Lemma: Let u be an odd integer and $e \geqslant 3$, then

$$u^{2^{e-2}} \equiv 1 \pmod{2^e}$$

Remark: Hence $\text{ord}_{2^e}(u) \leqslant 2^{e-2} < 2^{e-1} = \phi(2^e)$ and u cannot be a primitive root.

Proof: By induction on e

Base case $e = 3$: $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$

Assume $u^{2^{e-2}} \equiv 1 \pmod{2^e}$, i.e $u^{2^{e-2}} = k \cdot 2^e + 1$.

Then,

$$u^{2^{e-1}} = (e^{2^{e-2}})^2 = (k \cdot 2^e + 1)^2$$

$$= k^2 \cdot 2^{2e} + 2 \cdot k \cdot 2^e + 1$$

$$\equiv 0 + 0 + 1$$

$$\equiv 1 \pmod{2^{e+1}}. \quad \blacksquare$$

2 behaves very different than odd primes p. We should investigate this further.

Is there a unit u such that $\text{ord}_{2^n}(u) = 2^{n-2}$? $(n \geqslant 3)$

Theorem: $\text{ord}_{2^n}(5) = 2^{n-2}$

Proof: We already know $\text{ord}_{2^n}(5) \mid \phi(n) = 2^{n-1}$.

To prove $\text{ord}_{2^n}(5) = 2^{n-2}$, we need

1. $5^{2^{n-2}} \equiv 1 \pmod{2^n}$ – already proved in lemma
2. $5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$

Then, $\text{ord}_{2^n}(5) \mid 2^{n-2}$ and $\text{ord}_{2^n}(5) \nmid 2^{n-3}$ gives $\text{ord}_{2^n}(5) = 2^{n-2}$

$$
\begin{aligned}
5^{2^{n-3}} - 1 &= (5^{2^{n-4}} + 1)(5^{2^{n-4}} - 1) \\
&= (5^{2^{n-4}} + 1)(5^{2^{n-5}} + 1)(5^{2^{n-5}} - 1) \\
&\vdots \\
&= (5^{2^{n-4}} + 1)(5^{2^{n-5}} + 1)(5^{2^{n-6}} + 1) \ldots (5^2+1)(5+1)(5-1)
\end{aligned}
$$

Each factor above is $2 \pmod 4$, except $5-1$.

Therefore, the power of 2 contained in $5^{2^{n-3}} - 1$ is $\underbrace{1 + 1 + 1 + \ldots + 1}_{n-3 \text{ times}} + 2 = n-1$, i.e.

$2^{n-1} \,\|\, 5^{2^{n-3}} - 1 \Rightarrow 5^{2^{n-3}} \not\equiv 1 \pmod{2^n}$. ∎

5 generates 2^{n-2} units of $\mathbb{Z}_{2^n}$ (half of them),
so the units $\mathbb{Z}_{2^n}$ forms "almost cyclic" group

Examples: (1) $n = 4$

units of $\mathbb{Z}_{16}$: 1, 3, 5, 7, 9, 11, 13, 15

$1 \to 5^4$, $5 \to 5^1$, $9 \to 5^2$, $13 \to 5^3$

(2) $n = 5$

units of $\mathbb{Z}_{32}$: 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31

$1 \to 5^8$, $5 \to 5^1$, $9 \to 5^6$, $13 \to 5^7$, $17 \to 5^4$, $21 \to 5^5$, $25 \to 5^2$, $29 \to 5^3$

Observation: $u, -u \pmod{2^n}$: one of them is generated by 5 while the other is not
In particular, $-1 \pmod{2^n}$ is not generated by 5

Theorem: Units of $\mathbb{Z}_{2^n}$ can be generated by two units : 5 and -1. In other words,

$$\text{units of } \mathbb{Z}_{2^n} \equiv \{\pm 5^k : 1 \leq k \leq 2^{n-2}\}$$

Proof: There are $\phi(2^n) = 2^{n-1}$ units in $\mathbb{Z}_{2^n}$.

Clearly all the 2^{n-1} numbers in $\{\pm 5^k : 1 \leq k \leq 2^{n-2}\}$

are all units and we just need to show that they are all distinct.

Want to show

- $5^k \not\equiv 5^\ell \pmod{2^n}$ for $1 \leqslant k < \ell \leqslant 2^{n-2}$:

This is equivalent to $5^{\ell-k} \not\equiv 1 \pmod{2^n}$ which is true because $1 \leqslant \ell - k \leqslant 2^{n-2} - 1$ and $\operatorname{ord}_{2^n}(5) = 2^{n-2}$

- $-5^k \not\equiv -5^\ell \pmod{2^n}$ for $1 \leqslant k < \ell \leqslant 2^{n-2}$

Equivalent to the previous case.

- $5^k \equiv -5^\ell \pmod{2^n}$ for $1 \leqslant k < \ell \leqslant 2^{n-2}$

This is equivalent to $5^{\ell-k} \not\equiv -1 \pmod{2^n}$

which is true because $5^{\ell-k} \not\equiv -1 \pmod{4}$

- $5^k \equiv -5^\ell \pmod{2^n}$ for $1 \leqslant \ell < k \leqslant 2^{n-2}$

This is equivalent to $5^{k-\ell} \not\equiv -1 \pmod{2^n}$

which is true because $5^{k-\ell} \not\equiv -1 \pmod{4}$. ■