

## Quadratic residues

**Theorem.** For prime  $p > 2$  and  $0 < a < p$ , the congruence  $x^2 \equiv a \pmod{p}$  has exactly 2 solutions (in a CSR) if  $a$  is a QR mod  $p$  and no solution if  $a$  is a QNR mod  $p$ .

**Proof:** By definition, “QNR” means “no solution”. If  $a$  is a QR, then there at least one solution  $x_1$ . Then also  $x_2 = p - x_1$  is a solution, and  $x_2 \not\equiv x_1 \pmod{p}$ . If  $y$  is a third solution, then  $y^2 \equiv a \equiv x_1^2 \pmod{p}$ , so  $p|(x_1 + y)(x_1 - y)$ . As  $p$  is prime,  $p$  must divide one of the factors, so  $y \equiv \pm x_1 \pmod{p}$ .

**Theorem.** For prime  $p > 2$ , there are  $(p - 1)/2$  QR and  $(p - 1)/2$  QNR in a CSR (or RSR) mod  $p$

**Proof:** The  $(p - 1)/2$  quadratic residues  $\{i^2 \pmod{p}; 1 \leq i \leq (p - 1)/2\}$  are all different and use up all available square roots mod  $p$ .

**Theorem.** (The Euler Criterion.) For prime  $p > 2$  and  $0 < a < p$ ,  $a^{(p-1)/2} \equiv 1 \pmod{p}$  if  $a$  is a QR mod  $p$  and  $a^{(p-1)/2} \equiv -1 \pmod{p}$  if  $a$  is a QNR mod  $p$ .

**Proof:** By Fermat,  $a^{p-1} \equiv 1 \pmod{p}$ , so  $p$  divides  $(a^{(p-1)/2} + 1)(a^{(p-1)/2} - 1)$ . Since  $p$  is prime,  $p$  must divide *one* of the factors  $a^{(p-1)/2} \pm 1$ . Thus  $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ . If  $a$  is a QR mod  $p$ , then there exists an  $x$  so that  $x^2 \equiv a \pmod{p}$ , so

$$a^{(p-1)/2} \equiv (x^2)^{(p-1)/2} \equiv x^{p-1} \equiv +1 \pmod{p}.$$

Thus the  $(p-1)/2$  QR's are some of the solutions to  $a^{(p-1)/2} \equiv +1 \pmod{p}$ . There can be no more solutions because the degree of this polynomial congruence is  $(p-1)/2$  and the integers mod  $p$  form a field. Therefore, if  $a$  is a QNR, then  $a^{(p-1)/2} \equiv -1 \pmod{p}$ .

Euler's Criterion motivates the definition of Legendre symbol:

**Definition:** If  $p$  is prime and  $a$  is an integer, the Legendre symbol  $(a/p)$  is defined to be  $+1$  if  $a$  is a QR mod  $p$ ,  $-1$  if  $a$  is a QNR mod  $p$ , and  $0$  if  $\gcd(a, p) > 1$ .

Here are some simple properties of the Legendre symbol:

1. The congruence  $x^2 \equiv a \pmod{p}$  has exactly  $1 + (a/p)$  solutions.

2.  $(a/p) \equiv a^{(p-1)/2} \pmod{p}$  (from Euler's Criterion).

3.  $(ab/p) = (a/p)(b/p)$ .

4. If  $a \equiv b \pmod{p}$ , then  $(a/p) = (b/p)$ .

5. If  $p \nmid a$ , then  $(a^2/p) = +1$  and  $(a^2b/p) = (b/p)$ .

6.  $(-1/p) = (-1)^{(p-1)/2}$ , which is  $+1$  when  $p \equiv 1 \pmod{4}$  and  $-1$  when  $p \equiv 3 \pmod{4}$ .

7.  $(2/p) = +1$  if  $p \equiv \pm 1 \pmod{8}$  and  $(2/p) = -1$  if  $p \equiv \pm 3 \pmod{8}$ .

Note that the "denominator" of a Legendre symbol is always an odd prime number. We have said nothing (so far) about solving  $x^2 \equiv a \pmod{n}$  when  $n$  is 2 or a composite number. (You can always solve  $x^2 \equiv a \pmod{2}$ .)