

I&R $\int \lambda^{(p-1)} \text{ If } m \nmid (p-1), \text{ let } d := (m, p-1) \text{ then } \{\lambda : \lambda^m = 1\} = \{\lambda : \lambda^d = 1\}$

3.8

We have:

8. SQU

$$\sum_{t \in F_p} x(1-t^m) = \sum_{\alpha \in F_p} N(\alpha^m = 1) \cdot x(1-\alpha) = \sum_{\alpha \in F_p} \left(\sum_{\lambda^m=1} x(\alpha) \right) \cdot x(1-\alpha) =$$

$$= \sum_{\lambda^m=1} \sum_{\alpha \in F_p} x(\alpha) x(1-\alpha) = \sum_{\lambda^m=1} \left(\sum_{\substack{a+b=1 \\ a,b \in F_p}} x(a) x(b) \right) =$$

$$= \sum_{\lambda^m=1} J(x, \lambda)$$

Now since char ~~one~~ cyclic gp., $| \{ \lambda : \lambda^m = 1 \} | = \begin{cases} m-1 & \text{if } m \nmid (p-1) \\ d & \text{if } m \mid (p-1) \end{cases}$

$$\therefore \left| \sum x(1-t^m) \right| \leq (d-1) \cdot p^{1/2}$$

$\lambda=1$



8.15) (I think we need D+O, here.)

$$\begin{aligned}
 N - N(y^2 = x^3 + D) &= \sum_{a+b=D} N(y^2 = a) N(x^3 = b) = \\
 &= \sum_{a+b=D} \left(\sum_{i=0}^{p-1} \ell(a) \right) \left(\sum_{j=0}^{p-1} \chi(b) \right) \\
 &= \sum_{a+b=D} 1 + \rho(a) + \chi(b) + \chi^2(b) + \rho(a)\chi(b) + \rho(a)\chi^2(b) = \\
 &= p + \sum_{a=0}^{p-1} (\cancel{\rho(a) + \chi(b) + \chi^2(b)}) + \sum_{a+b=D} (\cancel{\rho(a)\chi(b)} + \cancel{\rho(a)\chi^2(b)}) \\
 &\qquad\qquad\qquad\downarrow \\
 &= p + \sum_{\substack{a+b=1 \\ a'=a_D \\ b'=-b_D}} \rho(Da') \chi(-Db') + \rho(Da') \bar{\chi}(-Db') = \\
 &\qquad\qquad\qquad\downarrow \\
 &= p + \ell(\chi(D)) \cdot \sum_{a+b=1} \rho(a) \chi(b) + \ell(\bar{\chi}(D)) \cdot \sum_{a+b=1} \rho(a) \bar{\chi}(b) \\
 &= p + \underbrace{\ell(\chi(D)) \cdot J(\rho, \chi)}_{\pi} + (\bar{\chi}(D)) \cdot J(\rho, \bar{\chi}) = \\
 &= p + \pi + \bar{\pi} \\
 &\qquad\qquad\qquad\downarrow \text{since } \rho(a) = \pm 1 \text{ or } 0, \quad \rho = \bar{\rho}
 \end{aligned}$$

Now, suppose that $\chi(2) = 1$ and $D = 1$. ($\therefore \pi = J(\chi, e)$.)

Since $p \equiv 1 \pmod{6}$, clearly $p \equiv 1 \pmod{3}$. So, Problem 8.9 tells us that $g(x^3) = p \cdot (\chi(2) \cdot J(\chi, \rho)) = p \cdot \pi$

Now, we follow the idea of hop 8.3.4:

$$g(x) \stackrel{3}{=} -1 \quad (\text{check the book at pg 96/97})$$

REMEMBER: $\omega = e^{2\pi i/3}$

$$\underset{\parallel}{PJ}(x, \ell)$$

$$\omega = \zeta_3 = e^{2\pi i/3}$$

now, since the range of x is in $\mathbb{Z}[\omega]$, and the range of ℓ is in $\{0, 1, -1\}$, $\underset{\parallel}{PJ}(x, \ell) = a + b\omega, a, b \in \mathbb{Z}$

We can repeat this whole argument with \bar{x} (as it also has order 3) and set $\underset{\parallel}{PJ}(\bar{x}, \ell) = a + b\bar{\omega}$.

$$g(\bar{x})^3$$

thus: $\underset{\parallel}{g(x)}^3 = \underset{\parallel}{g(\bar{x})}^3 = 1$ seen above

$$\begin{array}{ll} p \equiv 1 \pmod{3} & \rightarrow a + b\omega \equiv -1 \pmod{3} \\ \underset{\parallel}{PJ}(x, \ell) & a + b\bar{\omega} \equiv -1 \pmod{3} \\ \underset{\parallel}{J}(x, \ell) & \text{and } a \equiv 1 \pmod{3} \\ \underset{\parallel}{J}(\bar{x}, \ell) & \end{array}$$

subtracting, we get $3 \mid b$ (check pg 97 for some steps)

We have that $|\underset{\parallel}{J}(x, \ell)|^2 = p$ (Dual at pg 94)

$$\underset{\parallel}{a^2 - ab + b^2} = p$$

$$\therefore 4p = \underbrace{(2a-b)^2}_{A} + 3 \underbrace{b^2}_{3B \text{ as } 3 \mid b} = A^2 + 27B^2 \quad (A \text{ is unique when } A \equiv 1 \pmod{3})$$

$\sum_{n=1}^{\infty} \frac{1}{n^2} = \pi^2/6$

↳ theorem 2

now $N = p + \pi + \bar{\pi} = p + (a + b\omega) + (a + b\bar{\omega}) = p + \underbrace{2a - b}_A$

$$\text{ex: } 31 = (-2)^2 + 27 \cdot 1^2$$

$$\therefore N = 31 + (-2) = 29 \text{ points!}$$

TR
(8.26)

(a)

$$N(\gamma_f^2 + \chi^4 = 1) = \sum_{\alpha+\beta=1} N(\gamma_f^2 = \alpha) \cdot N(\chi^4 = \beta) =$$

$$= \sum_{\alpha+\beta=1} \left(\sum_{i=0}^1 \rho^i(\alpha) \right) \cdot \left(\sum_{j=0}^3 \chi^j(\beta) \right) =$$

$$= \sum_{\alpha+\beta=1} 1 + \rho(\alpha) + \chi(\beta) + \chi^2(\beta) + \chi^3(\beta) + \rho(\alpha)\chi(\beta) + \rho(\alpha)\chi^2(\beta) + \rho(\alpha)\chi^3(\beta) =$$

$$= p + J(\ell, \chi) + J(\ell, \chi^2) + J(\ell, \chi^3) =$$

$\downarrow \chi^3 = \chi^{-1} = \bar{\chi}$

$$= p + a+bi + J(\ell, \rho) + a-bi =$$

$$\begin{array}{l} \hookrightarrow \text{order } \chi=4 \\ \text{order } \ell=2 \Rightarrow \chi^2=\rho \end{array}$$

$$= p + 2a - \rho(-1) = p + 2a - (-1)^{\frac{p-1}{2}} = p + 2a - 1$$

Theo 8.1(c)

$$p \equiv 1 \pmod{4}$$

$$\text{as } \rho = \ell^{-1}$$

$$\begin{array}{c} \text{a complete residue system mod 4: } \{0, 1, 2, 3\} \\ \text{and in mod 4: } \{0, 1, 2, 3\} \end{array}$$

$$(b) \quad N(\gamma^2 = 1 - x^4) = \sum_{x \in \mathbb{F}_p} N(\gamma^2 = 1 - x^4)$$

$$= \sum_{x \in \mathbb{F}_p} \left(\underbrace{\sum_{i=0}^1 \rho(i(1-x^4))}_{1 + \rho(1-x^4)} \right) = p + \sum_{x \in \mathbb{F}_p} \rho(1-x^4)$$

(c)

From (a) and (b):

$$2\alpha - 1 = \sum_{x \in \mathbb{F}_p} \rho(1-x^4)$$

Remember:

$$\rho(z) \equiv z^{\frac{p-1}{2}} \pmod{p}$$

$$\therefore 2\alpha - 1 \equiv \sum_{x \in \mathbb{F}_p^x} (1-x^4)^{\frac{(p-1)}{2} = 2m} = 1 +$$

$$= 1 + \sum_{x \in \mathbb{F}_p^x} \left(\sum_{i=0}^{2m} \binom{2m}{i} (-1)^i x^{4i} \right) =$$

$$= 1 + \sum_{i=0}^{2m} \left[\binom{2m}{i} (-1)^i \left(\sum_{x \in \mathbb{F}_p^x} x^{4i} \right) \right]$$

Now, if $(p-1) \nmid 4i$, $\sum_{x \in \mathbb{F}_p^x} x^{4i} = 0$ (I'm pretty sure we did this, but could not find it). Set $\mathbb{F}_p^x = \langle \alpha \rangle$. Then $\sum_{x \in \mathbb{F}_p^x} x^{4i} = \sum_{j=0}^{p-2} (\alpha^j)^{4i} = \frac{\alpha^{4ip-1} - 1}{\alpha^{4i} - 1} = 0$.

(ie, $p \nmid 4i$)

If $(p-1) \mid 4i$, then $\sum_{x \in \mathbb{F}_p^x} x^{4i} = p-1 = -1$. Since the sum ranges from

① to $2m = \frac{p-1}{2}$, we have that

$$\begin{aligned}2a-1 &\equiv 1 + \sum_{i=0}^{2m} \left[\binom{2m}{i} (-1)^i \cdot \left(\sum_{x \in \mathbb{F}_p^{\times}} x^{4i} \right) \right] = -\frac{b}{2} \binom{b-1}{2} w_{b-1}^2 \\&\quad \text{since } a \text{ is a primitive root mod } p \Rightarrow b \text{ maps to an argument of } 1 \text{ mod } b \text{ in the same}\\&\quad \text{sense as } a \text{ does mod } p \Rightarrow \text{the } i\text{-th power of } b \text{ maps to the } 4i\text{-th power of } 1 \text{ mod } b \\&= 1 + \binom{2m}{0} (-1)^0 (-1) + \binom{2m}{m} (-1)^m (-1) + \binom{2m}{2m} (-1)^{2m} (-1) \\&= -(-1)^m \binom{2m}{m} - 1 \pmod{p} \\&\therefore 2a \equiv -(-1)^m \binom{2m}{m} \pmod{p}.\end{aligned}$$

Since a is a primitive root mod p , we know that $a^m \not\equiv 1 \pmod{p}$. \square

$$\begin{aligned}&\sum_{i=1}^{b-1} \binom{b}{i} w_i \frac{b}{a_{i+1} b_{i+1} - b_{i+1} a_{i+1}} \\&= \frac{b_2}{a_1 a_2} - \sum_{i=1}^{b-1} \frac{b_3}{i+1} \binom{i}{b} w_i a_{i+1} \\&\quad \left[\sum_{i=1}^{b-1} \binom{i}{b} w_i a_{i+1} b_{i+1} - \sum_{i=1}^{b-1} \binom{i}{b} w_i a_{i+1} \right] \\&= \frac{b_2}{a_1 a_2} - \sum_{i=1}^{b-1} \frac{b_3}{i+1} \binom{i}{b} w_i a_{i+1} \\&= \frac{b_2}{a_1 a_2} - \overline{w_{b-1}^2} \cdot \overline{a_{b-1}}\end{aligned}$$

$$= \overline{a_{b-1} w_{b-1}^2} = \overline{a_{b-1} w_{b-1}} + \overline{w_{b-1}^2} \cdot \overline{a_{b-1}}$$

Since $w_{b-1} \neq 0$, we have

Since $w_{b-1} \neq 0$, we can multiply both sides by w_{b-1} to get a contradiction to the fact that $w_{b-1} \neq 0$.

$$\begin{aligned}\sum_{i=1}^{b-1} \frac{b_3}{i+1} \binom{i}{b} w_i a_{i+1} &= \sum_{i=1}^{b-1} \frac{b_3}{i+1} \binom{i}{b} a_{i+1} w_i = 0 \\&\Rightarrow \sum_{i=1}^{b-1} \frac{b_3}{i+1} \binom{i}{b} w_i a_{i+1} = 0\end{aligned}$$

Since $w_{b-1} \neq 0$,

Since $w_{b-1} \neq 0$, we can multiply both sides by w_{b-1} to get a contradiction to the fact that $w_{b-1} \neq 0$.