

if $a=1$, $x^{p^a}-1 = x^p-1 = a(x-1)^p$ in F_p

if $a \geq 1$, $x^{p^a}-1 = \frac{\prod_{d|a} \Phi_d(x)}{\prod_{d|p^a} \Phi_d(x)}$

cl

$$m=0$$

$$J^p a = I + \cancel{(J-I)} p^a (J-I) + \frac{b(a-1)}{2} (J-I)^2 + \dots$$

$$p^a \equiv 0, \quad p^a = 0 \text{ at } F_p$$

$$1) \quad J^p a = I.$$

$$p^a \geq n \Rightarrow a \geq \log_p n$$

$$\min a = \lceil \log_p n \rceil$$

$$q \quad \Phi(x) = \prod_{\alpha|p} \alpha^a \Phi_d(x)$$

in part to several part

$$\{1,1,1\}, \{3,3,3\}, \{3,2,2\}, \{3,1,1,1\}, \{2,2,2\}, \{2,2,1,1\}$$

$$n_A(x) = (x-1)^4$$

are distinct.

invariant classes

invariant classes

invariant classes

$$C_B(x) = (x-1)(x-2)$$

$$(x-1)^2(x-2) = (x-1)(x-2)^2$$

or diagonalize

$\dots \in \mathcal{P}(\mathcal{A})$

$$f(x) = \prod_i f_i(x)^{k_i}$$

mod \mathcal{A}

$$f_i(x) \in \mathcal{A} \quad \forall i \in \{1, \dots, r\}$$

dep i bit 0

$$f_i(x) \in \mathcal{A}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

\oplus

$$\begin{pmatrix} 0 & 1 & 0 \\ -1 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

1^4
 2^2
 (1)

the degree of each part of $c(x)$ is bigger than

to make A and B is not similar, but $G_A(x) = G_B(x)$

$a(b) \in \mathbb{O} J(A)$, $J_{2a}(b)$ or $J_{2a}(b) \in J(B)$ $\angle A, B \in \mathbb{O}$'s equal ~~so~~ does not matter here.

J_{2a}

deg

> the remainder of ~~the~~ $J(B_1) / J_{2a}(b) = 1$, it is not true

, the remainder is \mathbb{Z}

$$J(b_1) \oplus J_3(b_1) \oplus J_3(b_2) \quad J(B) = J_6(b_1) J_3(b_2)$$

$$= \cancel{J_2(A)} J_2 \quad J_2(b_1) \oplus J_2(b_2) \oplus J_5(b_3) \quad J(B) \cong J_4(b_1) \quad J_5(b_3)$$

$$x^3 + x^2 - x + 1)$$

$$m_A(x) = m_B(x) = (x^2 + 1)^3 (x^3 + x^2 - x + 1)$$

$$(x^2 + 1)^3$$

$$\in C(x^3 + x^2 - x + 1)$$

$$B = \notin C(x^2 + 1) \oplus (C(x^3 + 1))^2 \oplus C(x^3 + x^2 - x + 1)$$

are irreducible, $A \neq B$

$$(CB) \neq$$

$$+1$$

$$\text{rank } A = \text{rank } B$$

range is rank -

$$= \text{rank } A - 3 = \text{rank } B - 3$$

$$(x) = \pi, f, i, x, k,$$

$$m_B(x)$$

$$f, f(B) = 0, \text{ while } f(A) \neq 0$$

$$f(A) = \text{rank } f(B), \text{ ~~rank~~ } m_A(x) = m_B(x)$$

$$e \oplus v_1' \oplus \dots \oplus v_0'$$

$$v_i(x) = f; a_i$$

$$C[f(x)]^{k_2} \oplus \dots \oplus C[f(x)]^{k_2'} \oplus \dots$$

$$B^{a_i-r}$$