let $p > 2$ be prime. We describe an algorithm (due to A. Tonelli (Atti Accad. Lincei 1892) and D. Shanks (1970ies)) to compute a square root of a given square $a \in \mathbf{Z}_p^*$. For this we need to know a non-square $g \in \mathbf{Z}_p^*$. We write $p-1 = 2^m q$ with q odd and put $\zeta = g^q$. The number ζ is a generator of the 2-part of the cyclic group $\mathbf{Z}_p^*$.

Putting

$$b = a^{\frac{q+1}{2}}, \qquad c = a^q,$$

we have

$$b^2 = ac, \qquad c \in \langle \zeta^2 \rangle.$$

If $c = 1$ we are done. If not, then we modify b, c and ζ as follows. Let $k, l \geq 0$ be the unique integers for which $c^{2^k} = -1$ and $\zeta^{2^l} = -1$ respectively. Since c is contained in the cyclic group generated by ζ^2, we have $l > k$. Put

$$\begin{aligned} b &\leftarrow b\,\zeta^{2^{l-k-1}}, \\ c &\leftarrow c\,\zeta^{2^{l-k}}, \\ \zeta &\leftarrow \zeta^{2^{l-k}}. \end{aligned}$$

Then we still have $b^2 = ac$ and $c \in \langle \zeta^2 \rangle$. This follows from the fact that the new ζ has order 2^{k+1}, while the new ζ raised to the power 2^k is equal to 1.

In every step the order of ζ and hence of c decreases. Eventually $c = 1$ and $b^2 = ac = a$ and we are done. The time needed to perform the computations is essentially equal to the time needed to compute a $p-1$-th power in $\mathbf{Z}_p^*$. It is bounded by $O(\ln^3 p)$.

Example. Let $p = 400009$. Then $g = 19$ is a primitive root mod p. We have $p - 1 = 400008 = 2^m q$ with $m = 3$ and $q = 50001$ and hence $\zeta = g^q = 284991$. We compute the square root of $a = 2$. We have $b = a^{(q+1)/2} = 357332$ and $c = a^q = 42676$. One checks that $b^2 = ac$ in $\mathbf{Z}_p^*$.

We make the first step. We have $c^2 = -1$ and $\zeta^4 = -1$. Therefore $k = 1$ and $l = 2$. We replace b by $b\,\zeta = 112747$ and c by $c\,\zeta^2 = -1$. We also replace ζ by $\zeta^2 = 42676$. One checks that $b^2 = ac$.

Since $c \neq 1$ we make a second step. We have $c = -1$ and $\zeta^2 = -1$. Therefore $k = 0$ and $l = 1$. We replace b by $b\,\zeta = 282720$ and c by $c\,\zeta^2 = 1$. We also replace ζ by $\zeta^2 = -1$. This time $c = 1$ and $b^2 = a$. So we are done.