Evaluation of Certain Legendre Symbols

David Angell

Abstract. We state and prove an apparently hitherto unrecorded evaluation of certain Legendre symbols: if p is prime, $p \neq 2$, and $ab = p - 1$, then the Legendre symbol $\left(\frac{b}{p}\right)$ is given by

$$\left(\frac{b}{p}\right) = (-1)^{\lceil a/2 \rceil \lfloor b/2 \rfloor}.$$

1. INTRODUCTION. Suppose that p is prime, $p \neq 2$, and b is not a multiple of p (these conditions will apply throughout this note). We say that b is a *quadratic residue* modulo p if the congruence $x^2 \equiv b \pmod{p}$ has a solution, and we define the *Legendre symbol*

$$\left(\frac{b}{p}\right) = \begin{cases} 1 & \text{if } b \text{ is a quadratic residue modulo } p \\ -1 & \text{if not.} \end{cases}$$

Many elementary results are known which facilitate the efficient evaluation of Legendre symbols; the present note offers a very elegant equality which appears to have escaped notice.

We begin with **Gauss' lemma**, which may be formulated as follows. A proof will be found in almost any standard number theory text and therefore none is given here.

Lemma (Gauss, 1808). *Suppose that p is prime, $p \neq 2$, and b is not a multiple of p. For $k = 1, 2, \ldots, (p-1)/2$, write $m_k = kb$, and let $\overline{m}_k$ be the least positive residue of m_k modulo p. Then*

$$\left(\frac{b}{p}\right) = (-1)^n,$$

where n is the number of k for which $\overline{m}_k$ exceeds $(p-1)/2$.

The Legendre symbol $\left(\frac{b}{p}\right)$ may be evaluated systematically by means of the following algorithm, though commonly the attentive calculator will find many short cuts. First reduce b modulo p, so that we may assume $0 < b < p$; then factor b as a product of primes and use the total multiplicativity of the Legendre symbol,

$$\left(\frac{b}{p}\right) = \left(\frac{b_1 b_2 \cdots b_k}{p}\right) = \left(\frac{b_1}{p}\right)\left(\frac{b_2}{p}\right) \cdots \left(\frac{b_k}{p}\right).$$

On the right-hand side, any Legendre symbols with $b_j = 2$ are found from the result

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}; \end{cases}$$

http://dx.doi.org/10.4169/amer.math.monthly.119.08.690
MSC: Primary 11A15

for other (prime) values of b_j we apply the celebrated *theorem of quadratic reciprocity* to write

$$\left(\frac{b_j}{p}\right) = -\left(\frac{p}{b_j}\right) \text{ if } b_j \equiv p \equiv 3 \pmod 4, \quad \text{and } \left(\frac{b_j}{p}\right) = \left(\frac{p}{b_j}\right) \text{ otherwise.}$$

We now have a product of Legendre symbols in which all the "denominators" b_j are less than the original p, and following the same procedure recursively will ultimately complete the evaluation.

2. A CONSEQUENCE OF GAUSS' LEMMA. In an undergraduate number theory class, a worked example on evaluating Legendre symbols came down to the question of finding $\left(\frac{10}{31}\right)$. A student, Daniel Apin, proposed using Gauss' lemma to evaluate this. I demurred, suggesting that it would be easier to begin with the equality $\left(\frac{10}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{5}{31}\right)$. Daniel pointed out, however, that the first fifteen multiples of 10, when reduced modulo 31, form a clear and simple pattern

$$10, 20, 30, 9, 19, 29, 8, 18, 28, 7, 17, 27, 6, 16, 26$$

which makes it very easy to apply Gauss' lemma and obtain $\left(\frac{10}{31}\right) = (-1)^{10} = 1$. The present note generalises this observation.

Theorem. *Suppose that p is prime, $p \neq 2$, and a, b are positive integers with $ab = p - 1$. Then*

$$\left(\frac{b}{p}\right) = (-1)^{\lceil a/2 \rceil \lfloor b/2 \rfloor}, \tag{1}$$

where for any real number x we write $\lceil x \rceil$ for the least integer $n \geq x$ and $\lfloor x \rfloor$ for the greatest integer $n \leq x$.

Proof. We use Gauss' lemma, considering the numbers $m_k = kb$ for $k = 1, 2, \dots, ab/2$ (of course ab is even). Dividing each k by a to obtain a slightly unconventional quotient and remainder, we have $k = aq + r$ with

$$q = 0, 1, 2, \dots, \left\lfloor \frac{b}{2} \right\rfloor - 1 \quad \text{and} \quad r = 1, 2, \dots, a$$

or

$$q = \left\lfloor \frac{b}{2} \right\rfloor \quad \text{and} \quad r = 1, 2, \dots, \frac{ab}{2} - a\left\lfloor \frac{b}{2} \right\rfloor.$$

The latter case occurs only if b is odd and then we have

$$r \leq \frac{ab}{2} - a\left(\frac{b-1}{2}\right) = \frac{a}{2}.$$

Reducing $m_k = (aq + r)b$ modulo p gives

$$\overline{m}_k = rb - q,$$

observing that the right-hand side is indeed the least positive residue of m_k because it satisfies the inequalities

$$rb - q \ge b - \left\lfloor \frac{b}{2} \right\rfloor \ge 0 \quad \text{and} \quad rb - q \le ab < p.$$

Now if $r \le a/2$ then

$$\overline{m}_k \le \frac{ab}{2} - q \le \frac{ab}{2} = \frac{p-1}{2},$$

while if $r > a/2$ then

$$\overline{m}_k \ge \left(\frac{a}{2} + \frac{1}{2}\right) b - q > \left(\frac{a}{2} + \frac{1}{2}\right) b - \left\lfloor \frac{b}{2} \right\rfloor \ge \frac{ab}{2} = \frac{p-1}{2},$$

noting that the second inequality is strict since this case never occurs for $q = \lfloor b/2 \rfloor$. So the number of multiples of b for which $\overline{m}_k > (p-1)/2$ is

$$\left(a - \left\lfloor \frac{a}{2} \right\rfloor\right) \left\lfloor \frac{b}{2} \right\rfloor = \left\lceil \frac{a}{2} \right\rceil \left\lfloor \frac{b}{2} \right\rfloor,$$

and the result follows. ■

3. COROLLARIES. Various standard and almost standard results can be proved anew by using this theorem. First,

$$\left(\frac{-1}{p}\right) = \left(\frac{p-1}{p}\right) = (-1)^{\lceil 1/2 \rceil \lfloor (p-1)/2 \rfloor} = (-1)^{(p-1)/2}.$$

This is usually proved as an immediate consequence of Euler's criterion

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}.$$

Next,

$$\left(\frac{2}{p}\right) = (-1)^{\lceil (p-1)/4 \rceil} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8). \end{cases}$$

The latter equality follows from the former by considering separately the four possibilities for p modulo 8. That we can easily deduce this from (1) is not surprising, as the customary proof employs Gauss' lemma in much the same way as we did in our proof of (1). Furthermore, if $b = 4k + 1$ is a factor of $p - 1$ then

$$\left(\frac{b}{p}\right) = (-1)^{\lceil a/2 \rceil (2k)} = 1;$$

this result is immediately clear from quadratic reciprocity if b is prime, but takes a moment's thought if not. Finally, if $4k$ is a factor of $p - 1$ then

$$\left(\frac{k}{p}\right) = \left(\frac{4k}{p}\right) = (-1)^{\lceil a/2 \rceil (2k)} = 1,$$

which again may alternatively be proved by using quadratic reciprocity and the known value of $\left(\frac{2}{p}\right)$.

To conclude, we show that our main theorem also holds for negative values of a and b. First, if a, b are any integers then

$$\left\lceil \frac{a}{2} \right\rceil \left\lfloor \frac{b}{2} \right\rfloor - \left\lceil \frac{-a}{2} \right\rceil \left\lfloor \frac{-b}{2} \right\rfloor \tag{2}$$

is even if ab is a multiple of 4, odd if ab is a multiple of 2 but not of 4. To see this write

$$a = 2c + x, \quad b = 2d + y,$$

where c, d are integers and $x, y \in \{0, 1\}$. Then the expression (2) is

$$(c + x)d - (-c)(-d - y) = dx - cy.$$

If ab is a multiple of 4 then either $x = y = 0$; or $x = 0$, c is even; or $y = 0$, d is even. In each case (2) is even. If ab is a multiple of 2 but not of 4, then either $x = 0$, c is odd, $y = 1$; or $x = 1$, d is odd, $y = 0$. In each case (2) is odd, and our first claim is proved. Consequently, if a, b are negative and $ab = p - 1$, then

$$\left\lceil \frac{a}{2} \right\rceil \left\lfloor \frac{b}{2} \right\rfloor - \left\lceil \frac{-a}{2} \right\rceil \left\lfloor \frac{-b}{2} \right\rfloor \quad \text{and} \quad \frac{p-1}{2}$$

have the same parity and so

$$\left(\frac{b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{-b}{p}\right) = (-1)^{(p-1)/2}(-1)^{\lceil -a/2 \rceil \lfloor -b/2 \rfloor} = (-1)^{\lceil a/2 \rceil \lfloor b/2 \rfloor},$$

as we have already shown for positive a and b.

School of Mathematics and Statistics, University of New South Wales, Sydney 2052, Australia
david.angell@unsw.edu.au

An Elementary Counterexample in the Compact-Open Topology

Jonathan Groves

Abstract. We give a short proof that the space of continuous functions from [0, 1] to [0, 1] is not compact in the compact-open topology.

Suppose X and Y are compact topological spaces. Let $\mathcal{C}(X, Y)$ be the space of continuous functions from X to Y, and give this space the compact-open topology. An interesting problem from topology is to prove or disprove that $\mathcal{C}(X, Y)$ is compact.

http://dx.doi.org/10.4169/amer.math.monthly.119.08.693
MSC: Primary 54C35