The Law of Quadratic Reciprocity

Rahbar Virk
Department of Mathematics
University of Wisconsin
Madison, WI 53706, USA
virk@math.wisc.edu

Throughout we will be working in $\mathbb{Z}$. Consider the equation

$$ax^2 + bx + c \equiv 0 \mod p \tag{1}$$

where p is an odd prime and $a \not\equiv 0 \mod p$. So we have that $gcd(a,p) = 1$ and as p is odd, $gcd(4a,p) = 1$. Thus, (1) is equivalent to $4a(ax^2 + bx + c) \equiv 0 \mod p$ which gives us that $(2ax + b)^2 - (b^2 - 4ac) \equiv 0 \mod p$. Putting $y = 2ax + b$ and $d = b^2 - 4ac$ we obtain

$$y^2 \equiv d \mod p. \tag{2}$$

So finding a solution for (1) has been reduced to finding a solution for

$$x^2 \equiv a \mod p. \tag{3}$$

To avoid trivialities we assume that p does not divide a. Suppose x_0 is a solution to (3) then $x = p - x_0$ is also a solution to (3), furthermore $p - x_0 \not\equiv x_0$ as otherwise we would have that $p|x_0$ and so $p|a$. If $x^2 \equiv a \mod p$ admits a solution we call a a quadratic residue of p and a quadratic non residue otherwise.

Lemma (Euler's criterion). *Let p be an odd prime and suppose $gcd(a,p) = 1$, then a is a quadratic residue of p if and only if $a^{\frac{p-1}{2}} \equiv 1 \mod p$.*

Proof. Suppose a is a quadratic residue of p then, $x^2 \equiv a \mod p$ which implies that

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p.$$

Conversely, let r be a primitive root of p (we know one always exists for $p > 2$), we then have that $a \equiv r^k \mod p$, for some $k \in \mathbb{Z}_{>0}$. So

$$r^{\frac{k(p-1)}{2}} \equiv a^{\frac{p-1}{2}} \equiv 1 \mod p,$$

however, the order of r is $p - 1$, so $p - 1$ divides $\frac{k(p-1)}{2}$. Thus k is even and a is a quadratic residue. □

Define the Legendre symbol as,

$$(a|p) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue of } p \\ -1 & \text{if } a \text{ is not a quadratic residue of } p \end{cases}$$

Observe that Euler's criterion restated in terms of Legendre's symbol is just that

$$(a|p) \equiv a^{\frac{p-1}{2}} \mod p$$

Lemma. *Let p be an odd prime, then $\sum_{a=1}^{p-1}(a|p) = 0$.*

Proof. Let r be a primitive root of p, then $r^{\frac{p-1}{2}} \equiv -1 \mod p$, also, $r^k \equiv a \mod p$ for a unique k if $1 \leq a \leq p-1$. So $(a|p) = (r^k)^{\frac{p-1}{2}} \equiv (-1)^k \mod p$. It now follows clearly that $\sum_{a=1}^{p-1}(a|p) = 0$. □

Lemma (Gauss' lemma)**.** *Let p be an odd prime and suppose that $gcd(a, p) = 1$. If n denotes the number of integers in the set $S = \{a, 2a, 3a, \ldots, \frac{p-1}{2}a\}$ whose remainders upon division by p exceed $\frac{p}{2}$, then $(a|p) = (-1)^n$.*

Proof. As $gcd(a, p) = 1$ none of the members of S is congruent to 0 and no two are congruent to each other modulo p. Let $r_1, \ldots, r_m$ be the remainders upon division by p such that $0 < r_i < \frac{p}{2}$ and let $s_1, \ldots, s_n$ be those remainders such that $\frac{p}{2} < s_i < p$. Then we have that $m + n = \frac{p-1}{2}$ and the integers $r_1, \ldots, r_m, p - s_1, \ldots, p - s_n$ are all positive and less than $\frac{p}{2}$. We prove that they are all distinct. Suppose that $p - s_i = r_j$, so there exists $u, v \in S$ such that $s_i = ua$ and $r_j = va$, this means that $s_i + r_j \equiv 0 \equiv (u + v)a \mod p$, which gives us that $u + v \equiv 0 \mod p$, but $1 < u+v \leq p-1$, so this is a contradiction. It now follows that $r_1, \ldots, r_m, p-s_1, \ldots, p-s_n$ are all distinct. We thus have that

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &\equiv r_1 \cdots r_m(p - s_1) \cdots (p - s_n) \\ &\equiv r_1 \cdots r_m(-s_1) \cdots (-s_n) \\ &\equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \mod p.\end{aligned}$$

So $1 \equiv (-1)^n a^{\frac{p-1}{2}} \mod p$ and consequently $a^{\frac{p-1}{2}} \equiv (a|p) \equiv (-1)^n \mod p$, and the result now follows. □

Lemma. *Let p be an odd prime and a an odd integer such that $gcd(a, p) = 1$, then*

$$(a|p) = (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor}.$$

Proof. Let S be the set as in Gauss' lemma. Divide each element by p to get $ka = q_k p + t_k$ and so $k\frac{a}{p} = q_k + \frac{t_k}{p}$, this gives us that $\lfloor \frac{ka}{p} \rfloor = q_k$ and thus $ka = \lfloor \frac{ka}{p} \rfloor p + t_k$. If $t_k < \frac{p}{2}$ then it is one of the $r_1, \ldots, r_m$, if $t_k > \frac{p}{2}$ then its one of the $s_1, \ldots, s_n$. So

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor p + \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} s_k,$$

but we also have that

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{m} r_k + \sum_{k=1}^{n} (p - s_k) = \sum_{k=1}^{m} r_k + np - \sum_{k=1}^{n} s_k.$$

Combining the last two equations we obtain that

$$(a - 1)\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor p + 2\sum_{k=1}^{n} s_k - np.$$

So we have that $n \equiv \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{ka}{p} \rfloor \mod 2$. Now Gauss' lemma translates to the required result. □

Proposition (The Law of Quadratic Reciprocity). *If p and q are distinct odd primes then*

$$(p|q)(q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. Consider the rectangle in $\mathbb{R}^2$ whose vertices are at $(0,0), (\frac{p}{2}, 0), (0, \frac{q}{2}), (\frac{p}{2}, \frac{q}{2})$. Clearly the number of lattice points in this rectangle R is $\frac{p-1}{2}\frac{q-1}{2}$.
Observe that the diagonal D from $(0,0)$ to $(\frac{p}{2}, \frac{q}{2})$ has equation $y = \frac{q}{p}x$ or equivalently $py = qx$. Now as $gcd(p,q) = 1$ no lattice point in R lies on D. Let T_1 be the region of R below D and T_2 be the region above. Now the number of lattice points in T_1 above the point $(k, 0)$ are $\lfloor \frac{kq}{p} \rfloor$, so the total number of points in T_1 is $\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor$. Similarly in T_2 the total number of lattice points is $\sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor$, hence we must have that

$$\frac{p-1}{2}\frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor.$$

The result now follows from the previous lemma. $\square$