The Quadratic Residue Theorem

This MINIATURE will overlap slightly with MINIATURE number 7 but, to make it as self-contained as possible, no reference will be made to the individual results which were stated there and mainly left as exercises. Let p and q be odd primes. Then the "Quadratic residue theorem" states that if either or both of these primes is congruent to 1 (mod 4), then q is a quadratic residue of p iff p is a quadratic residue of q. On the other hand, if each of p and q is congruent to 3 (mod 4) then one and one only of p and q is a quadratic residue of the other. This is often stated using the "Legendre symbol" $(\frac{x}{p})$ which has the value 1 if x is congruent to a perfect square (mod p) (that is, if x is a "quadratic residue" of p), and to -1 if no such perfect square exists (that is, x is a "non-residue"). Using this notation we have

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

where we note that the exponent of -1 is even iff at least one of p and q is congruent to 1 (mod 4).

This result once existed only as an experimentally supported conjecture until Gauss stepped in and produced a number of different proofs. The proof that will be presented here will make use of a result known as "Gauss's Lemma" which states that, if x is not a multiple of p,

$$\left(\frac{x}{p}\right) = (-1)^{\mu},$$

where μ is the number of members of the set $\{x, 2x, 3x, \dots, (\frac{p-1}{2})x\}$ which are congruent (mod p) to members of the set $\{\frac{p+1}{2}, \dots, p-2, p-1\}$ (rather than to members of the set $P = \{1, 2, \dots, \frac{p-1}{2}\}$). Stepping back a little further, we can use as a criterion for x being a quadratic residue of p the fact that $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}}$ (mod p). This result, known as "Euler's crirerion", follows by considering the polynomial equation $t^{p-1} - 1 \equiv 0$ (mod p) and its factorisation $(t^{\frac{p-1}{2}} - 1)(t^{\frac{p-1}{2}} + 1) \equiv 0$ (mod p). All the remainders (mod p), that is the members of the set $S = \{1, 2, \dots, p-1\}$, satisfy the unfactorised equation (by the Fermat theorem) and hence exactly half of them satisfy each of (i) $t^{\frac{p-1}{2}} - 1 \equiv 0$ (mod p) an (ii) $t^{\frac{p-1}{2}} + 1 \equiv 0$ (mod p). Because exactly half of the members of S are quadratic residues and because these necessarily satisfy (i), the preliminary lemma follows.

Let n be any positive integer relatively prime to p and let x be a member of the set P. We will look at what happens when nx is divided by p to give a quotient m and a remainder r. The quotient is given by $m = \left[\frac{nx}{p}\right]$, where the brackets [.] denote "integer part of" and the remainder is either $x' \in P$ or $p - x'$ where $x' \in P$. It is easy to verify that the set of x' values for all members $x \in P$ is exactly P. From the identity $nx = pm + r$, we have

$$nx = \begin{cases} p\left[\frac{nx}{p}\right] + x', & \text{for } p-\mu \text{ values of } x, \\ p\left[\frac{nx}{p}\right] + p - x', & \text{for } \mu \text{ values of } x. \end{cases} \tag{1}$$

Gauss's lemma follows by interpreting (1) modulo p and forming the product for all $x \in P$. It follows that

$$n^{\frac{p-1}{2}} \prod_{x\in P} x \equiv (-1)^{\mu} \prod_{x \in P} x \pmod{p},$$

and because the product is not zero (mod p), the result follows.

As a step towards proving the quadratic reciprocity theorem, replace n by the odd prime q in (1) and now interpret the formula (mod 2). This time we *sum* over all $x \in P$ and we find

$$\sum_{x\in P} x \equiv \sum_{x\in P}\left[\frac{qx}{p}\right] - \mu + \sum_{x\in P} x \pmod{2},$$

where we have exchanged addition and subtraction where it has suited us because we are working modulo 2. It follows that μ is congruent (mod 2) to the number of lattice points in the set $(0, \frac{p}{2}) \times (0, \frac{q}{2})$ in the plane lying *beneath* the line $py = qx$. Reverse the roles of p and q and let ν denote the number of members y of $Q = \{1, 2, \dots, \frac{q-1}{2}\}$ such that yq is congruent (mod q) to a member of the set $\{\frac{q+1}{2}, \dots, q-2, q-1\}$; thus $\left(\frac{p}{q}\right) = (-1)^{\nu}$. With the roles of p and q interchanged we see that ν is congruent (mod 2) to the number of lattice points in $(0, \frac{p}{2}) \times (0, \frac{q}{2})$ *above* $py = qx$. Because p and q are primes, no lattice point actually lies on the line and hence $\mu + \nu$ differs by an integer multiple of 2 from the total number of lattice points. However, the total number of lattice points in this rectangle is simply $\frac{p-1}{2}\frac{q-1}{2}$.

We now fill in the details as follows:

$$\begin{aligned} \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) &= (-1)^{\mu}(-1)^{\nu} \\ &= (-1)^{\mu+\nu} \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \end{aligned}$$

John Butcher, `butcher@math.auckland.ac.nz`