THE JACOBI SYMBOL AND A METHOD OF EISENSTEIN FOR CALCULATING IT

STEVEN H. WEINTRAUB

ABSTRACT. We present an exposition of the basic properties of the Jacobi symbol, with a method of calculating it due to Eisenstein.

Fix a prime p. For an integer a relatively prime to p the Legendre symbol is defined by $(a/p) = 1$ if a is a quadratic residue (mod p) and $(a/p) = -1$ if a is a quadratic nonresidue (mod p). We recall Euler's theorem that $(a/p) \equiv a^{(p-1)/2} \pmod{p}$.

We have the famous Law of Quadratic Reciprocity:

Theorem 1. *(The Law of Quadratic Reciprocity) Let p and q be distinct odd primes. Then*

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

We also recall the following, where (a) follows directly from Euler's theorem and (b) follows directly from Gauss's Lemma.

Theorem 2. *(Supplement to the Law of Quadratic Reciprocity) Let p be an odd prime. Then (1)*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$
$$= 1 \text{ if } p \equiv 1 (\mathrm{mod}\, 4) \text{ and } = -1 \text{ if } p \equiv -1 (\mathrm{mod}\, 4),$$

(2)

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$
$$= 1 \text{ if } p \equiv \pm 1 (\mathrm{mod}\ 8) \text{ and } = -1 \text{ if } p \equiv \pm 3 (\mathrm{mod}\ 8).$$

We often regard these results as providing a method for calculating Legendre symbols.

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

Example 3. We wish to calculate $(4661/9901)$. We have:

$$\begin{aligned}\left(\frac{4661}{9901}\right) &= \left(\frac{59\cdot 79}{9901}\right)\\ &= \left(\frac{59}{9901}\right)\left(\frac{79}{9901}\right)\\ &= \left(\frac{9901}{59}\right)\left(\frac{9901}{79}\right)\\ &= \left(\frac{48}{59}\right)\left(\frac{26}{79}\right)\\ &= \left(\frac{3}{59}\right)\left(\frac{2}{79}\right)\left(\frac{13}{79}\right)\\ &= (-1)\left(\frac{59}{3}\right)(+1)\left(\frac{79}{13}\right)\\ &= (-1)\left(\frac{2}{3}\right)(+1)\left(\frac{1}{13}\right)\\ &= (-1)(-1)(+1)(+1) = 1.\end{aligned}$$

Note the first step in this example required us to factor 4661. In general, factorization is difficult, so this is not an effective method for calculating Legendre symbols. We now introduce Jacobi symbols, which generalize Legendre symbols. In addition to their own intrinsic interest, they enable us to compute Legendre symbols without having to factor integers.

Definition 4. Let b be a positive odd integer, and suppose that $b = b_1 \cdots b_\ell$, a product of (not necessarily distinct) primes. For an integer a relatively prime to b, the *Jacobi symbol* (a/b) is defined to be the product

$$\left(\frac{a}{b}\right) = \left(\frac{a}{b_1}\right)\cdots\left(\frac{a}{b_\ell}\right).$$

If $b = 1$, then $(a/b) = 1$.

We now derive basic properties of the Jacobi symbol. First, we need a lemma from elementary number theory.

Lemma 5. *Let u and v be odd integers. Then*

$$\frac{uv-1}{2} \equiv \frac{u-1}{2} + \frac{v-1}{2} \pmod 2$$

and

$$\frac{(uv)^2-1}{8} \equiv \frac{u^2-1}{8} + \frac{v^2-1}{8} \pmod 2.$$

Proof. We simply calculate

$$\frac{uv-1}{2} - \left[\frac{u-1}{2} + \frac{v-1}{2}\right] = \frac{uv-u-v+1}{2} = \frac{(u-1)(v-1)}{2},$$

which is always even, and similarly

$$\frac{(uv)^2-1}{8} - \left[\frac{u^2-1}{8} + \frac{v^2-1}{8}\right] = \frac{(uv)^2-u^2-v^2+1}{8} = \frac{(u^2-1)(v^2-1)}{8},$$

which is also always even. □

Theorem 6. *(Properties of the Jacobi symbol)*

(1) If b is a prime, the Jacobi symbol (a/b) is the Legendre symbol (a/b).

(2) If $(a/b) = -1$, then a is not a quadratic residue (mod b). *The converse need not hold if b is not a prime.*

(3) $(aa'/bb') = (a/b)(a/b')(a'/b)(a'/b')$ if aa' and bb' are relatively prime.

(4) $(a^2/b) = (a/b^2) = 1$ if a and b are relatively prime.

(5) $(-1/b) = (-1)^{\frac{b-1}{2}} = 1$ if $b \equiv 1 (\mathrm{mod}\, 4)$ and $= -1$ if $b \equiv -1 (\mathrm{mod}\, 4)$.

(6) $(2/b) = (-1)^{\frac{b^2-1}{8}} = 1$ if $b \equiv \pm 1 (\mathrm{mod}\ 8)$ and $= -1$ if $b \equiv \pm 3 (\mathrm{mod}\ 8)$.

(7) If a and b are relatively prime odd positive integers, then

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

Proof. Parts (1) through (4) are straightforward.

We prove part (5) by induction on the number of prime factors ℓ of b. The critical case is $\ell = 2$. Thus let $b = b_1 b_2$, with b_1 and b_2 each prime. In this case the left-hand side is

$$\left(\frac{-1}{b}\right) = \left(\frac{-1}{b_1 b_2}\right) = \left(\frac{-1}{b_1}\right)\left(\frac{-1}{b_2}\right) = (-1)^{\frac{b_1-1}{2}}(-1)^{\frac{b_2-1}{2}} = (-1)^{\frac{b_1-1}{2}+\frac{b_2-1}{2}}$$

while the right-hand side is

$$(-1)^{\frac{b-1}{2}} = (-1)^{\frac{b_1 b_2-1}{2}}$$

and these are equal.

We prove part (6) similarly. Again let $b = b_1 b_2$, with b_1 and b_2 each prime. In this case the left-hand side is

$$\left(\frac{2}{b}\right) = \left(\frac{2}{b_1 b_2}\right) = \left(\frac{2}{b_1}\right)\left(\frac{2}{b_2}\right) = (-1)^{\frac{b_1^2-1}{8}}(-1)^{\frac{b_2^2-1}{8}} = (-1)^{\frac{b_1^2-1}{8}+\frac{b_2^2-1}{8}}$$

while the right-hand side is

$$(-1)^{\frac{b^2-1}{8}} = (-1)^{\frac{b_1^2 b_2^2-1}{8}}$$

and these are equal.

For part (7), let $a = a_1 \cdots a_k$ and $b = b_1 \cdots b_\ell$, products of primes. Then, by the Law of Quadratic Reciprocity,

$$\begin{aligned}\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) &= \prod_{i,j}\left(\frac{a_i}{b_j}\right)\left(\frac{b_j}{a_i}\right)\\ &= \prod_{i,j}(-1)^{\frac{a_i-1}{2}\cdot\frac{b_j-1}{2}} = (-1)^{\varepsilon}\end{aligned}$$

with $\varepsilon = \sum_{i,j}\frac{a_i-1}{2}\cdot\frac{b_j-1}{2}$. But then

$$\begin{aligned}\varepsilon &= \sum_{i,j}\frac{a_i-1}{2}\cdot\frac{b_j-1}{2} = \sum_j\left[\sum_i\frac{a_i-1}{2}\right]\frac{b_j-1}{2}\\ &\equiv \sum_j\left[\frac{a-1}{2}\right]\frac{b_j-1}{2}\\ &= \left[\frac{a-1}{2}\right]\sum_j\frac{b_j-1}{2} \equiv \left[\frac{a-1}{2}\right]\left[\frac{b-1}{2}\right](\mathrm{mod}\ 2).\end{aligned}$$

□

Theorem 7. *Let a and b be relatively prime odd positive integers.*

(1) If $\varepsilon = \pm 1$, then

$$\left(\frac{\varepsilon a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{\varepsilon a-1}{2}\cdot\frac{b-1}{2}}.$$

(2) If $\varepsilon_1 = \pm 1$ and $\varepsilon_2 = \pm 1$, then

$$\left(\frac{\varepsilon_1 a}{b}\right)\left(\frac{\varepsilon_2 b}{a}\right) = (-1)^{\frac{\varepsilon_1 a-1}{2}\cdot\frac{\varepsilon_2 b-1}{2}+\frac{\varepsilon_1-1}{2}\cdot\frac{\varepsilon_2-1}{2}}.$$

Proof. (1) If $\varepsilon = 1$ there is nothing more to prove. Let $\varepsilon = -1$. Then

$$\begin{aligned}\left(\frac{\varepsilon a}{b}\right)\left(\frac{b}{a}\right) &= \left(\frac{-a}{b}\right)\left(\frac{b}{a}\right) = \left(\frac{-1}{b}\right)\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)\\ &= (-1)^{\frac{b-1}{2}}(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} = (-1)^x\end{aligned}$$

where $x = \frac{b-1}{2} + \frac{a-1}{2}\cdot\frac{b-1}{2} = \frac{a+1}{2}\cdot\frac{b-1}{2}$.

On the other hand, in this case,

$$(-1)^{\frac{\varepsilon a-1}{2}\cdot\frac{b-1}{2}} = (-1)^{\frac{-a-1}{2}\cdot\frac{b-1}{2}} = (-1)^y$$

where $y = \frac{-a-1}{2}\cdot\frac{b-1}{2} = -\frac{a+1}{2}\cdot\frac{b-1}{2} = -x$, and $y \equiv x \pmod 2$.

(2) The only new case here is $\varepsilon_1 = \varepsilon_2 = -1$, so suppose that is the case. Then the left-hand side is

$$\begin{aligned}\left(\frac{-a}{b}\right)\left(\frac{-b}{a}\right) &= \left(\frac{-1}{a}\right)\left(\frac{-1}{b}\right)\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)\\ &= (-1)^{\frac{a-1}{2}}(-1)^{\frac{b-1}{2}}(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}} = (-1)^x,\end{aligned}$$

where, setting $u = \frac{a-1}{2}$ and $v = \frac{b-1}{2}$, $x = uv+u+v$.

In this case the right-hand side is

$$(-1)^{\frac{-a-1}{2}\cdot\frac{-b-1}{2}+(-1)\cdot(-1)} = (-1)^{\frac{a+1}{2}\cdot\frac{b+1}{2}+1} = (-1)^y,$$

where $y = (u+1)(v+1)+1 = uv+u+v+2$, and $y \equiv x \pmod 2$. □

Remark 8. It is convenient to observe here that if $\varepsilon = \pm 1$, then

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

(If $\varepsilon = 1$ this is $(1/b) = 1$, which is trivial, and if $\varepsilon = -1$ this is $(-1/b) = (-1)^{\frac{b-1}{2}}$, which we know.)

We now come to Eisenstein's method of computing Jacobi symbols.

Theorem 9. *(Eisenstein [1]) Let b be a positive odd integer and let a be an odd integer that is relatively prime to b. Set $a_1 = a$, $a_2 = b$, and then*

$$\begin{aligned} a_1 &= a_2 q_1 + \varepsilon_1 a_3 \\ a_2 &= a_3 q_2 + \varepsilon_2 a_4 \\ &\dots \\ a_n &= a_{n+1} q_n + \varepsilon_n a_{n+2} \end{aligned}$$

with $a_2 > a_3 > \ldots > a_{n+2} = 1$, all a_i odd, and $\varepsilon_i = \pm 1$ for each i.

For each $i = 1, \ldots, n$, let

$$\begin{aligned} s_i &= 0 \text{ if at least one of } a_{i+1} \text{ and } \varepsilon_i a_{i+2} \equiv 1 (\mathrm{mod}\, 4), \\ &= 1 \text{ if both of } a_{i+1} \text{ and } \varepsilon_i a_{i+2} \equiv 3 (\mathrm{mod}\, 4). \end{aligned}$$

Let $t = \sum_{i=1}^{n} s_i$. Then

$$\left(\frac{a}{b}\right) = (-1)^t.$$

Proof. We have $(a/b) = (a_1/a_2)$. Now

$$\begin{aligned} \left(\frac{a_1}{a_2}\right) = \left(\frac{\varepsilon_1 a_3}{a_2}\right) &= (-1)^{\frac{\varepsilon_1 a_3 - 1}{2} \cdot \frac{a_2 - 1}{2}} \left(\frac{a_2}{a_3}\right) = (-1)^{s_1} \left(\frac{a_2}{a_3}\right) \\ \left(\frac{a_2}{a_3}\right) = \left(\frac{\varepsilon_2 a_4}{a_3}\right) &= (-1)^{\frac{\varepsilon_2 a_4 - 1}{2} \cdot \frac{a_3 - 1}{2}} \left(\frac{a_3}{a_4}\right) = (-1)^{s_2} \left(\frac{a_3}{a_4}\right) \\ &\dots \\ \left(\frac{a_n}{a_{n+1}}\right) = \left(\frac{\varepsilon_n a_{n+2}}{a_{n+1}}\right) &= (-1)^{\frac{\varepsilon_n a_{n+2} - 1}{2} \cdot \frac{a_{n+1} - 1}{2}} = (-1)^{s_n} \end{aligned}$$

so

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{n} (-1)^{s_i} = (-1)^{\sum_{i=1}^{n} s_i} = (-1)^t.$$

□

Actually, it is not necessary to carry the computation all the way to the end.

Corollary 10. *In the situation of the above theorem, let $t_k = \sum_{i=1}^{k} s_i$. Then for any $k \leq n$*

$$\left(\frac{a}{b}\right) = (-1)^{t_k} \left(\frac{a_{k+1}}{a_{k+2}}\right).$$

Proof. Exactly the same. □

Example 11. We present several typical computations. The first is Eisenstein's illustration of his method.

(1) We compute $(773/343)$.

$$\begin{aligned} 773 &= 343 \cdot 2 + 87 && \text{so } s_1 = 1 \\ 343 &= 87 \cdot 4 - 5 && \text{so } s_2 = 1 \\ 87 &= 5 \cdot 18 - 3 && \text{so } s_3 = 0 \\ 5 &= 3 \cdot 2 - 1 && \text{so } s_4 = 1 \end{aligned}$$

Hence

$$\left(\frac{773}{343}\right) = (-1)^3 = -1.$$

(2) We compute $(4661/9901)$.

$$\begin{aligned} 4661 &= 9901 \cdot 0 + 4661 && \text{so } s_1 = 0 \\ 9901 &= 4661 \cdot 2 + 579 && \text{so } s_2 = 0 \\ 4661 &= 579 \cdot 8 + 29 && \text{so } s_3 = 0 \\ 579 &= 29 \cdot 20 - 1 && \text{so } s_4 = 0 \end{aligned}$$

Hence

$$\left(\frac{4661}{9901}\right) = (-1)^0 = 1.$$

(3) We compute $(10399/2341)$.

$$\begin{aligned} 10399 &= 2341 \cdot 4 + 1035 && \text{so } s_1 = 0 \\ 2341 &= 1035 \cdot 2 + 271 && \text{so } s_2 = 1 \\ 1035 &= 271 \cdot 4 - 49 && \text{so } s_3 = 1 \end{aligned}$$

Hence

$$\left(\frac{10399}{2341}\right) = (-1)^2 \left(\frac{49}{a_6}\right) = 1$$

as $49 = 7^2$.

Remark 12. We may speed up Eisenstein's algorithm. Suppose that we are using this algorithm and at some stage we arrive at (a_i/a_{i+1}). Write $a_i = a_{i+1}q'_i + \varepsilon_i 2^{e_i} a'_{i+2}$ where $\varepsilon_i = \pm 1$, $e_i > 0$, $2^{e_i} a'_{i+2} < a_{i+1}$, and a'_{i+2} is a positive odd number. Then $(a_i/a_{i+1}) = (2^{e_i}/a_{i+1})(\varepsilon_i a'_{i+2}/a_{i+1})$, and the first factor is easy to compute. Note that $a_{i+2} < \frac{1}{2}a_{i+1}$. Hence we see that this modified algorithm reduces the "denominator" of the Jacobi symbol by a factor of at least 2 every step, ensuring that it ends quickly.

It turns out that sometimes the choice of odd remainder leads to the smaller value of a_{i+2}, and sometimes the choice of even remainder does, so the most efficient way to proceed is to choose whichever one yields the smaller value.

We thus obtain the following modified algorithm:

Theorem 13. *Let b be a positive odd integer and let a be an integer that is relatively prime to b. Set $a_1 = a$, $a_2 = b$, and then, assuming that a_i and a_{i+1} are defined, set*

$$a_i = a_{i+1}q'_i + \varepsilon'_i a'_{i+2},$$
$$a_i = a_{i+1}q''_i + \varepsilon''_i 2^{e_i} a''_{i+2}$$

with a'_{i+2} and a''_{i+2} positive odd integers, $e_i > 0$, $a'_{i+2} < a_{i+1}$, $2^{e_i} a''_{i+2} < a_{i+1}$, $\varepsilon'_i = \pm 1$, and $\varepsilon''_i = \pm 1$.

If $a'_{i+2} \leq a''_{i+2}$, set $a_{i+2} = a'_{i+2}$, $\varepsilon_i = \varepsilon'_i$, and $r_i = 0$.

If $a''_{i+2} < a'_{i+2}$, set $a_{i+2} = a''_{i+2}$, $\varepsilon_i = \varepsilon''_i$, and set $r_i = 0$ if e_i is even or $a_{i+1} \equiv \pm 1 \pmod 8$ and $r_i = 1$ if e_i is odd and $a_{i+1} \equiv \pm 3 \pmod 8$.

Set $s_i = 0$ if at least one of a_{i+1} and $\varepsilon_i a_{i+2} \equiv 1 \pmod 4$, and $s_i = 1$ if both of a_{i+1} and $\varepsilon_i a_{i+2} \equiv 3 \pmod 4$.

Let $u_k = \sum_{i=1}^{k} (r_i + s_i)$. Then

$$\left(\frac{a_1}{a_2}\right) = (-1)^{u_k} \left(\frac{a_{k+1}}{a_{k+2}}\right).$$

In particular, if $a_{n+2} = 1$,

$$\left(\frac{a_1}{a_2}\right) = (-1)^{u_n}.$$

Example 14. The computation of $(32767/99989)$ by Eisenstein's original algorithm takes 38 steps. We compute $(32767/99989)$ using this faster algorithm.

$$\begin{aligned}
32767 &= 99989 \cdot 0 + 32767 && \text{so } r_1 = 0,\ s_1 = 0\\
99989 &= 32767 \cdot 3 + 2^3 \cdot 211 && \text{so } r_2 = 0,\ s_2 = 1\\
32767 &= 211 \cdot 155 + 2 \cdot 31 && \text{so } r_3 = 1,\ s_3 = 1\\
211 &= 31 \cdot 7 - 2 \cdot 3 && \text{so } r_4 = 0,\ s_4 = 0\\
31 &= 3 \cdot 10 + 1 && \text{so } r_5 = 0,\ s_5 = 0
\end{aligned}$$

Hence

$$\left(\frac{32767}{99989}\right) = (-1)^3 = -1.$$

Note that in the first step of this computation, we had the choice of using $32767 = 99989 \cdot 0 + 32767$ or $32767 = 99989 \cdot 1 - 2 \cdot 33611$ and we used the first of these. In the second step, we had the choice of using $99989 = 32767 \cdot 4 - 31079$ or $99989 = 32767 \cdot 3 + 2^3 \cdot 211$ and we used the second of these.

Example 15. We compute $(-12034/84331)$.

$$\begin{aligned}
-12034 &= 84331 \cdot 0 - 2 \cdot 6017 && \text{so } r_1 = 1,\ s_1 = 1\\
84331 &= 6017 \cdot 14 + 93 && \text{so } r_2 = 0,\ s_2 = 0\\
6017 &= 93 \cdot 65 - 2^2 \cdot 7 && \text{so } r_3 = 0,\ s_3 = 0\\
93 &= 7 \cdot 13 + 2 \cdot 1 && \text{so } r_4 = 0,\ s_4 = 0
\end{aligned}$$

Hence

$$\left(\frac{-12034}{84331}\right) = (-1)^2 = 1.$$

Remark 16. Of course, any valid computation with Legendre symbols is also a valid computation with Jacobi symbols.

REFERENCES

[1] G. Eisenstein, Einfacher Algorithmus zur Bestimmung des Werthes von (a/b), J. reine angew. Math. 27 (1844), 317-318.

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