We want to show the following:

1 Theorem. *Let $n \in \mathbb{N}$, $n \geq 3$ and $N = 2^n$. Let $x \in \mathbb{Z}$ be odd (i.e. $x \in \mathbb{Z}_N^\times$), then*

$$x \text{ is a square modulo } N \iff x \equiv 1 \mod 8$$

Proof. We follow Gauss, Disquisitiones Arithmeticae, Art. 103 (see also "Arithmetische Untersuchungen", translated by H.Maser for a german translation, available at google-books).

Put

$$A := \{x \mid x \in \mathbb{Z}, 0 \leq x < 2^n, x \equiv 1 \mod 8\}$$

and

$$B := \{x^2 \mid x \in \mathbb{Z}, 0 \leq x < 2^{n-2}\}$$

We claim that $A = B$.

"$\supset$": Let $y = x^2 \in B$, i.e. in particular $y \equiv x^2 \mod 2^n$. Since $n \geq 3$, it makes sense to reduce this equation modulo 8. Remark that in $\mathbb{Z}_8$, we have $1^2 \equiv 1, 3^2 \equiv 9 \equiv 1, 5^2 \equiv 24 + 1 \equiv 1, 7^2 \equiv 48 + 1 \equiv 1$ and since x is odd, it is congruent to either $1, 3, 5$ or 7 modulo 8, hence, $y \equiv x^2 \equiv 1 \mod 8$.

"$\subset$": Let $x, y \in \mathbb{Z}$ be odd, $0 \leq y < x < 2^{n-2}$, then we claim that $x^2 \not\equiv y^2 \mod 2^n$. Assume for a moment that $x^2 \equiv y^2 \mod 2^n$, then $2^n \Big| x^2 - y^2 = (x - y)(x + y)$. It cannot be true that $4 \Big| (x - y)$ and $4 \Big| (x + y)$ as then, $4 \Big| (x + y) + (x - y) = 2x$ so that $2 \Big| x$ in contradiction to the assumption that x is odd. Hence, one of the following cases must occur: $2^n \Big| x - y$ or $2^n \Big| x + y$ or $2 \Big| (x - y)$ and $2^{n-1} \Big| (x + y)$ or $2 \Big| (x + y)$ and $2^{n-1} \Big| (x - y)$. In any case, 2^{n-1} either divides $(x + y)$ or $(x - y)$. Both cases lead to a contradiction: if $2^n \Big| x - y$ then in particular $2^{n-1} \leq x - y \leq x < 2^{n-2}$. If $2^{n-1} \Big| x + y$ then $2^{n-1} \leq x + y < 2^{n-2} + 2^{n-2} = 22^{n-2} = 2^{n-1}$. Consequently, the map $\{x \in \mathbb{Z} \mid x \text{ odd and } 0 \leq x < 2^{n-2}\} \mapsto \mathbb{Z}_{2^n}, \quad x \mapsto x^2 \mod 2^n$ is injective. There are 2^{n-2} numbers x with $0 \leq x < 2^{n-2}$. Every second of them is odd so that there are $2^{n-2}/2 = 2^{n-3}$ different odd numbers x in the range $0 \leq x < 2^{n-2}$. By the above, each of them gives rise to a new square $x^2 \mod 2^n$ so that we have shown $|B| \geq 2^{n-3}$. We have seen above that $B \subset A$ so in order to show $A = B$, it now suffices to show that $|A| \leq 2^{n-3}$. There are precisely 2^n numbers x such that $0 \leq x < 2^n$. Every eighth of them is congruent to 1 modulo 8 so that there are at most $2^n/8 = 2^{n-3}$ numbers in the set A. □