Assignment 5

Problem 1 (2.35)

Calculate the square roots of 1 modulo 4, 8, and 16.

1) $x^2 \equiv 1 \pmod 4$ find x

$0^2 \equiv 0 \bmod 4$, $1^2 \equiv 1 \pmod 4$, $2^2 \equiv 4 \equiv 0 \bmod 4$, $3^2 \equiv 9 \equiv 1 \pmod 4$

$\therefore \{1, 3\}$

2) $x^2 \equiv 1 \pmod 8$ find x

$0^2 \equiv 0 \pmod 8$, $1^2 \equiv 1 \pmod 8$, $2^2 \equiv 4 \pmod 8$, $3^2 \equiv 9 \equiv 1 \pmod 8$, $4^2 \equiv 16 \equiv 0 \pmod 8$,
$5^2 \equiv 25 \equiv 1 \pmod 8$, $6^2 \equiv 36 \equiv 4 \pmod 8$, $7^2 \equiv 49 \equiv 1 \pmod 8$

$\therefore \{1, 3, 5, 7\}$

3) $x^2 \equiv 1 \pmod{16}$, find x

$0^2 \equiv 0 \pmod{16}$, $1^2 \equiv 1 \pmod{16}$, $2^2 \equiv 4 \pmod{16}$, $3^2 \equiv 9 \pmod{16}$, $4^2 \equiv 16 \equiv 0 \pmod{16}$,
$5^2 \equiv 25 \equiv 9 \pmod{16}$, $6^2 \equiv 36 \equiv 4 \pmod{16}$, $7^2 \equiv 49 \equiv 1 \pmod{16}$, $8^2 \equiv 64 \equiv 0 \pmod{16}$,
$9^2 \equiv 81 \equiv 1 \pmod{16}$, $10^2 \equiv 100 \equiv 4 \pmod{16}$, $11^2 \equiv 121 \equiv 9 \pmod{16}$, $12^2 \equiv 144 \equiv 0 \pmod{16}$,
$13^2 \equiv 169 \equiv 9 \pmod{16}$, $14^2 \equiv 196 \equiv 4 \pmod{16}$, $15^2 \equiv 225 \equiv 1 \pmod{16}$

$\therefore \{1, 7, 9, 15\}$

$2! \quad 2\times 1 = 2$
4×1

$4! \quad 4\times 3\times 2\times 1 \quad 24$
$6 \qquad b = a^{\frac{p-1}{4}}$

Problem 2 (2.37)

Let p be a prime with $p \equiv 1 \pmod 4$, and $b := ((p-1)/2)!$, show that $b^2 \equiv -1 \pmod p$

When $p \equiv 1 \bmod 4$ and odd prime number, Then $(p-1)/2$ is a even number.
And from the question $b := ((p-1)/2)!$ and we need to show $b^2 \equiv -1 \pmod p$
In order to be $B^2 \equiv -1 \pmod p$, by Euler's Criterion we need to show that $B^2 \equiv -1$

we also know from the question $p \equiv 1 \bmod 4$ so $p \equiv 4t+1$ for $t \in \mathbb{Z}$

from Book wilson's theory " Let p be an odd prive. Then $\prod_{\beta \in \mathbb{Z}_p^*} \beta = -1$
Then $(p-1)! \equiv -1 \pmod p$."

So wilson's theorem says $1\times 2\times 3\times \cdots p-1 \equiv -1 \pmod p$. In wilson's theoem expect $p-1$, there is an each inverse pair so $1\times p-1 \times 2\times p-2 \times 3\times p-3 \times \cdots \lfloor \frac{p}{2} \rfloor \times \frac{p}{2}+1$
and it would cancel out expect $p-1$ since $p = 4t+1$ we can put it as.

$(4t-1)! = 1\times 2\times 3\times \cdots 2t \times 2t+1 \cdots \times -3 \times -2 \times -1$ so $1\times -1 \times 2\times -2 \times \cdots 2t\times -2t$ so this is
$(p-2t)$ same as $(4t-1)$
$2t$ same as $-2t$

same as $\prod_{i=1}^{2t} i^2 \equiv -1 \bmod p$ so $(2t!)^2 \equiv -1 \bmod p$ And $2t = \frac{p-1}{2}$

so $\left(\frac{p-1}{2}!\right)^2 \equiv -1 \bmod p$

Problem 3 (2.40)

Show that if p is an odd prime, with $p \equiv 3 \pmod 4$, then $(\mathbb{Z}_p^*)^4 = (\mathbb{Z}_p^*)^2$. More generally, Show that if n is an odd positive integer, where $p \equiv 3 \pmod 4$ for each prime $p | n$, then $(\mathbb{Z}_n^*)^4 = (\mathbb{Z}_n^*)^2$.

when p is an odd prime with $p \equiv 3 \pmod 4$. that means $\left(\frac{p-1}{2}\right)$ is an odd integer. so $(-1)^{(p-1)/2} = -1$ so -1 is not a quadratic residue modulo p

we need to show $(\mathbb{Z}_p^*)^4 = (\mathbb{Z}_p^*)^2$ so we need to show $(\mathbb{Z}_p)^4 \subseteq (\mathbb{Z}_p^*)^2$ and $(\mathbb{Z}_p^*)^4 \supseteq (\mathbb{Z}_p^*)^2$

First let's show $(\mathbb{Z}_p^*)^4 \subseteq (\mathbb{Z}_p^*)^2$.

let's say $\alpha \in (\mathbb{Z}_p^*)^4$, so from $(\mathbb{Z}_p^*)^4 \subseteq (\mathbb{Z}_p^*)^2$, for some $\beta \in (\mathbb{Z}_p)$, $\beta^4 \equiv \alpha \pmod p$
we also need to show $r^2 \equiv \alpha \pmod p$, for some $r \in (\mathbb{Z}_p)$ similar to β.
From the following observation $\beta^4 \equiv \alpha \pmod p \Rightarrow 1 \times \beta^4 \equiv \alpha \pmod p \Rightarrow$ (Since $\beta^{\varphi(p)} \equiv 1 \bmod p$) $\beta^{\varphi(p)} \cdot \beta^4 \equiv \alpha \pmod p \Rightarrow \beta^{p-1} \cdot \beta^4 \equiv \alpha \pmod p$.

we know $p = 4t+3$ for some $t \in \mathbb{Z}$, Substitute $4t+3$ to p in above equation
$\beta^{4t+2} \cdot \beta^4 \equiv \alpha \pmod p \Rightarrow \beta^{4t+6} \equiv \alpha \pmod p \Rightarrow \beta^{2(2t+3)} \equiv \alpha \pmod p \equiv (\beta^{2t+3})^2 \equiv \alpha \pmod p$
$\Rightarrow r^2 \equiv \alpha \pmod p$ when $r \equiv \beta^{2t+3}$ r and β are both in $\mathbb{Z}_p$, so $(\mathbb{Z}_p^*)^4 \subseteq (\mathbb{Z}_p^*)^2$

For $(\mathbb{Z}_p^*)^2 \subseteq (\mathbb{Z}_p^*)^4$
Simlarly let's say $\alpha \in (\mathbb{Z}_p^*)^2$. so from $(\mathbb{Z}_p^*)^4 \subseteq (\mathbb{Z}_p^*)^2$. for some $\beta \in (\mathbb{Z}_p)$ $\beta^2 \equiv \alpha \pmod p$
There is also $r^4 \equiv \alpha \pmod p$, for some $r \in (\mathbb{Z}_p)$ similar to β
from the following observation. $\beta^2 \equiv \alpha \pmod p \Rightarrow 1 \; \beta^2 \equiv \beta^{\varphi(p)} \cdot \beta^2 \equiv \beta^{p-1} \cdot \beta^2 \equiv \beta^{4t+2} \cdot \beta^2 \equiv \beta^{4t+4} \equiv \beta^{4(t+1)} \equiv \alpha \pmod p$. so when $r \equiv \beta^{t+1}$ this statement is true but r and $\beta \in \mathbb{Z}_p$ so this condition true

More generally $(\mathbb{Z}_n^*)^4 = (\mathbb{Z}_n^*)^2$ if n is an odd positive integer, when $p \equiv 3 \pmod 4$ for each prime $p|n$

This prove also need two parts $(\mathbb{Z}_n^*)^4 \subseteq (\mathbb{Z}_n^*)^2$ and $(\mathbb{Z}_n^*)^2 \subseteq (\mathbb{Z}_n^*)^4$

For $(\mathbb{Z}_n^*)^4 \subseteq (\mathbb{Z}_n^*)^2$

n is an arbitrary integer now. $n = p_1^{e_1} \times p_2^{e_2} \times p_3^{e_3} \cdots$ and p divides n. which means p is one of prime factor of n.

There is $\alpha \in (\mathbb{Z}_n^*)^4$ then for some $\beta \in (\mathbb{Z}_n)$ $\beta^4 \equiv \alpha \pmod n$, we need to show $r^2 \equiv \alpha \pmod n$ for some $r \in \mathbb{Z}_n$.

$\beta^4 \equiv \alpha \pmod n \Rightarrow 1 \times \beta^4 \equiv \alpha \pmod n \Rightarrow \beta^{\varphi(n)} \cdot \beta^4 \equiv \alpha \pmod n$.

From the theorem 2.10 and 2.11 $n = p_1^{e_1} \cdots p_r^{e_r}$, $\varphi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}(p_i - 1)$
$= n \prod_{i=1}^{r} (1 - 1/p_i)$. But we can say simplified n as p^e which is one of the smallest p factor. $\varphi(p^e) = p^{e-1}(p-1)$.

$\Rightarrow \beta^{p^{e-1}(p-1)} \times \beta^4 \equiv a \bmod n) \Rightarrow$ we can substitute $4t+3$ into p. $\Rightarrow \beta^{(4t+3)^{e-1}(4t+2)} \beta^4 \equiv a \bmod n)$
$\Rightarrow ((4t+3)^{e-1}(4t+2))^4$ is also has a squre root. so $r^2 \equiv a \pmod n$ for some β's power.

For $(\mathbb{Z}_n^*)^2 \subseteq (\mathbb{Z}_n^*)^4$ has the same approach as above. so prove is done.