Finding Square Roots in The Integers Mod p, with p Prime

Let p be an odd prime.

We have an easy test that will tell us whether an integer a, $a \not\equiv 0 \pmod{p}$, has a square root mod p, or not. (i.e., whether a is a quadratic residue or quadratic nonresidue, mod p.)

$$\text{Specifically, } a \text{ is } \begin{cases} \text{a quadratic residue if } & a^{(p-1)/2} \equiv 1 \pmod{p} \\ \text{a quadratic nonresidue if} & a^{(p-1)/2} \equiv -1 \pmod{p} \end{cases}$$

Assuming the a passes the test above for being a quadratic residue, the algorithm below will actually find a square root of a mod p. It is most useful when $p \equiv 1 \pmod{4}$, as the case $p \equiv 3 \pmod{4}$ is very easy to solve.

Write $p - 1 = 2^s \cdot m$, with m odd.	
z = any nonresidue mod p.	
$c \equiv z^m \pmod{p}$.	*Note* $o(c)$ *is* 2^s.
$u \equiv a^m \pmod{p}$.	$o(u)$ *divides* 2^{s-1}*, as u is a quad res.*
$v \equiv a^{(m+1)/2} \pmod{p}$.	*Note* $v^2 \equiv ua \pmod{p}$.
for ($i = s-1, s-2, \ldots, 2, 1$) {	*Each pass starts with o(u) dividing dividing* 2^i*. Either o(u) divides* 2^{i-1}*, or* $u^{2^{i-1}} \equiv -1 \pmod{p}$*. In the latter case, we modify u and v so as to make o(u) divide* 2^{i-1}*, while maintaining the property* $v^2 \equiv ua \pmod{p}$*.*
if ($u^{2^{i-1}} \equiv -1 \pmod{p}$) {	
$u = uc^2$.	
$v = vc$.	
}	
$c = c^2$.	
}	
Now v is a square root of a.	

Example: Find a square root of 83 mod 673.

$672 = 2^5 \cdot 21$, so $s = 5$ and $m = 21$.

After trying several possibilities, we discover that $5^{336} \equiv -1 \pmod{673}$, so we may choose $z = 5$.

$u \equiv a^m \equiv 589, \quad v \equiv a^{(m+1)/2} \equiv 190, \quad c \equiv z^m \equiv 118 \pmod{673}$

$i = 4$: $u^8 \equiv -1$

$u \equiv uc^2 \equiv 58, \quad v \equiv vc \equiv 211, \quad c \equiv c^2 \equiv 464 \pmod{673}$

$i = 3$: $u^4 = 1$

u and v are unchanged, $\quad c \equiv c^2 \equiv 609$

$i = 2$: $u^2 \equiv -1$

$u \equiv uc^2 \equiv 672, \quad v \equiv vc \equiv 629, \quad c \equiv c^2 = 58$

$i = 1$: $u \equiv -1$

$u \equiv uc^2 \equiv 1, \quad v \equiv vc \equiv 140, \quad c \equiv c^2 \equiv -1$

$u \equiv 1$

Thus 140 is square root of 83 mod 673, as is -140 .