THE JACOBI-LEGENDRE PROOF OF THE LAW OF QUADRATIC RECIPROCITY

STEVEN H. WEINTRAUB

ABSTRACT. We present an exposition of a proof of the Law of Quadratic Reciprocity due to Jacobi, with a simplification by Legendre.

Fix a prime p. The quadratic residue character χ modulo p is defined as follows: For an integer k relatively prime to p, $\chi(k) = 1$ if k is a quadratic residue (mod p) and $\chi(k) = -1$ if k is a quadratic nonresidue (mod p). We immediately see that $\chi(k) = (k/p)$, where the right-hand side denotes the Legendre symbol. We recall Euler's theorem that for any k relatively prime to p, $\chi(k) \equiv k^{(p-1)/2} \pmod{p}$. (In particular, $\chi(-1) = (-1)^{(p-1)/2}$, so $\chi(-1) = 1$ and -1 is a quadratic residue (mod p) if $p \equiv 1 \pmod{4}$, while $\chi(-1) = -1$ and -1 is a quadratic nonresidue (mod p) if $p \equiv -1 \pmod{4}$.)

Let $\zeta = \exp(2\pi i/p)$. We consider the *Gauss sum*

$$S = \sum_{k=1}^{p-1} \chi(k)\zeta^k.$$

Lemma 1. *(Gauss)*

$$S^2 = p\chi(-1)$$

Proof.

$$S^2 = \sum_{k=1}^{p-1}\sum_{j=1}^{p-1} \chi(k)\zeta^k\chi(j)\zeta^j = \sum_{k=1}^{p-1}\sum_{j=1}^{p-1} \chi(kj)\zeta^{k+j}.$$

Set $j \equiv km \pmod{p}$ and notice that as j runs over the nonzero congruence classes mod p, so does m. Also, $\chi(kj) = \chi(k^2m) = \chi(m)$. Thus

$$S^2 = \sum_{k=1}^{p-1}\sum_{m=1}^{p-1} \chi(m)\zeta^{k+km} = \sum_{m=1}^{p-1} \chi(m) \sum_{k=1}^{p-1} (\zeta^{1+m})^k.$$

Now $1+\zeta+\cdots+\zeta^{p-1} = 0$, so as long as $m \neq p-1$, the inner sum is -1. If $m = p-1$, then the inner sum is of course $p-1$.

Thus

$$S^2 = \left(-\sum_{m=1}^{p-2} \chi(m) \right) + (p-1)\chi(p-1).$$

2000 *Mathematics Subject Classification.* 11A15, Secondary 01A55.
Key words and phrases. Quadratic reciprocity, Jacobi, Legendre.

But $\sum_{m=1}^{p-1} \chi(m) = 0$, so the first term is $+\chi(p-1)$ and we see

$$S^2 = p\chi(-1)$$

as required. □

Theorem 2. *(The Law of Quadratic Reciprocity) Let p and q be distinct odd primes. Then*

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

Proof. By the multinomial theorem,

$$S^q = \sum_{k=1}^{p-1} \chi(k)^q \zeta^{kq} + \text{terms of the form } qA\zeta^x$$

where A is an integer, as is x. Let us write this as

$$S^q = T + qU.$$

Now

$$T = \sum_{k=1}^{p-1} \chi(k)\zeta^{kq}$$

and then

$$\begin{aligned} T = \chi(q)^2 T &= \chi(q) \sum_{k=1}^{p-1} \chi(q)\chi(k)\zeta^{kq} \\ &= \chi(q) \sum_{k=1}^{p-1} \chi(kq)\zeta^{kq} = \chi(q)S \end{aligned}$$

since this last sum is simply a reordering of the terms in the sum for S.

Thus

$$S^q = \chi(q)S + qU$$

so

$$S^{q-1} - \chi(q) = q(U/S).$$

The left-hand side is an integer, so the right-hand side must be an integer as well. But

$$q(U/S) = q(US/S^2) = q(US/(\chi(-1)p))$$

and, since p and q are relatively prime, U/S must be an integer[1]. We thus see that

$$S^{q-1} \equiv \chi(q) \pmod{q}.$$

[1] by Euclid's Lemma

Now

$$\begin{aligned} S^{q-1} &= (S^2)^{(q-1)/2} = (\chi(-1)p)^{(q-1)/2} = \chi(-1)^{(q-1)/2}p^{(q-1)/2} \\ &\equiv ((-1)^{(p-1)/2})^{(q-1)/2}\chi'(p) \pmod{q} \end{aligned}$$

where χ' denotes the quadratic residue character modulo q, by Euler's theorem. Thus we obtain

$$\chi(q) \equiv (-1)^{((p-1)/2)((q-1)/2)}\chi'(p) \pmod{q}$$

and since each side of this congruence is equal to ± 1, they must be equal. □

Gauss sums were introduced by Gauss, who not only proved the easy Lemma 1, but in fact determined the exact value of S (i.e., resolved the ambiguity of sign in taking $\sqrt{S^2}$), this being a celebrated theorem of his. Jacobi gave a proof of the Law of Quadratic Reciprocity in [1], using the value of S. Legendre realized that the proof could be simplified to only use the value of S^2, and gave this proof in [2, par. (679)]. This paper is an exposition of this proof. All the ideas are there, but we have rewritten the proof to be more accessible to the modern reader. (In particular, our use of the quadratic residue character is an anachronism.)

REFERENCES

[1] C. G. J. Jacobi, Letter to Legendre of 5 August 1827, in *Collected Works*, vol. I, C. W. Borchardt, ed., Chelsea, New York, 1969, 390–396; reprint of the original edition, G. Reimer, Berlin, 1881.

[2] A. M. Legendre, *Théorie des Nombres*, Tomes I et II, Paris 1830. (Available in German translation in *Zahlentheorie von Adrien-Marie Legendre*, (trans. H. Maser), Michigan Historical Reprint Series, University of Michigan Library.)

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PA 18015-3174, USA
E-mail address: shw2@lehigh.edu