

Q1a: From previous results, we know that  $\Phi_8(x) = x^4 + 1$ . By assumption  $s(x)$  is a factor of  $\Phi_8(x)$ , and  $\xi$  is a root of  $s(x)$  it must also be a root of  $\Phi_8(x)$ . Hence  $\xi^4 + 1 = 0$ . Therefore  $\xi^4 = -1$ , and so  $\xi^8 = 1$ . Therefore  $\xi$  is nonzero. Hence by Lagrange's theorem, the order of the subgroup generated by  $\xi$  must divide 8. Suppose the order is not 8. Then we have that if  $m = \text{ord}(\xi)$ , then

$$\xi^k = \xi^{k \frac{4}{m}} + 1 = 1 + 1 = 0$$

Hence  $2 = 0 \pmod p$ , and so  $p$  is 2. This is a contradiction, since we assume that  $p$  is odd. Therefore, the order of  $\xi$  is 8.

1b: Let  $\tau = \xi + \xi^{-1}$ . Since  $\xi^4 + 1 = 0$ , we have that  $\xi^{-2}(\xi^4 + 1) = 0$  and so  $\xi^2 + \xi^{-2} = 0$ . Therefore,

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

Which implies that  $\tau^2 = 2 \cdot 1 = 2$

1c: By Euler's Criterion, we have that

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = \tau^{2 \frac{p-1}{2}} = \tau^{p-1}$$

Where the second equality follows from 1b.

1d: We will use the result that if  $p \equiv \pm 1 \pmod 8$ ,  $\tau^p = \tau$ , but that we can discard the case when  $p \equiv \pm 3 \pmod 8$  in our proof. First if  $p \equiv \pm 1 \pmod 8$ , then

$$\tau^p = \xi^{8^k} \xi^{\pm 1} + \xi^{8^k} \xi^{\pm 1} = \xi^{\pm 1} + \xi^{\pm 1} = \tau$$

Now if  $p \equiv \pm 3 \pmod 8$ , then

$$\tau^p = \xi^{8^k} \xi^{\pm 3} + \xi^{8^k} \xi^{\pm 3} = \xi^{\pm 3} + \xi^{\pm 3} = \xi^3 + \xi^{-3} = \xi = \xi^{-1}$$

Thus if  $\tau^p = \tau$ ,

$$\xi^6 + 1 = \xi^4 + \xi^2 \implies \xi^4(\xi^2) + 1 = -1 + \xi^2$$

Which implies that  $2\xi^2 = 2$ , which can not happen since the order is 8. We now prove the result.

$\implies$

Suppose that  $p \equiv \pm 1 \pmod 8$ . Then we have that  $p = 8k + 1$ , and so  $p^2 - 1 = (8k + 1)^2 - 1 = 64k^2 + 16k$ . It is clear that  $\frac{p^2-1}{8} = 8k^2 + 2k$  which is 0 mod 2.

$\Longleftarrow$

Suppose that  $\frac{p^2-1}{8} \equiv 0 \pmod 2$ . Therefore  $16 \mid p^2 - 1 = (p-1)(p+1)$ . If we have that  $4 \mid p-1$  and  $4 \mid p+1$ . Hence  $p \equiv 3 \pmod 4$ . Which can not be the case. Therefore  $8 \mid p+1$  or  $8 \mid p-1$ , because  $2 \mid (p+1)$  and so  $p \equiv \pm 1 \pmod 8$ .

Q1e: By  $c, d$ , we have that  $\left(\frac{2}{p}\right) = 1 \iff \frac{p^2-1}{8} \equiv 0 \pmod 2$ , or  $\left(\frac{2}{p}\right) \equiv -1 \pmod 2 \equiv \frac{p^2-1}{8} \equiv 1 \pmod 2$ . Thus,  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$