A shortened classical proof of the quadratic reciprocity law

Wouter Castryck*

Abstract

We present a short and conceptual proof of Gauss' quadratic reciprocity law. It is an optimized version of V.A. Lebesgue's 1838 proof computing the number of solutions to $x_1^2 + x_2^2 + \cdots + x_p^2 \equiv 1 \bmod q$.

Let p, q be distinct odd prime numbers. The law of quadratic reciprocity states that

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

where $\left(\frac{\cdot}{\cdot}\right)$ is the Legendre symbol. In 1838, V.A. Lebesgue gave a proof by determining the number of solutions to $x_1^2+x_2^2+x_3^2+\cdots+x_p^2 \equiv 1 \bmod q$ in two different ways (see Lebesgue's original paper [1] or Lemmermeyer's book for a related proof and more references [2, Exercise 1.25]). One way – the analogue of our first way below – was rather technical. Below, we get around this by working instead with an alternating sum $x_1^2 - x_2^2 + x_3^2 - \cdots + x_p^2$. The result is a short and conceptual proof of quadratic reciprocity.

First, for any odd $n \in \mathbb{N}$, denote by N_n the number of solutions in $(\mathbb{Z}/(q))^n$ to the equation

$$x_1^2 - x_2^2 + x_3^2 - \cdots + x_n^2 = 1.$$

If we substitute $x_1 \leftarrow x_1 + x_2$ we get

$$x_1^2 + x_3^2 - \cdots + x_n^2 - 1 = -2x_1x_2.$$

For any non-zero x_1-value and any value of $x_3, \ldots, x_n$, there is a unique corresponding x_2-value. If $x_1 = 0$, there are no solutions, except if $x_3^2 - \cdots + x_n^2 = 1$ (which happens in N_{n-2} cases): then all possible values of x_2 do the job. We find that

$$N_n = q^{n-2}(q-1) + qN_{n-2},$$

and hence $N_n = q^{n-1} + q^{\frac{n-1}{2}}(N_1 - 1) = q^{n-1} + q^{\frac{n-1}{2}}$. In particular, $N_p \equiv 1 + \left(\frac{q}{p}\right) \bmod p$.

Next, N_p can be classically determined as

$$\sum_{t_1+\cdots+t_p=1} N(x_1^2 = t_1)N(x_2^2 = -t_2)N(x_3^2 = t_3)\cdots N(x_p^2 = t_p),$$

*Research assistant of the Fund for Scientific Research - Flanders (FWO - Vlaanderen)

where the t_i are in $\mathbb{Z}/(q)$ and $N(\dots)$ denotes the number of solutions to the corresponding univariate equation. This can be rewritten as

$$\sum_{t_1+\cdots+t_p=1} \left(1+\left(\frac{t_1}{q}\right)\right)\left(1+\left(\frac{-t_2}{q}\right)\right)\left(1+\left(\frac{t_3}{q}\right)\right)\cdots\left(1+\left(\frac{t_p}{q}\right)\right).$$

When expanding out the product, only the terms $1\cdot 1\cdot 1\cdots 1$ and $\left(\frac{t_1}{q}\right)\cdot\left(\frac{-t_2}{q}\right)\cdot\left(\frac{t_3}{q}\right)\cdots\left(\frac{t_p}{q}\right)$ should be taken into consideration; the other terms disappear because Legendre symbols sum up to zero, i.e. $\sum_{t\in\mathbb{Z}/(q)}\left(\frac{t}{q}\right)=0$. Therefore, the above expression simplifies to

$$q^{p-1}+\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\sum_{t_1+\cdots+t_p=1}\left(\frac{t_1t_2t_3\dots t_p}{q}\right).$$

Now modulo p, the latter sum almost completely vanishes, since the tuples $(t_1,\dots,t_p)$ satisfying $t_1+\cdots+t_p=1$ with not all t_i equal to p^{-1} can be collected in groups of size p by shifting. Note that p is indeed a multiplicative unit in $\mathbb{Z}/(q)$. We thus obtain

$$N_p \equiv 1+\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p^{-p}}{q}\right) \equiv 1+(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right) \mod p.$$

The last congruence follows from the well-known formula $\left(\frac{a}{q}\right)\equiv a^{\frac{q-1}{2}} \mod q$ (which in the case $a=-1$ becomes an exact equality) and the obvious observation that p^{-p} is a square in $\mathbb{Z}/(q)$ if and only if p is a square in $\mathbb{Z}/(q)$.

By comparing, the reciprocity law follows.

References

[1] V. A. Lebesgue, *Recherches sur les nombres*, J. Math. Pure Appl. **3**, pp. 113-144 (1838)

[2] F. Lemmermeyer, *Reciprocity Laws. From Euler to Eisenstein*, Springer Monographs in Math. (2000)

Wouter Castryck
Department of Mathematics
K.U. Leuven
Celestijnenlaan 200B
B-3001 Leuven (Heverlee)
e-mail address: `wouter.castryck@wis.kuleuven.be`