Cipolla's algorithm for finding square roots mod p
Optional reading for Math 2803: Number Theory and Cryptography

Suppose we're given an odd prime number p and a quadratic residue $a \in (\mathbf{Z}/p\mathbf{Z})^*$. We'll discuss a probabilistic method for efficiently computing a square root (and hence both square roots) of a mod p which does not make any assumptions about p. (Recall that if $p \equiv 3 \pmod 4$ then $b := a^{(p+1)/4} \pmod p$ is a square root of a, so we're mainly interested in the case $p \equiv 1 \pmod 4$.)

The first step is to find an integer t with $0 \le t \le p-1$ such that $u := t^2 - a$ is a quadratic nonresidue mod p. The only known method to do this is probabilistic: for random values of t, the number $t^2 - a$ will be a quadratic nonresidue with probability about $1/2$. Thus, if $t_1, \ldots, t_n$ are chosen randomly, the probability that none of the $t_i^2 - a$ is a nonresidue is about $1/2^n$. So in practice, we will always very quickly be able to find a suitable value of t, since for any particular t_i we can use Euler's criterion to efficiently decide if $t_i^2 - a$ is a quadratic residue or not.

Let $\mathbf{F}_p$ denote the set $\{0, 1, \ldots, p-1\}$ endowed with the operations of multiplication and addition modulo p. We define $\mathbf{F}$ as the set of all ordered pairs (x, y) with $x, y \in \mathbf{F}_p$, together with the addition and multiplication laws

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

and

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 + y_1 y_2 u, x_1 y_2 + x_2 y_1).$$

The motivation for this is that we are secretly thinking of $\mathbf{F}$ as consisting of sums of the form $\{x + \omega y \; : \; x, y \in \mathbf{F}_p\}$, where ω is a formal symbol representing a square root of u. Of course, u doesn't have a square root in $\mathbf{F}_p$ by assumption, so ω should be thought of as analogous to the complex number i. We have identified $x + y\omega$ with the ordered pair (x, y), just as we often represent a complex number $x + yi$ as a point (x, y) in the complex plane.

Two important facts are that (i) every element $x + y\omega$ of $\mathbf{F}$ has an additive inverse $x - y\omega$, and (ii) every nonzero $x + y\omega \in \mathbf{F}$ has a multiplicative inverse. To see (ii), note that if we define

$$\|x + y\omega\|^2 = (x + y\omega)(x - y\omega) = x^2 - y^2 u,$$

then $\|x + y\omega\|^2 \neq 0$ for $x + y\omega \neq 0$ because u is a quadratic nonresidue. Thus

$$(x + y\omega)^{-1} = \frac{x - y\omega}{\|x + y\omega\|^2}.$$

It follows that $\mathbf{F}$ is what mathematicians call a (finite) **field**. The importance of this is that our "Polynomial Roots mod p Theorem" holds in any field, with essentially the same proof as the one given in the book. In particular:

A nonzero polynomial of degree n with coefficients in $\mathbf{F}$ has at most n distinct roots in $\mathbf{F}$.

The other key fact we need about arithmetic in $\mathbf{F}$ is the following:

Lemma 1. *For every element $x + y\omega \in \mathbf{F}$, we have*

$$(x + y\omega)^p = x - y\omega.$$

Proof. Since u is a quadratic nonresidue, Euler's criterion tells us that

$$\omega^{p-1} = (\omega^2)^{\frac{p-1}{2}} = u^{\frac{p-1}{2}} = -1$$

in $\mathbf{F}$. Thus $\omega^p = -\omega$. From this, the fact that all binomial coefficients $\binom{p}{j}$ for $1 \leq j \leq p-1$ are divisible by p, and Fermat's Little Theorem (which in this context says that $x^p = x$ for all $x \in \mathbf{F}_p$), it follows that

$$(x + y\omega)^p = x^p + y^p\omega^p = x + y\omega^p = x - y\omega$$

as desired. □

Our main result is the following theorem:

Theorem 1. *Let $b = (t + \omega)^{\frac{p+1}{2}} \in \mathbf{F}$. Then:*

(i) $b^2 = a$ *in* $\mathbf{F}$.

(ii) $b \in \mathbf{F}_p$.

Proof. We compute that

$$b^2 = (t + \omega)^{p+1} = (t + \omega)(t + \omega)^p = (t + \omega)(t - \omega) = t^2 - \omega^2 = t^2 - (t^2 - a) = a.$$

This proves (i). Part (ii) follows from the fact that a nonzero polynomial of degree n with coefficients in $\mathbf{F}$ has at most n distinct roots in $\mathbf{F}$. Since we know that $x^2 - a$ has 2 roots in $\mathbf{F}_p$, these must be all of the roots in $\mathbf{F}$. Since b and $-b$ are both roots of $x^2 - a$ in $\mathbf{F}$, we must in fact have $\pm b \in \mathbf{F}_p$. □

Cipolla's algorithm: Compute $x_0 = (t + \omega)^{\frac{p+1}{2}}$ using repeated squaring in $\mathbf{F}$. The result will be an element of $\mathbf{F}_p$ with $x^2 = a$.

Example: Find the square roots of 2 (mod 17).

By trial and error, we see that $3^2 - 2 = 7$ is a quadratic nonresidue, so we can take $t = 3$ and $u = 7$. We have $\omega = \sqrt{7}$ and $\mathbf{F} = \{x + y\sqrt{7}\}$. We compute $x_0 = (3 + \sqrt{7})^9$:

$$
\begin{aligned}
&(3+\sqrt{7})^2 = 16 + 6\sqrt{7} \\
&(3+\sqrt{7})^4 = (161 + 6\sqrt{7})^2 = 15 + 5\sqrt{7} \\
&(3+\sqrt{7})^8 = (15 + 5\sqrt{7})^2 = 9 + 14\sqrt{7} \\
&(3+\sqrt{7})^9 = (3+\sqrt{7})^8(3+\sqrt{7}) = (9 + 14\sqrt{7})(3+\sqrt{7}) = 6.
\end{aligned}
$$

We conclude that $6^2 = 2$ in $\mathbf{F}_{17}$, so that 6 and $-6 = 11$ are the two square roots of 2 mod 17.

For a more elementary version of this algorithm, which does not make explicit use of the theory of finite fields, see my blog post `http://mattbakerblog.wordpress.com/2013/12/07/lucas-sequences-and-chebyshev-polynomials/`