I&K

8.8

If $m\nmid(p-1)$, let $d:=(m,p-1)$ then $\{\lambda:\lambda^m=1\}=\{\lambda:\lambda^d=1\}$.

we have:

$$\sum_{t\in\mathbb{F}_p}\chi(1-t^m)=\sum_{a\in\mathbb{F}_p}N(x^m=a)\cdot\chi(1-a)=\sum_{a\in\mathbb{F}_p}\left(\sum_{\lambda^m=\varepsilon}\lambda(a)\right)\chi(1-a)=$$

$$=\sum_{\lambda^m=\varepsilon}\sum_{a\in\mathbb{F}_p}\lambda(a)\chi(1-a)=\sum_{\lambda^m=\varepsilon}\left(\sum_{a+b=1}\chi(a)\lambda(b)\right)=$$

$$=\sum_{\lambda^m=\varepsilon}J(\chi,\lambda)$$

now since char ~~are~~ form a cyclic gp, $|\{\lambda:\lambda^m=\varepsilon\}|=\begin{cases}m & \text{if } m\mid(p-1)\\ \underset{(m,p-1)}{\underset{\shortparallel}{d}} & \text{if } m\nmid p-1\end{cases}$

$$\therefore\left|\sum\chi(1-t^m)\right|\leq(d-\underbrace{1}_{\lambda=\varepsilon})\cdot p^{1/2}$$

//

II

(8.15) (I think we need $D \neq 0$, here.)

$$N = N(y^2 = x^3 + D) = \sum_{a-b=D} N(y^2 = a)\, N(x^3 = b) =$$

$$= \sum_{a-b=D} \left(\sum_{i=0}^{1} \rho(a) \right) \left(\sum_{j=0}^{2} \chi(b) \right)$$

$$= \sum_{a-b=D} 1 + \rho(a) + \chi(b) + \chi^2(b) + \rho(a)\chi(b) + \rho(a)\chi^2(b) =$$

$$= p + \underbrace{\sum_{a=0}^{p-1} \left(\rho(a) + \chi(b) + \chi^2(b) \right)}_{0} + \sum_{a-b=D} \left(\rho(a)\chi(b) + \rho(a)\underbrace{\chi^2(b)}_{\chi^2 = \bar{\chi}} \right)$$

$$= p + \sum_{a'+b'=1} \rho(Da')\chi(-Db') + \rho(Da')\bar{\chi}(-Db') =$$

assuming that $D \neq 0$ in $\mathbb{F}_p$

$a' = a/D$

$b' = -b/D$

$$= p + \rho\chi(D) \cdot \sum_{a+b=1} \rho(a)\chi(b) + \rho \cdot \bar{\chi}(D) \sum_{a+b=1} \rho(a)\chi(b)$$

$$= p + \underbrace{\rho\,\chi(D) \cdot J(\rho, \chi)}_{\pi} + \rho\bar{\chi}(D) \cdot J(\rho, \bar{\chi}) =$$

$$= p + \pi + \bar{\pi}$$

↳ since $\rho(a) = \pm 1$ or 0, $\rho = \bar{\rho}$

now, suppose that $\chi(2) = 1$ and $D = 1$ ($\therefore \bar{\pi} = J(\chi, \rho)$)

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

now, we follow the idea of hop 8.3.4:

$$\underset{\substack{\shortparallel \\ pJ(\chi,\rho)}}{g(\chi)^3} \equiv -1$$ (check the book at pgs 96/97)

now, since the range of χ is in $\mathbb{Z}[\omega]$, and the range of ρ is in $\{0,1,-1\}$, $J(\chi,\rho) = a+b\omega$, $a,b \in \mathbb{Z}$ ($\omega = \zeta_3 = e^{2\pi i/3}$)

we can repeat this whole argument with $\bar{\chi}$ (as it also has order 3) and set $\underset{\substack{\shortparallel \\ g(\bar{\chi})^3}}{pJ(\bar{\chi},\rho)} = a+b\bar{\omega}$

thus: $g(\chi)^3 \equiv g(\bar{\chi})^3 \equiv -1$ (seen above) $\Rightarrow$ $a+b\omega \equiv -1 \pmod 3$

$\quad\ \ pJ(\chi,\rho) \quad pJ(\bar{\chi},\rho) \qquad a+b\bar{\omega} \equiv -1 \pmod 3$

$\quad\ \ J(\chi,\rho) \quad\ \ J(\bar{\chi},\rho)$ ($p \equiv 1 \pmod 3$)

subtracting, we get $3 \mid b$ and $a \equiv 1 \pmod 3$ (check pg 97 for some steps)

we have that $|\overbrace{J(\chi,\rho)}^{\pi}|^2 = p$ (check at pg 94)

$$|J(\chi,\rho)|^2 = a^2 - ab + b^2$$

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

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

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

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

(8.26)

(a)

$$N(y^2+x^4=1)=\sum_{a+b=1} N(y^2=a)\cdot N(x^4=b)=$$

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

$$=\sum_{a+b=1} 1+\rho(a)+\chi(b)+\chi^2(b)+\chi^3(b)+\rho(a)\chi(b)+\rho(a)\chi^2(b)+\rho(a)\chi^3(b)=$$

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

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

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

$\hookrightarrow$ order $\chi=4$, order $\rho=2$ $\Rightarrow \chi^2=\rho$

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

theo 8.1(c) as $\rho=\rho^{-1}$

$p\equiv 1 \pmod 4$

(b) now x seen as a fixed element.

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

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

(c)

From (a) and (b):

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

Remember:

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

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

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

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

now, if $(p-1)\nmid 4i$, $\sum_{x\in\mathbb{F}_p^\times} x^{4i}=0$ (I'm pretty sure we did this, but could not find it). Set $\mathbb{F}_p^\times=\langle\alpha\rangle$ then $\sum_{x\in\mathbb{F}_p^\times} x^{4i} = \sum_{j=0}^{p-2}(\alpha^j)^{4i} \underset{\substack{\downarrow\\ \text{if } \alpha^{4i}\neq 1\\ (\text{ie},\ p-1\nmid 4i)}}{=} \frac{(\alpha^{4i})^{p-1}-1}{\alpha^{4i}-1}=0.$

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

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

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

$$= 1 + \binom{2m}{0}(-1)^0(-1) + \binom{2m}{m}(-1)^m \cdot (-1) + \binom{2m}{2m}(-1)^{2m} \cdot (-1)$$

$$= -(-1)^m \binom{2m}{m} - 1 \pmod{p}$$

$$\therefore \; 2a \equiv -(-1)^m \binom{2m}{m} \pmod{p}.$$