In last class I proved the following theorem:

Thm 5.44: Let $U(\mathbb{Z}/m)$ be the multiplicative group,

$$U(\mathbb{Z}/_2m) = \{ [a] \in \mathbb{Z}_{2m} : a \text{ is odd} \}$$

If $m \geq 3$, then

$$U(\mathbb{Z}/_2m) = \langle [-1], [5] \rangle \cong \mathbb{Z}/_2 \times \mathbb{Z}/_{2^{m-2}}$$

Here, $\mathbb{Z}/_2 \times \mathbb{Z}/_{2^{m-2}}$ represents the internal direct product of two additive groups. (They are cyclic too.)

$$\mathbb{Z}/_2 \times \mathbb{Z}/_{2^{m-2}} = \{ \mathbb{Z}/_2 + \mathbb{Z}/_{2^{m-2}} : \mathbb{Z}/_2 \cap \mathbb{Z}/_{2^{m-2}} = \phi \}$$

$$= \{ x+y \mid x \in \mathbb{Z}/_2, y \in \mathbb{Z}/_{2^{m-2}} \text{ and } \mathbb{Z}/_2 \cap \mathbb{Z}/_{2^{m-2}} = \phi \}$$

Observation: No. of elements of order 2 in $U(\mathbb{Z}/_2m)$ are exactly 3.

Proof: As $U(\mathbb{Z}/_2m) \cong \mathbb{Z}/_2 \times \mathbb{Z}/_{2^{m-2}} \cong \mathbb{Z}/_2 \oplus \mathbb{Z}/_{2^{m-2}}$

Therefore, No. of elements of order 2 in $U(\mathbb{Z}/_2m)$ is same as the no. of elts of order 2 in $\mathbb{Z}/_2 \oplus \mathbb{Z}/_{2^{m-2}}$

Now we know that,

$$|(g_1, g_2)| = \text{lcm}(|g_1|, |g_2|), \text{ where } (g_1, g_2) \in \mathbb{Z}/_2 \oplus \mathbb{Z}/_{2^{m-2}}$$

As we are only interested in elements of order 2.

$|(g_1, g_2)| = 2$

$\Rightarrow$ $\text{lcm}(|g_1|, |g_2|) = 2$

This means that there are three possibilities, which are as follows,

(i) $|g_1| = 1$, $|g_2| = 2$

(ii) $|g_1| = 2$, $|g_2| = 1$

(iii) $|g_1| = 2$, $|g_2| = 2$

As we already know that $U(2^m)$ has an element of order 2 i.e. (-1), so we only need to find ~~one~~ two more elements. ⇒ on next page

---

~~For~~ ~~From~~ (i) & (iii) you see that

$|g_2| = 2$ and $g_2 \in 2^{m-2}$ (Assumption)

Now 2^{m-2} is cyclic and we know that no. of elements of order a in a cyclic group is $\phi(a)$.

Therefore,

no. of elts. of order 2 = $\phi(2) = 1$

~~Proof will continue on next page.~~

Observa that

$$(2^{m-1})^2 + 2^m = 2^{2m-2} + 2^m = 2^m 2^{m-2} + 2^m$$

$$= 2^m (1 + 2^{m-2}) \equiv 0 \pmod{2^m}$$

Adding 1 both sides,

$$\Rightarrow \quad 1 + (2^{m-1})^2 + 2 \cdot 2^{m-1} \equiv 1 \pmod{2^m}$$

$$\Rightarrow \quad (1 + 2^{m-1})^2 \equiv 1 \pmod{2^m}$$

This gives us two more elements of order 2 in $U(\mathbb{Z}/2^m)$ and they are

$\pm 1 + 2^{m-1}$ { I am not writing $\pm 2^{m-1}$ because they are same modulo 2^m i.e. ~~$2^{m-1} \equiv 2^{m-1} \pmod{2^m}$~~ $2^{m-1} \equiv -2^{m-1} \pmod{2^m}$

Corollary 5.45: Let G be a group containing elements x and y such that x has order 2^m (where $m \geq 3$), $y^2 = x^{2^r}$, and $yxy^{-1} = x^t$. Then

$$t = \pm 1 \quad \text{and} \quad t = \pm 1 + 2^{m-1}$$

In the latter case, G contains at least two involutions.

Defn: An element of a group is an involution if it is of order 2.

Proof: Since $y^2 = x^{2^r}$ commutes with x, we have

~~$x = y^2$~~

$$xy^2 = y^2x \Rightarrow x = y^2xy^{-2}$$

or $x = yyxy^{-1}y^{-1} = yx^ty^{-1} = x^{t^2}$ (given in the theorem)

$\Rightarrow x^{t^2-1} = 1$

as x has order 2^m; this means that

$t^2 \equiv 1 \pmod{2^m}$ {which is same as saying that $2^m \mid (t^2-1)$}

If we now consider the group of ~~unit~~ units of $\mathbb{Z}/2^m$ namely $U(\mathbb{Z}/2^m)$ the t can be viewed

as an element of $U(2^m)$ and not just any element, it is an element ~~whose order~~ which is identity or ~~an element~~ whose order is 2.

~~For~~ From our observation earlier we know there are exactly three possibilities for order 2 element and they are:

$$-1, \quad \pm 1 + 2^{m-1}$$

Therefore,

$$t = \pm 1 \quad \text{or} \quad t = \pm 1 + 2^{m-1}.$$

This completes half the proof.

Next we have to show that G contains at least two involutions. This means we have to find 3 elts. in G of order 2.

Notice that,

~~$(x^{m-1})^2 = x^{2m-2} = x^m \cdot x^{m-2} \equiv 0 \pmod{2^m}$~~

$$(x^{2^{m-1}})^2 = x^{2^{m-1} \cdot 2} = x^{2^m} = 1 \quad (\text{as } x \text{ has order } 2^m).$$

This implies that,

$$O(x^{2^{m-1}}) = 2, \quad (\text{because 2 is a prime number})$$

Therefore $x^{2^{m-1}}$ is an involution in G.

Suppose $t = 1 + 2^{m-1}$. For any integer k (remember this),

$$(x^k y)^2 = x^k (y x^k y^{-1}) y^2 = x^k \cdot x^{kt} x^{2^r}$$ {using the given conditions

$$\Rightarrow (x^k y)^2 = x^{k+kt+2^r} = x^{2s}$$

where, $2s = k + kt + 2^r = k(1+t) + 2^r = k(2+2^{m-1}) + 2^r$

$$\Rightarrow s = k(1+2^{m-2}) + 2^{r-1}$$

Since $m \geq 3$, $1 + 2^{m-2}$ is odd, and considering the fact that G has elements of order 2^{m-1} we conclude that the congruence

$$s = k(1+2^{m-2}) + 2^{r-1} \equiv 0 \pmod{2^{m-1}} \quad \ldots (i)$$

can be solved for some k.

For this choice of k,

$$(x^k y)^2 = x^{2s}$$

using (i) we have,

$$s = a \cdot 2^{m-1}$$

$$2s = a\, 2^m$$

$$\Rightarrow (x^k y)^2 = x^{2s} = x^{a 2^m} = (x^{2^m})^a = 1$$

$(\because O(x) = 2^m)$

Hence, $x^k y$ is the second involution.

Sp z, $t = -1 + 2^{m-1}$. As above for any integer k,

$$(x^k y)^2 = x^{k+k+2^r} = x^{k2^{m-1}+2^r}$$

Now,

$$yx^{2^r}y^{-1} = (yxy^{-1})^{2^r} = x^{-1+2^{m-1}}(xt)^{2^r}$$

as $t = -1 + 2^{m-1}$ so,

$$(xt)^{2^r} = (x^{-1+2^{m-1}})^{2^r} = x^{-2^r + 2^{m+r-1}} = x^{-2^r}.(x^{2^m})^{2^{r-1}}$$

$$= x^{-2^r} \quad (\because O(x) = 2^m)$$

Therefore,

$$yx^{2^r}y^{-1} = x^{-2^r}.$$

~~because $r \geq 1$ implies~~

The above equation implies that,

$$1 = (yx^{2^r}y^{-1})x^{2^r} \quad \text{(operating } x^{2^r} \text{ from right)}$$

as $y^2 = x^{2^r}$, we have

$$1 = yy^2y^{-1}y^2 = y^4$$

This gives us the third involution y^2.

This completes our proof as we have shown that there are three involutions implying that there would be atleast two.