HW05 CoderBak

I. Equivalent Polynomials

(a) $f(p) \not\equiv g(p) \pmod{p}$

(b) $x^5 \equiv x \pmod{5}$, $\forall x \in GF(5)$

$$4x^{70} + 9x^{11} + 3 \equiv 4x^{10} + 9x + 3 \pmod{11}, \forall x \in GF(11)$$

(c) By using $x^p \equiv x \pmod{p}$.

II. Secret sharing

Consider $f(x) = ax^2 + bx + c$, where c is the answer

Every TA will be given 2 points on f

Every reader will be given 1 point on f

2 TAs: 4 points.

3 readers: 3 points

1 TA + 1 reader: 3 points

1 TA x 2 readers x

III. One Point Interpolation

(a) $X_i = i$

$$\Rightarrow \begin{cases} 0^k + 0^{k-1} c_{k-1} + \cdots + c_0 = y_0 \\ 1^k + 1^{k-1} c_{k-1} + \cdots + c_0 = y_1 \\ 2^k + 2^{k-1} c_{k-1} + \cdots + c_0 = y_2 \\ \vdots \end{cases}$$

$$\begin{vmatrix} 0^{k-1} & 0^{k-2} & \cdots & 0^1 & 1 \\ & \vdots & & & \end{vmatrix} \neq 0$$

(b) $\chi_* = 100$.

$$C_0 + 100C_1 + 100^2 C_2 + \cdots + 100^{k-1} C_{k-1} + 100^k.$$

$$100\ 45\ 23\ 05\ 00\ 43\ \cdots$$

IV. Error-Correcting Codes

(a) $n/1-2$

(b) $n/1-2d$

V. Alice and Bob

(a) Every time we choose 3 points and check the rest using Python. we can calculate the result:

note: $A(a_1, b_1)$ $B(a_2, b_2)$ $C(a_3, b_3)$.

$$\frac{(x-a_2)(x-a_3)}{(a_1-a_2)(a_1-a_3)} b_1 + \frac{(x-a_1)(x-a_3)}{(a_2-a_1)(a_2-a_3)} b_2 + \cdots$$

$$\Rightarrow m_1 \equiv \frac{b_1}{(a_1-a_2)(a_1-a_3)} + \frac{b_2}{(a_2-a_1)(a_2-a_3)} + \frac{b_3}{(a_3-a_1)(a_3-a_2)}.$$

$$m_2 \equiv \frac{-(a_2+a_3)\, b_1}{(a_1-a_2)(a_1-a_3)} + \cdots$$

Result: $m_1 = m_2 = m_3 = 1$

$(3, P(3))$ is modified

$$m_3 \equiv \frac{a_2 a_3 b_1}{(a_1-a_2)(a_1-a_3)} + \cdots$$

(b) if Bob can find >1 pairs with 3 points laying on a line, he can't determin what has changed.

① (3.5) (4.0) ⇒ $y = 8x + 7$ ⇒ (2, 10)

② (3.5) (1.7) ⇒ $y = -x + 8$ ⇒ (2. 6).

③ (3.5) (0.5) ⇒ $y = 5$ ⇒ (2.5)

} ⇒ x = 5. 6. 10

(c) 10