The case of 2^k

a is an odd number. Is there a solution for the cogruence $x^2 \equiv a \pmod{2^k}$

k	units	QR
1	1	1
2	1, 3	1
3	1, 3, 5, 7	1
4	1, 3, 5, 7, 9, 11, 13, 15	1, 9
5	1, 3, 5, 7, 9, 11, 13, 15 17, 19, 21, 23, 25, 27, 29, 31	1, 9, 17, 25

Theorem: Let $k \geq 3$, then a is a QR modulo 2^k if and only $a \equiv 1 \pmod 8$. Therefore, there are 2^{k-3} QR modulo 2^k and $\underset{\phi(2^k)-2^{k-3}}{3 \cdot 2^{k-3}}$ QNR modulo 2^k.

Proof: The second part is an immediate result of the first part.
We prove by induction on k.

Base case $k = 3$ ✓

Assume true for some $k \geqslant 3$, then prove for $k+1$.

$(\Rightarrow)$ If a is a QR, then $x^2 \equiv a \pmod{2^{k+1}}$

$$\Rightarrow x^2 \equiv a \pmod 8$$

$$\Rightarrow a \equiv 1 \pmod 8$$

$(\Leftarrow)$: Suppose $a \equiv 1 \pmod 8$. By induction hypothesis $x^2 \equiv a \pmod{2^k}$ for some x (x must be odd obviously)

we have $\underbrace{x^2 \equiv a \pmod{2^{k+1}}}_{\text{(we are done)}}$ or $x^2 \equiv a + 2^k \pmod{2^{k+1}}$

Suppose $x^2 \equiv a + 2^k \pmod{2^{k+1}}$

Let $y = x + 2^{k-1}$, then

$$y^2 \equiv x^2 + \underbrace{2^{2k-2}}_{0 \pmod{2^{k+1}}} + \underbrace{2^k \cdot x}_{2^k \pmod{2^{k+1}}} \equiv (a + 2^k) + (0) + 2^k$$

$2k-2 \geqslant k+1$ $\qquad \equiv a \pmod{2^{k+1}}$. ∎

The general case $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$

Suppose $(a, n) = 1$.

a is a QR modulo n if and only if a is a QR modulo each $p_i^{\alpha_i}$.

$$x^2 \equiv a \pmod{n} \quad \longrightarrow \quad \begin{array}{c} x^2 \equiv a \pmod{p_1^{\alpha_1}} \\ \vdots \\ x^2 \equiv a \pmod{p_k^{\alpha_k}} \end{array}$$

<u>Remark</u>: QR × QR = QR, but QNR × QNR might not be a QR in the general case.
For example; 5 (mod 12), 7 (mod 12) are QNR but $35 \equiv 11 \pmod{12}$ also a QNR.

Law of Quadratic Reciprocity

$p \neq q$ odd primes.

p or q or both $\equiv 1 \pmod 4 \Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$

$p \equiv q \equiv 3 \pmod 4 \Rightarrow \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Proof

Consider the set

$$S = \left\{ 1 \leq n \leq \frac{pq-1}{2} \ : \ (n, pq) = 1 \right\}.$$

We'll look at the product of the elements of S mod (pq) (or equiv. mod (p) and mod (q)).

Step-1

In mod p : The product is

$$p \cdot \frac{q-1}{2} = \frac{pq-p}{2}$$

$$\frac{(1\cdot 2\cdot \ldots \cdot (p-1))\cdot(1\cdot 2\cdot \ldots (p-1))\cdot(1\cdot 2\cdot \ldots (p-1))\cdot \ldots \cdot (1\cdot 2 \cdot \ldots (p-1))\cdot 1\cdot 2\cdot \ldots \cdot \frac{p-1}{2}}{q \cdot 2q \cdot 3q \cdot \ldots \cdot \frac{p-1}{2}\cdot q}$$

modulo p, which is equivalent to

$$\frac{(p-1)!^{\frac{q-1}{2}} \cdot \cancel{\left(\frac{p-1}{2}\right)!}}{q^{\frac{p-1}{2}} \cdot \cancel{\left(\frac{p-1}{2}\right)!}} \equiv \frac{(-1)^{\frac{q-1}{2}}}{\left(\frac{q}{p}\right)} \equiv (-1)^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) \pmod p$$

The product is $(-1)^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right)$ modulo p

In mod q : Similarly, $(-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)$ modulo q.

Step-2

In mod pq using a different method

Claim : The product is 1 or -1 (mod pq) if and only if $p \equiv q \equiv 1 \pmod 4$

Proof of the claim:

For any $n \in S$, we have $n^{-1} \pmod{pq} \in S$ or $-n^{-1} \pmod{pq} \in S$

Pairing up n with n^{-1} or $-n^{-1}$, we get 1 or -1 modulo pq.

The only issue is $n^2 \equiv -1, 1 \pmod{pq}$

- $n^2 \equiv 1 \pmod{pq}$ have 4 solutions by CRT

Say $1, x, -x, -1$ are these solutions (suppose $x \in S$)

- $n^2 \equiv -1 \pmod{pq}$ have no solution unless $p \equiv q \equiv 1 \pmod 4$. In this case, the product of elements of S is $\pm x \pmod{pq}$ which is not $\pm 1 \pmod{pq}$

- $n^2 \equiv -1 \pmod{pq}$ have four solutions by CRT when $p \equiv q \equiv 1 \pmod 4$. Actually they will be $y, -y, xy, -xy$ for some y.

$\Rightarrow$ Then the product will be

$$(\pm x) \cdot (\pm y \cdot \pm xy) = \pm (xy)^2 \equiv \pm 1 \pmod{pq}.$$

Step-3 : (added after lecture)

Say s is the product of the elements of S

In Step-1, we showed

$$s \equiv \text{something} \equiv -1 \text{ or } 1 \pmod p$$

$$s \equiv \text{something} \equiv -1 \text{ or } 1 \pmod q$$

In Step-2, we showed

$$\boxed{s \equiv -1 \text{ or } 1 \pmod{pq}} \Leftrightarrow p \equiv q \equiv 1 \pmod 4$$

$\downarrow$

This means either

$s \equiv 1 \pmod p$, $s \equiv 1 \pmod q$

or

$s \equiv -1 \pmod p$, $s \equiv -1 \pmod q$

and that means

$$(-1)^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right)$$

both 1 or both -1

So, we have

$$(-1)^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \iff p \equiv q \equiv 1 \pmod 4$$

- If $p \equiv q \equiv 1 \pmod 4 \Rightarrow \text{LHS} = \text{RHS}$

$$\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

- If $p \equiv 1,\ q \equiv 3 \pmod 4 \Rightarrow \text{LHS} \neq \text{RHS}$

$$\Rightarrow -\left(\frac{q}{p}\right) \neq \left(\frac{p}{q}\right)$$

$$\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

- If $p \equiv 3,\ q \equiv 1 \pmod 4$: similar as above

$$\Rightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

- If $p \equiv q \equiv 3 \pmod 4 \Rightarrow \text{LHS} \neq \text{RHS}$

$$\Rightarrow -\left(\frac{q}{p}\right) \neq -\left(\frac{p}{q}\right)$$

$$\Rightarrow \left(\frac{q}{p}\right) \neq \left(\frac{p}{q}\right)$$

$$\Rightarrow \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$