Q04a Let n be a positive integer and let a be an integer, to begin we will take the contrapositive of the starting statement, we will thus get that:

$$\text{if a is odd} \implies (a^2)^{n-1} \equiv 1 \pmod{2^n}$$

We can prove this using induction;

Base Case: n = 1: Subsituting n for 1 into our starting equation we get:

$$\begin{aligned}(a^2)^{n-1} &\equiv 1 \pmod{2^n}\\(a^2)^{1-1} &\equiv 1 \pmod{2^1}\\a^0 &\equiv 1 \pmod{2}\\1 &\equiv 1 \pmod{2}\end{aligned}$$

Thus proving the base case or when n is 1.

Inductive Hypothesis: Let a k exist such that $k \geq 1$, we will also assume that any $(a^2)^{k-1} \equiv 1 \pmod{2^k}$. To start we will need to prove that $(a^2)^k \equiv 1 \pmod{2^{k+1}}$.

$$(a^2)^k \equiv (a^2)^{k-1}(a^2)$$

Note from out hypothesis that:

$$(a^2)^{k-1} \equiv 1 \pmod{2^k}$$

Which is the same thing as for some integer s:

$$(a^2)^{k-1} \equiv 1 + s \cdot 2^k$$

Thus plugging this in we get that:

$$\begin{aligned}(a^2)^k &\equiv (a^2)^{k-1}(a^2)\\&\equiv (1 + s \cdot 2^k)(a^2)\end{aligned}$$

We know that since a is odd that means for some t,a^2 can be expressed as:

$$a^2 = 1 + t \cdot 2$$

Thus our equation becomes

$$\begin{aligned}(1 + s \cdot 2^k)(a^2) &\equiv (1 + s \cdot 2^k)(1 + t \cdot 2)\\&\equiv 1 + t \cdot 2 + s \cdot 2^k + s \cdot 2^k \cdot t \cdot 2\end{aligned}$$

Let c = b + t, we thus get:

$$\begin{aligned} 1 + t \cdot 2 + s \cdot 2^k + s \cdot 2^k \cdot t \cdot 2 &\equiv 1 + 2 \cdot c \cdot 2^k + s \cdot 2^k \cdot t \cdot 2 \\ &\equiv 1 + c \cdot 2^{k+1} + s \cdot 2^{k+1} \cdot t \end{aligned}$$

Thus applying mod we get that:

$$\begin{aligned} (a^2)^k &\equiv 1 + c \cdot 2^{k+1} + s \cdot 2^{k+1} \cdot t \\ &\equiv 1 + c \cdot 2^{k+1} + s \cdot 2^{k+1} \cdot t \mod 2^{k+1} \\ &\equiv 1 + c \cdot 0 + s \cdot 0 \cdot t \mod 2^{k+1} \\ &\equiv 1 \mod 2^{k+1} \end{aligned}$$

Since the hypothesis is now correctly shown the induction is complete and thus we have proved the statement by contrapositive and induction/

Q04b First take the contrapositive of the statement, so we will get where p is prime:

$$p \not| a \implies \text{ if a is even or} (a^{2(p-1)})^n - 1 \equiv 1 \pmod{2^n p}$$

Lets look at the first case:

$$p \not| a \implies (a^{2(p-1)})^n - 1 \equiv 1 \pmod{2^n p}$$

Since we are we are assuming the second case is false, this means that a is even. We know from the previous question that when a is odd it can be expressed as for some integer k:

$$(a^2)^{k-1} \equiv 1 \text{ (mod } 2^k)$$

If we raise both sides to the power of (p-1) we end up getting:

$$(a^2)^{(k-1)(p-1)} \equiv 1^(p-1) \text{ (mod } 2^k)$$

$$(a^2)^{(k-1)(p-1)} \equiv 1 \text{ (mod } 2^k)$$

We can use FLT as p can not divide the left values and since $p|a$ and a is to the power of c:

$$(a^2)^{(k-1)(p-1)} \equiv 1 \text{ (mod } p)$$

We also know that the $\gcd(p, 2^n) = 1$ so we can use CRT:

$$(a^2)^{(k-1)(p-1)} \equiv 1 \text{ (mod } 2^k p)$$

Thus proving the contrapositive as in the other case p and never divide a as a is even and p by definition is an odd prime!