How to judge if a is QR (quadratic residue) or is QN (quadratic nonresidue) mod p?

There is a so called Jacobi symbol, which can be efficiently calculated. However, we shall use a simpler tool (not as efficient as the Jacobi symbol, but we are going to focus on EC).

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

(a; $\equiv 1$ by Fermat little theorem)

$$\forall a \in \mathbb{F}_p^* \quad a^{p-1} = 1 \pmod p$$

alternatively: $\operatorname{ord} a \mid |\mathbb{F}_p^*| = p-1$ for $a \in \mathbb{F}_p^*$

$$\exists k \in \mathbb{Z} \quad (\operatorname{ord} a)\cdot k = p-1 \Rightarrow k = 1$$

$\operatorname{ord} g = p-1$ because g is a generator

$$a^{p-1} = \left(a^{\operatorname{ord} a}\right)^{k} \equiv 1^k \equiv 1 \pmod p$$

$$\left(g^{2l+1}\right)^{\frac{p-1}{2}} = \left(g^{2l}\right)^{\frac{p-1}{2}} \cdot g^{\frac{p-1}{2}} \pmod p =$$

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

$$= g^{2l\cdot\frac{p-1}{2} + \frac{p-1}{2}} = \underbrace{\left(g^{2l}\right)^{\frac{p-1}{2}}}_{=1} \cdot g^{\frac{p-1}{2}} \pmod p$$

$$= 1 \cdot g^{\frac{p-1}{2}} \pmod p = g^{\frac{p-1}{2}} \pmod p$$

since g is a generator of $\mathbb{F}_p^*$

$\neq 1 \pmod p$ because otherwise $\operatorname{ord} g \leq \frac{p-1}{2}$

$$\left(g^{\frac{p-1}{2}}\right)^2 = 1 \pmod p$$ so we have to get a square root "$X^2 = 1 \pmod p$"

$$\Leftrightarrow X^2 - 1 = 0 \pmod p \Rightarrow X \in \{-1, 1\} = \{p-1, 1\}$$

Hence for $a \in \mathbb{F}_p^*$

$$\begin{cases} \text{if } a^{\frac{p-1}{2}} = 1 \pmod p \text{ then } a \text{ is a quadratic residue} \\ \text{if } a^{\frac{p-1}{2}} = -1 \pmod p \text{ then } a \text{ is a quadratic non-residue} \end{cases}$$

assume that

So we have a being QR.

How to find x such that

$$x^2 = a \pmod p \quad ?$$

If $p \equiv 3 \pmod 4$ then

$x = a^{\frac{p+1}{4}} \pmod p$ then:

$$x^2 = \left(a^{\frac{p+1}{4}}\right)^2 \pmod p = a^{\frac{p+1}{2}} \pmod p =$$

$$= a \cdot \underbrace{a^{\frac{p-1}{2}}}_{=1} \pmod p = a \pmod p$$

so $x = a^{\frac{p+1}{4}} \pmod p$ is a square root from a. $\quad x = -\left(a^{\frac{p+1}{4}}\right) \pmod p$

What if $p \equiv 1 \pmod 4$?

Represent $p-1$ as a product:

$$p - 1 = s \cdot 2^t \,, \quad \gcd(s, 2) = 1$$

From the CRT we have that any $k \pmod{p-1}$ is equivalent to a system of congruences:

$$k \pmod{p-1} \Leftrightarrow \begin{cases} k_1 \pmod s \\ k_2 \pmod{2^t} \end{cases}$$

in such a way that

$$k \equiv k_1 \cdot N_1 \cdot 2^t + k_2 N_2 \cdot s \pmod{p-1}$$

$$\begin{cases} N_1 \cdot 2^t \equiv 1 \pmod s \\ N_2 \cdot s \equiv 1 \pmod{2^t} \end{cases}$$

mod $p-1$ arithmetic is implicitly induced by ord $g = p-1$

That is $a = g^k \pmod p = g^{k_1 N_1 \cdot 2^t + k_2 \cdot N_2 \cdot s} \pmod p$

a is some power of the generator g

$$= g^{k_1 \cdot N_1 \cdot 2^t} \cdot g^{k_2 N_2 \cdot s} \pmod p =$$

$$= \left(\left(g^{2^t}\right)^{N_1}\right)^{k_1} \cdot \left(\left(g^s\right)^{N_2}\right)^{k_2} \pmod p$$

Define:

$$\begin{cases} g_1 := \left(g^{2^t}\right)^{N_1} \pmod p \\ g_2 := \left(g^s\right)^{N_2} \pmod p \end{cases}$$

since $\operatorname{ord} g = p-1$ $\quad \operatorname{ord} g_1 = s$

$$2^t \mid p-1 \quad \operatorname{ord} g^{2^t} = \frac{\operatorname{ord} g}{2^t} = s$$

and $(N_1, s) = 1$ hence

$$\operatorname{ord}\left(g^{2^t}\right)^{N_1} = \frac{s}{(N_1, s)} = \frac{s}{1} = s$$

$$\operatorname{ord} g^k = \frac{\operatorname{ord} g}{\gcd(k, \operatorname{ord} g)}$$

Similarly $\operatorname{ord} g_2 = 2^t$

All in all

$$a = g_1^{\overbrace{k_1}^{\text{mod } s}} \cdot g_2^{\overbrace{k_2}^{\text{mod } 2^t}} \pmod p$$

arithmetic, induced by the orders of g_1 and g_2

$(\_ \bmod s, \_ \bmod 2^t)$

$$\operatorname{ord} g^k = \frac{\operatorname{ord} g}{\gcd(k, \operatorname{ord} g)}$$

$$d = \gcd(k, \operatorname{ord} g)$$

from the extended Euclidean algorithm we have:

$$d = k \cdot u + (\operatorname{ord} g) \cdot v \quad \text{for some } u, v \in \mathbb{Z}$$

$g^k \in \langle g^d \rangle$ because $k = d \cdot q$, $q \in \mathbb{Z}$

$$g^k = (g^d)^q$$

$$\underline{\langle g^k \rangle \subseteq \langle g^d \rangle}$$

$g^d \in \langle g^k \rangle$

because $g^d = g^{ku + \text{ord}g \cdot v} \pmod p$

$= (g^k)^u \cdot \underbrace{(g^{\text{ord}g})^v}_{=1} \pmod p$

$= (g^k)^u \pmod p$

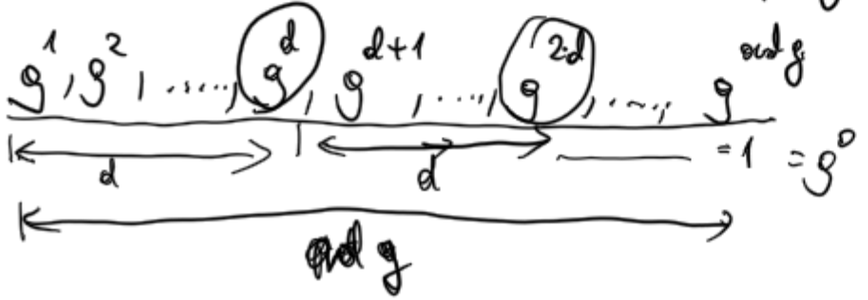
$\underline{\langle g^d \rangle \subseteq \langle g^k \rangle}$

From both inclusions we get

$\langle g^k \rangle = \langle g^d \rangle$

so the orders are equal as well:

$$\text{ord}\, g^k = \text{ord}\, g^d = \frac{\text{ord}\, g}{d} = \frac{\text{ord}\, g}{(k, \text{ord}\, g)}$$



$a = g_1^{k_1} \cdot g_2^{k_2} \pmod p$

Note that k_2 must be an even integer:

from CRT

$$k = k_1 \cdot N_1 \cdot 2^t + k_2 \cdot N_2 \cdot s \pmod{\underbrace{p-1}_{\text{ord}\, g}}$$

in the integers:

$$k = Q \cdot \underbrace{(p-1)}_{\text{even}} + \underbrace{k_1 \cdot N_{\not 2} \cdot 2^t}_{\text{even}} + k_2 \cdot N_2 \cdot s$$

Q for some $Q \in \mathbb{Z}$

even because a is QR

$N_2 \cdot s$ odd

$N_2 \cdot s \equiv 1 \pmod{2^t}$

$\Downarrow$

$(N_2, 2) = 1$

k_2 must be even (the only option)

Set $r := a^{\frac{s+1}{2}} \pmod p$

Note that:

$$a^{-1} \cdot r^2 = a^{-1} \left(a^{\frac{s+1}{2}}\right)^2 = a^{-1} \cdot a^{s+1} = a^s \pmod p$$

$$= \underbrace{g_1^{k_1 \cdot s}}_{\text{ord}\, g_1 = s} \cdot g_2^{k_2 \cdot s} = 1 \cdot g_2^{k_2 \cdot s} \pmod p$$

Thus

$a^{-1} \cdot r^2 \in \langle g_2 \rangle$, and $g_2 = 2^t \Rightarrow \text{ord}(a^{-1}r^2) = 2^l$ for some l

and since k_2 is even then $l \leq t-1$

So we can write

$$(a^{-1} \cdot r^2)^{2^{t-1}} = 1 \pmod p$$

because $\left((a^{-1} \cdot r^2)^{2^l}\right)^{2^{t-1-l}} = 1^{2^{t-1-l}} \pmod p$

$= 1$

Consider the case $p \equiv 3 \pmod 4$

In such a case $p - 1 = 2^1 \cdot 5$, so we expect that $l = 0$ and in r we have a complete square root. Indeed:

$$\left(a^{\frac{S+1}{2}}\right)^2 = a^{S+1} = a^{\frac{p-1}{2}+1} = \underbrace{a^{\frac{p-1}{2}}}_{1 \text{ because } a \text{ is QR}} \cdot a \equiv a \pmod p$$

so for $p \equiv 3 \pmod 4$ r is a square root from a.