SQUARE ROOTS (mod p)

Let $p \equiv 3 \pmod 4 =$ prime, and let $1 \leq a < p$.

We will show that if $x^2 \equiv a (\text{mod } p)$ is solvable for some $1 \leq x < p$ then all solutions are given by

$$\boxed{x \;\equiv\; \pm a^{\frac{p+1}{4}} \pmod p.} \tag{1}$$

Problem: Assume that $x^2 \equiv 11 \pmod{19}$. Find x.

Solution: It follows from (1) that $x \equiv 11^5 \pmod{19} = 7$. We check that $7^2 \equiv 11 \pmod{19}$. The other solution is $-7 \equiv 12 \pmod{19}$.

Proof. We will now prove that (1) gives all the square roots of $a \pmod p$. Since we assume there is a solution to $x^2 \equiv a (\text{mod } p)$ we can raise both sides to the $\frac{p-1}{2}$ power yielding $1 \equiv x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod p$.

It follows that

$$\left(\pm a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a^{\frac{p-1}{2}} \cdot a \;\equiv\; a \pmod p.$$

It only remains to show that $x \equiv \pm a^{\frac{p+1}{4}} \pmod p$ are the only solutions. This follows from the fact that a quadratic equation $x^2 \equiv a (\text{mod } p)$ either has no solutions or exactly 2 solutions as long as $a \not\equiv 0 \pmod p$. To see this last part assume $r^2 \equiv a \pmod p$. Then $\pm r$ are two distinct square roots of $a \pmod p$. Suppose $t^2 \equiv a \pmod p$. This implies

$$t^2 \equiv r^2 \pmod p.$$

It follows that $p \big| (t-r)(t+r)$ so p must divide one of the two factors, i.e.,

$$p \big| (t-r) \implies t \equiv r \pmod p \quad \text{while} \quad p \big| (t+r) \implies t \equiv -r \pmod p.$$

$\square$