1. Raise (r^2/a) to the $2^{\alpha-2}$-th power. We proved that the square of this is 1. Hence, you get either ± 1. If you get 1, take $j_0 = 0$; if you get -1, take $j_0 = 1$. Notice that j_0 has been chosen so that $((b^{j_0}r)^2/a)$ is a $2^{\alpha-2}$-th root of unity.
2. Suppose you've found $j_0, \ldots, j_{k-1}$ such that $(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}}r)^2/a$ is a $2^{\alpha-k-1}$-th root of unity, and you want to find j_k. Raise this number to half the power that gives 1, and choose j_k according to whether you get $+1$ or -1:

$$\text{if} \quad \left(\frac{\left(b^{j_0+2j_1+\cdots+2^{k-1}j_{k-1}}r\right)^2}{a}\right)^{2^{\alpha-k-2}} = \begin{cases} 1 \\ -1 \end{cases},$$

$$\text{then take} \quad j_k = \begin{cases} 0 \\ 1 \end{cases}, \quad \text{respectively.}$$

We easily check that with this choice of j_k the "corrected" value comes closer to being a square root of a, i.e., we find that $(b^{j_0+2j_1+\cdots+2^k j_k}r)^2/a$ is a $2^{\alpha-k-2}$-th root of unity.

When we get to $k = \alpha - 2$ and find $j_{\alpha-2}$, we then have

$$(b^{j_0+2j_1+\cdots+2^{\alpha-2}j_{\alpha-2}}r)^2/a = 1,$$

i.e., $b^j r$ is a square root of a, as desired.

Example 3. Use the above algorithm to find a square root of $a = 186$ modulo $p = 401$.

Solution. The first nonresidue is $n = 3$. We have $p - 1 = 2^4 \cdot 25$, and so $b = 3^{25} = 268$ and $r = a^{13} = 103$ (where we use equality to denote congruence modulo p). After first computing $a^{-1} = 235$, we note that $r^2/a = 98$, which must be an 8-th root of 1. We compute that $98^4 = -1$, and so $j_0 = 1$. Next, we compute $(br)^2/a = -1$. Since the 2-nd power of this is 1, we have $j_1 = 0$, and then $j_2 = 1$. Thus, $j = 5$ and the desired square root is $b^5 r = 304$.

Remarks. **1.** The easiest case of this algorithm occurs when p is a prime which is $\equiv 3 \bmod 4$. Then $\alpha = 1$, $s = (p-1)/2$, so $(s+1)/2 = (p+1)/4$, and we see that $x = r = a^{(p+1)/4}$ is already the desired square root.

2. We now discuss the time estimate for this algorithm. We suppose that we start already knowing the information that n is a nonresidue. The steps in finding s, b, and $r = a^{(s+1)/2}$ (working modulo p, of course) take at most $O(log^3 p)$ bit operations (see Proposition I.3.6). Then in finding j the most time-consuming part of the k-th induction step is raising a number to the $2^{\alpha-k-2}$-th power, and this means $\alpha - k - 2$ squarings mod p of integers less than p. Since $\alpha - k - 2 < \alpha$, we have the estimate $O(\alpha\, log^2 p)$ for each step. Thus, since there are $\alpha - 1$ steps, the final estimate is $O(log^3 p + \alpha^2 log^2 p) = O(log^2 p(log\, p + \alpha^2))$. At worst (if almost all of $p - 1$ is a power of 2), this is $O(log^4 p)$, since $\alpha < log_2 p = O(log\, p)$. Thus, given a nonresidue