Square roots modulo a prime

Robin Chapman

16 December 2003

Let p be an odd prime number. We shall consider how to solve the congruence $x^2 \equiv a \pmod p$ whenever a is a quadratic residue of p.

As **almost all** congruences in this note will be modulo p, we shall drop the notation "$(\mathrm{mod}\, p)$", just writing the congruence sign $\equiv$ when congruences modulo p are considered.

The easy case is where $p \equiv 3 \pmod 4$. Then $m = \frac{1}{2}(p-1)$ is an odd number. If a is a quadratic residue modulo p, then $a^m \equiv 1$ by Euler's criterion. Thus, as $m+1$ is even,

$$a \equiv a^{m+1} = (a^{(m+1)/2})^2$$

and it follows that the solution of $x^2 \equiv a$ is $x \equiv \pm a^{(m+1)/2} = \pm a^{(p+1)/4}$.

As an example, let $p = 1999$ and $a = 2$. Then using `MAPLE` we get the solution $\pm b$ where $b \equiv 2^{(p+1)/4} = 2^{500} \equiv 562$. We check that $562^2 \equiv 2$.

The hard case is where $p \equiv 1 \pmod 4$. In this case write $p = 2^s m$ where m is odd. Then $s \geq 2$. If a is a quadratic residue modulo p then $1 \equiv a^{(p-1)/2} = a^{2^{s-1}m} = (a^m)^{2^{s-1}}$. If we define

$$u_0 \equiv a^m \qquad \text{and} \qquad v_0 \equiv a^{(m+1)/2}$$

then

$$v_0^2 \equiv a^{m+1} \equiv a u_0.$$

If we are incredibly lucky, then u_0 will be congruent to 1 modulo p and then the solution of $x^2 \equiv a$ will be $x \equiv \pm v_0$. But we won't always be lucky. Note however, that $(u_0)^{2^{s-1}} \equiv 1$ and so the order of u_0 modulo p is a factor of 2^{s-1} and so is a power of 2.

In general, when $u_0 \not\equiv 1$, we shall construct sequences $u_0, u_1, u_2, \ldots$ and $v_0, v_1, v_2, \ldots$ with the property that

$$v_k^2 \equiv a u_k$$

and that the order of u_k modulo p is a power of 2, 2^{r_k} say, with $r_0 > r_1 > r_2 > \cdots$. If we can do this, we win, since eventually we get to a k with $r_k = 0$. This means that the order of u_k modulo p is $2^0 = 1$, which means that $1 \equiv u_k^1 = u_k$ so that $v_k^2 \equiv a$. The solution to $x^2 \equiv a$ is thus $x \equiv \pm v_k$.

To construct these sequences we need some more information. Let b be a quadratic nonresidue modulo p and let $c \equiv b^m$. Then

$$c^{2^{s-1}} \equiv b^{2^{s-1}m} = b^{(p-1)/2} \equiv -1$$

by Euler's criterion.

Now suppose we have some u_k and v_k with $v_k^2 \equiv au_k$ and also u_k having order 2^{r_k} modulo p with $0 < r_k \le s-1$. This means that

$$u_k^{2^{r_k}} \equiv 1 \qquad \text{but} \qquad u_k^{2^{r_k-1}} \not\equiv 1.$$

As $u_k^{2^{r_k}} = (u_k^{2^{r_k-1}})^2$ we conclude that

$$u_k^{2^{r_k-1}} \equiv -1.$$

Thus

$$1 \equiv u_k^{2^{r_k-1}} c^{2^{s-1}} = (u_k c^{2^{s-r_k}})^{2^{r_k-1}}.$$

Let us define

$$u_{k+1} \equiv u_k c^{2^{s-r_k}} \qquad \text{and} \qquad v_{k+1} \equiv v_k c^{2^{s-r_k-1}}$$

(this makes sense as $s - r_k - 1 \ge 0$). Then

$$v_{k+1}^2 \equiv v_k^2 c^{2^{s-r_k}} \equiv au_k c^{2^{s-r_k}} \equiv au_{k+1}$$

and also $u_{k+1}^{2^{r_k-1}} \equiv 1$. This means that the order of u_{k+1} modulo p is a factor of 2^{r_k-1}. This order is thus $2^{r_{k+1}}$ where $r_{k+1} \le r_k - 1 < r_k$. This completes the algorithm.

One stumbling block on this algorithm is that we need a quadratic nonresidue b of p. There is no deterministic algorithm that is proved to produce such a quadratic nonresidue in a short time. However one can easily find quadratic nonresidues randomly. For $p \equiv 1 \pmod 4$ if we choose uniformly at random an integer b with $2 \le b \le \frac{1}{2}(p-1)$ then it is a quadratic nonresidue with probability $> \frac{1}{2}$. The expected number of random picks to obtain a quadratic nonresidue is thus < 2.

Let us see this algorithm in action on a fairly complex example. Let $p = 769$. Then $p - 1 = 768 = 2^8 \times 3$, so $s = 8$ and $m = 3$. The first natural number which is a quadratic nonresidue of 769 is 7, so take $b = 7$

and so $c = 7^3 = 343$. It is convenient to calculate c^{2^j} for $0 \le j \le s-1$. We get $c^2 \equiv 343^2 \equiv 761$, $c^4 \equiv 761^2 \equiv 64$, $c^8 \equiv 64^2 \equiv 251$, $c^{16} \equiv 251^2 \equiv 712$, $c^{32} \equiv 712^2 \equiv 173$, $c^{64} \equiv 173^2 \equiv 707$ and $c^{128} \equiv 707^2 \equiv 768 \equiv -1$ as demanded by the theory.

Let us solve $x^2 \equiv 6$. We compute

$$u_0 = a^m = 6^3 = 216 \qquad \text{and} \qquad v_0 = a^{(m+1)/2} = 36.$$

Next, $u_0^2 = 216^2 \equiv 516$, $u_0^4 = 516^2 \equiv 182$, $u_0^8 = 182^2 \equiv 57$, $u_0^{16} = 57^2 \equiv 173$, $u_0^{32} = 173^2 \equiv 707$ and $u_0^{64} = 707^2 \equiv 768 \equiv -1$. Then

$$1 \equiv u_0^{64} c^{128} = (u_0 c^2)^{64}$$

so take

$$u_1 \equiv u_0 c^2 \equiv 216 \times 761 \equiv 579 \qquad \text{and} \qquad v_1 \equiv v_0 c = 36 \times 343 \equiv 44.$$

Next, $u_1^2 \equiv 579^2 \equiv 726$, $u_1^4 \equiv 726^2 \equiv 311$, $u_1^8 \equiv 311^2 \equiv 596$, $u_1^{16} \equiv 596^2 \equiv 707$, $u_1^{32} \equiv 707^2 \equiv -1$. Then

$$1 \equiv u_1^{32} c^{128} = (u_1 c^4)^{32}$$

so take

$$u_2 \equiv u_1 c^4 \equiv 579 \times 64 \equiv 144 \qquad \text{and} \qquad v_2 \equiv v_1 c^2 \equiv 44 \times 761 \equiv 417.$$

Next, $u_2^2 \equiv 144^2 \equiv 742$, $u_2^4 \equiv 742^2 \equiv 729$, $u_2^8 \equiv 729^2 \equiv 62$, $u_2^{16} \equiv 62^2 \equiv 768 \equiv -1$. Then

$$1 \equiv u_2^{16} c^{128} = (u_1 c^8)^{32}$$

so take

$$u_3 \equiv u_2 c^8 \equiv 144 \times 251 \equiv 1 \qquad \text{and} \qquad v_3 \equiv v_1 c^4 \equiv 417 \times 64 \equiv 542.$$

As $u_3 \equiv 1$ we conclude that the solution of $x^2 \equiv 6$ is $x \equiv \pm v_3 \equiv \pm 542 \equiv \mp 227$. Indeed we check that $227^2 \equiv 6$.