Quadratic Congruences

Solving the general quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

for an odd prime p (with $(a, p) = 1$) is equivalent to solving the simpler congruence

$$y^2 \equiv \Delta \pmod{p},$$

where $\Delta = b^2 - 4ac$ (the *discriminant* of the quadratic); further, x and y are related by the linear congruence $y \equiv 2ax + b \pmod{p}$. (Since $(2a, p) = 1$, we can recover x once we find y.)

The same line of argument works for arbitrary modulus m, as long as $(2a,m) = 1$. (Notice that we did not use the fact that p was prime above!) So solving quadratic congruences can be reduced to the consideration of the simple quadratic congruence

$$(*) \qquad x^2 \equiv a \pmod{m}.$$

We say that a is a **quadratic residue** (resp. **nonresidue**) if (*) is (resp. is not) solvable.

But if m has prime factorization $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, then by the CRT, (*) is equivalent to the system of congruences

$$(**)\qquad \begin{aligned} x^2 &\equiv a \pmod{p_1^{e_1}} \\ x^2 &\equiv a \pmod{p_2^{e_2}} \\ &\vdots \\ x^2 &\equiv a \pmod{p_k^{e_k}} \end{aligned}$$

Further, each of these congruences in (**) is controlled by means of the Lifting Theorem: since the underlying polynomial whose roots we are searching for is $f(x) = x^2 - a$, and $f'(x) = 2x$, we will always have $p \nmid f'(x_0) = 2x_0$ for any potential solution x_0 (none of the p's equals 2 as $(2a,m) = 1$), thus each solution to the congruence $x^2 \equiv a \pmod{p}$ will lift to a <u>unique</u> solution to $x^2 \equiv a \pmod{p^e}$, for any e. This focuses our attention finally on the fundamental case $x^2 \equiv a \pmod{p}$, p an odd prime.

Earlier we showed that $x^2 \equiv a \pmod{p}$ has only one solution $\Leftrightarrow$ $a \equiv 0 \pmod{p}$, which is not the case here since $(2a,m) = 1 \Rightarrow (2a, p) = 1 \Rightarrow p \nmid a$. But by Lagrange's Theorem, $x^2 \equiv a \pmod{p}$ can have at most 2 solutions.

So either $x^2 \equiv a \pmod p$ has 2 solutions – when a is a quadratic residue mod p, or $x^2 \equiv a \pmod p$ has no solutions – when a is a quadratic nonresidue mod p. Working back through the analysis, it follows that (**) can have no solutions if any one of the congruences $x^2 \equiv a \pmod{p_i}$ fails to have a solution. If all the congruences in (**) are solvable, they will have exactly two solutions each, whence the system will have 2^k solutions mod m.

This leaves us with the problem of solving the fundamental congruence $x^2 \equiv a \pmod p$: how does one tell whether a is a quadratic residue, and if so, how does one compute a square root of a mod p?

Proposition Exactly half of the p – 1 residue classes in U_p are quadratic residues (p an odd prime). In fact, where a is a primitive root mod p, the even powers, $a^2, a^4, \ldots, a^{p-1} (= 1)$, are the quadratic residues, and the odd powers, $a^1, a^3, \ldots, a^{p-2}$, are the quadratic nonresidues mod p.

Proof The residue classes in U_p correspond to the powers $a^1, a^2, \ldots, a^{p-1} (= 1)$ of a; a^k is a quadratic residue iff $a^k \equiv (a^n)^2 \pmod p$ for some n, $1 \le n \le p-1$, iff $k \equiv 2n (\mathrm{mod}(p-1))$. But p – 1 is even, so k is even iff a^k is a quadratic residue. Exactly half the numbers between 1 and p – 1 are even. //

Corollary Let p be an odd prime. (1) The product of two quadratic residues mod p is a quadratic residue. (2) The product of two quadratic nonresidues mod p is a quadratic residue. (3) The product of a quadratic residue and a quadratic nonresidue is a quadratic nonresidue.

Proof Let a be a primitive root mod p. Then x is a quadratic residue iff it is congruent to 0 or an even power of a, and is a quadratic nonresidue iff it is an odd power of a. The result follows, since multiplying powers of a corresponds to adding exponents. //

In 1798, a few years before the publication of Gauss' *Disquisitiones Arithmeticae*, Adrien-Marie Legendre introduced the following notation in his *Essai sur la theorie des nombres* to deal with the study of quadratic residues:

If p is an odd prime, the **Legendre symbol** $\left(\frac{a}{p}\right)$ is defined to be

- 0 if $p \mid a$,
- 1 if a is a quadratic residue mod p that is not divisible by p, and
- –1 iff a is a quadratic nonresidue mod p.

The corollary we just proved allows us to say that the Legendre symbol is multiplicative:

Proposition Let p be an odd prime. Then

(1) $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof Immediate. //

An important benefit of this notation is the way it simplifies the determination of quadratic residues mod p. In particular, if n has prime factorization $q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}$, then

$$\left(\frac{n}{p}\right) = \left(\frac{q_1}{p}\right)^{e_1} \left(\frac{q_2}{p}\right)^{e_2} \cdots \left(\frac{q_k}{p}\right)^{e_k}$$

so we need only worry about the determination of Legendre symbols of the form $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, and $\left(\frac{q}{p}\right)$, where q is an odd prime. One way to resolve this is through

Theorem (Euler's Criterion) If p is an odd prime and a is prime to p, then $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Proof Let g be a primitive root mod p. If a is a quadratic residue, then $a \equiv g^{2k} \pmod{p}$ for some k and $a^{(p-1)/2} \equiv (g^{2k})^{(p-1)/2} \equiv (g^{p-1})^k \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$. If a is a quadratic nonresidue, then $a \equiv g^{2k+1} \pmod{p}$ for some k and

$$\begin{aligned} a^{(p-1)/2} &\equiv (g^{2k+1})^{(p-1)/2} \\ &\equiv (g^{p-1})^k g^{(p-1)/2} \\ &\equiv g^{(p-1)/2} \\ &\equiv -1 \\ &\equiv \left(\frac{a}{p}\right) \pmod{p} \end{aligned}$$

//

We can also work out the Legendre symbol computation for $\left(\frac{-1}{p}\right)$ with ease:

Corollary Let p be an odd prime. Then

$$\left(\frac{-1}{p}\right) \equiv p \pmod{4}$$

Proof $(-1)^{(p-1)/2}$ is 1 $\Leftrightarrow$ $p \equiv 1 \pmod{4}$. //