$

$P(1) = 2$

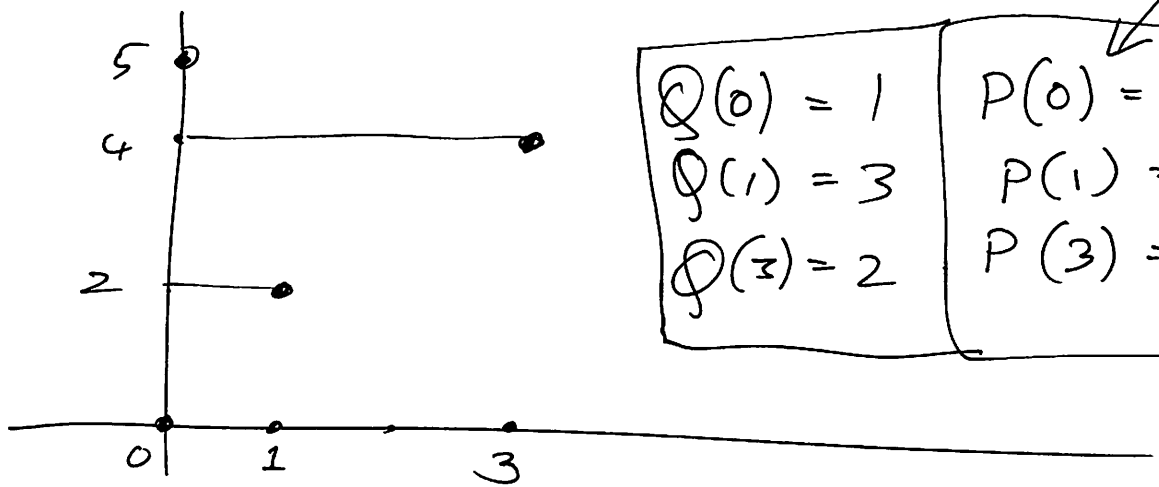
$P(3) = 5 \times 9 + 3 \times 3 + 5$

$= 1 + 9 + 5$

$= 4$

$P(x) = \underline{5}x^2 + \underline{3}x + \underline{5}$ (mod 11)

coefficients of polynomial. (5, 3, 5).



$Q(0) = 1$	$P(0) = 5$	$PQ(0) = 5$
$Q(1) = 3$	$P(1) = 2$	$PQ(1) = 6$ (5, 2, 4).
$Q(3) = 2$	$P(3) = 4$	$PQ(3) = 8$

value representation.

Value of $P(7)$?

Value rep $\xrightarrow{\text{Lagrange}}$ coefficients.

evaluate.

$P(x) \cdot Q(x)$.

$(a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0)(b_d x^d + b_{d-1} x^{d-1} + \cdots + b_0)$.

$d \times d$ multiplications.

mod 15

Polynomial of degree d has at most d roots.

$x^2 - 1 = 0 \qquad x = \pm 1$.

$x^2 = 1 \pmod{15}$

$x = 1$

$x = -1 = 14$

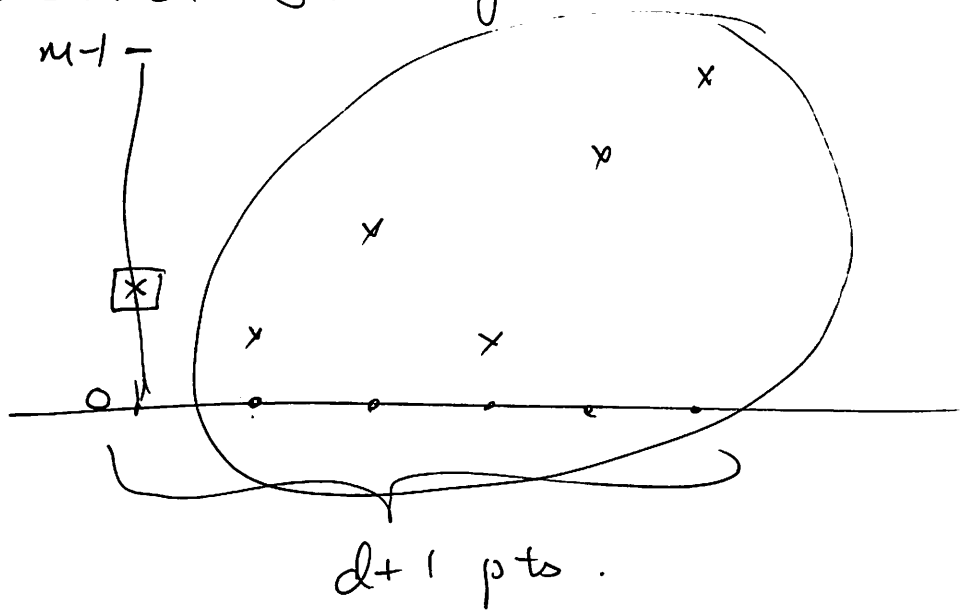
$x = 4$

$x = -4 = 11$

Midterm : Wheeler & Li Ka Shing.

Review Session: Friday 5-7 pm
2050 VLSB.

Secret Sharing:



d mod m

d+1 pts: Lagrange.

d pts: exactly m polynomials.

Secret = P(0). P random polynomial of degree d: P(0) = S.

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_1 x + a_0$$

Pick a_i's at random except $a_0 = S$.

$P(0) = S$

$P(1)$, $P(2)$, $\vdots$, $P(d)$ } at random.

Share any n people.

$P(1) \longrightarrow 1^{st}$ person

$P(2)$

$\vdots$

$P(n) \longrightarrow n^{th}$ person.

p prime.

Fermat: $\gcd(a,p)=1 \qquad a^{p-1} \equiv 1 \pmod p$

$\forall a \quad a^{k(p-1)+1} \equiv a \pmod p$

RSA: $N = P \cdot Q.$

$a^{k(p-1)(q-1)+1} \equiv a \pmod N$

$5^{782} \pmod{11} = 5^{782 \pmod{10}} \pmod{11}$

$= 5^2 \pmod{11} =$

$5^{782 \bmod 10} \pmod{22}$

2×11

$(p-1)(q-1)$

$782^2 \bmod 10.$

$2^2 \bmod 10$

11

$4.$

$5^4 \pmod{22}$

$5^{782} \pmod{22}$

$782 \bmod 10$

$2 \times 5.$

$782^{258} \bmod 10 = 782^{258 \bmod 4} \pmod{10}$

$2 \times 5 \quad (p-1)(q-1) = 4.$

$5^{782^{258}} \pmod{22}$

Since $22 = 2 \times 11$ is of form $P \cdot Q$ with P, Q prime,
we can reduce the exponent mod $(P-1)(Q-1) = 1 \times 10 = 10$
without changing the answer (by RSA).

∴ want $782^{258} \pmod{10}$.

But $10 = 2 \times 5$ is for form $P \cdot Q$ with P, Q prime.
Now $(P-1)(Q-1) = 1 \times 4 = 4$.

So can reduce exponent mod 4 without changing answer.

So can replace 258 by $258 \bmod 4 = 2$.

So exponent is $782^{258} \pmod{10} = 782^2 \pmod{10}$
$= 2^2 \pmod{10}$.
$= 4$.

So original quantity
$5^{782^{258}} \pmod{22} = 5^4 \pmod{22} = (25)^2 \bmod 22 = 3^2 = 9$.