

Spring, 2009

## Quadratic Reciprocity

In the previous set of notes, we introduced the Legendre Symbol, defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a \\ 1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a quadratic non residue modulo } p. \end{cases}$$

We also had  $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ ,

and the special case

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv 3 \pmod{4}, \end{cases}$$

along with several other properties. In this set of notes, we prove Gauss's Law of Quadratic Reciprocity, which greatly simplifies the calculation of  $\left(\frac{a}{p}\right)$ .

**Theorem (Gauss's Criterion)** Let  $p$  be an odd prime and let  $a$  be a positive integer not divisible by  $p$ . For each positive integer  $k \leq \frac{p-1}{2}$ , let  $r$  be the least residue of  $ka \pmod{p}$ . That is,  $r$  is the unique integer such that  $0 < r < p$  and  $r \equiv ka \pmod{p}$ . Let  $t$  be the number of  $r$ 's for which  $\frac{p-1}{2} < r < p$ . Then  $\left(\frac{a}{p}\right) = (-1)^t$ .

Before we prove this theorem, we give some examples: Let  $p = 29$  and consider the three values of  $a$ :  $a = 3$ ,  $a = 4$ ,  $a = 7$ . In each case, we multiply the numbers less than  $\frac{29-1}{2} = 14$  by  $a$  and reduce  $\pmod{29}$ :

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	t
3k	3	6	9	12	15	18	21	24	27	1	4	7	10	13	5
4k	4	8	12	16	20	24	28	3	7	11	15	19	19	23	8
7k	7	14	21	28	6	13	20	27	5	12	19	26	4	11	6

From the table, we see that  $t = 5$  if  $a = 3$ ,  $t = 8$  if  $a = 4$ , and  $t = 6$  if  $a = 7$ . Thus, by the theorem,  $\left(\frac{3}{29}\right) = (-1)^5 = -1$ ,  $\left(\frac{4}{29}\right) = (-1)^8 = 1$ ,  $\left(\frac{7}{29}\right) = (-1)^6 = 1$ .

**Proof of theorem:** Let  $p = 2m + 1$ . Then there are  $m$  values for  $k$ . Let  $u_1, u_2, \dots, u_t$  be the remainders  $> m$ , and  $v_1, v_2, \dots, v_{m-t}$  be the remainders  $\leq m$ . For example, when  $p = 29$  and  $a = 7$ , from the bottom row of our table, the  $u$ 's are 21, 28, 20, 27, 19, 26 and the  $v$ 's are 7, 14, 6, 13, 5, 12, 4, 11, 6. Since  $k_1 a \equiv k_2 a$  if and only if  $k_1 \equiv k_2$ , which happens if and only if  $k_1 = k_2$  ( $k$  values all being less than  $p$ ), all the  $r$ 's are different. Thus, all the  $u$ 's are different, all the  $v$ 's are different. Now consider the list  $p - u_1, p - u_2, \dots, p - u_t, v_1, v_2, \dots, v_{m-t}$ . In our example, this would be the list: 8, 1, 9, 2, 10, 3, 7, 14, 6, 13, 5, 12, 4, 11. Note that the list in our example is a reordering of the numbers from 1 to  $m$ . We claim that this happens in general.

To verify the claim, by the remarks above, the only way for a repeat on the list is if  $p - u_i = v_j$  for some  $i$  and  $j$ . In this case,  $p = u_i + v_j \equiv ka + la \pmod{p}$  for some integers  $k, l$  (since the  $u$ 's and  $v$ 's are remainders  $r_k$ ) Thus,  $0 \equiv a(k + l) \pmod{p}$ . Since  $1 \leq k, l \leq m$ , and  $2m < p$ , so this can't happen. Thus, since these numbers are all different, each is between 1 and  $m$ , and there are  $m$  numbers total, it must be that  $p - u_1, p - u_2, \dots, p - u_t, v_1, v_2, \dots, v_{m-t}$  is a reordering of the numbers 1 to  $m$ .

Having verified the claim, if we multiply the things in the list together:

$$\begin{aligned} (p - u_1)(p - u_2) \cdots (p - u_t) v_1 \cdots v_{m-t} &\equiv (-u_1)(-u_2) \cdots (-u_t) v_1 v_2 \cdots v_{m-t} \\ &\equiv (-1)^t r_1 r_2 \cdots r_m \pmod{p} \\ &\equiv (-1)^t (a)(2a) \cdots (ma) \pmod{p} \\ &\equiv (-1)^t a^m m! \pmod{p}. \end{aligned}$$

But also,

$$(p - u_1)(p - u_2) \cdots (p - u_t)v_1 \cdots v_{m-t} \equiv 1 \cdot 2 \cdots m \pmod{p}.$$

Putting these together,

$$(-1)^t a^m m! \equiv m! \pmod{p}.$$

Canceling out the  $m!$  gives

$$(-1)^t a^m \equiv 1 \pmod{p},$$

or

$$\left(\frac{a}{p}\right) \equiv a^m \equiv (-1)^t \pmod{p},$$

and the theorem follows.

**Technical Lemma.**  $\left(\frac{a}{p}\right) = (-1)^n$ , where  $n = \sum_{k=1}^{(p-1)/2} \lfloor ka/p \rfloor + \frac{1}{8}(p^2 - 1)(a - 1)$ .

For example, if  $a = 6$ ,  $p = 19$ :  $n = \sum_{k=1}^9 \lfloor 6k/19 \rfloor = 0 + 0 + 0 + 1 + 1 + 1 + 2 + 2 + 2 = 9$ ,

and  $\frac{(p^2 - 1)(a - 1)}{8} = 45 \cdot 5 = 225$  so  $\left(\frac{6}{19}\right) = (-1)^{9 + 225} = 1$ .

**Proof of lemma.** For each  $k$ , we write  $ka = q_k p + r_k$ , with  $0 \leq r_k < p$ . Then  $\lfloor ka/p \rfloor = q_k$ .

If we add up  $a = q_1 p + r_1$ ,  $2a = q_2 p + r_2$ ,  $3a = q_3 p + r_3$ ,  $\dots$ ,  $ma = q_m p + r_m$  we have

$$(1 + 2 + \cdots + m)a = p(q_1 + q_2 + \cdots + q_m) + r_1 + r_2 + \cdots + r_m.$$

Now with notation as in the proof of the previous theorem,  $p - u_1, p - u_2, \dots, p - u_t, v_1, v_2, \dots, v_{m-t}$  is just a reordering of the numbers 1 through  $m$ . Thus, the sum of these numbers is just  $1 + 2 + \cdots + m$ . The sum of these numbers is also

$$\begin{aligned} & tp - u_1 - u_2 - \cdots - u_t + v_1 + v_2 + \cdots + v_{m-t} \\ &= tp + (u_1 + u_2 + \cdots + u_t + v_1 + v_2 + \cdots + v_{m-t}) - 2(u_1 + \cdots + u_t) \\ &= tp + (r_1 + r_2 + \cdots + r_m) - 2(u_1 + \cdots + u_t). \end{aligned}$$

Since  $p$  is odd, we have

$$1 + 2 + 3 + \cdots + m \equiv t + r_1 + r_2 + \cdots + r_m \pmod{2},$$

$$\text{or} \quad r_1 + r_2 + \cdots + r_m \equiv 1 + 2 + \cdots + m + t \pmod{2}.$$

$$\text{Now } 1 + 2 + 3 + \cdots + m = \frac{m(m+1)}{2} = \frac{p^2-1}{8}. \quad \text{Thus,}$$

$$\begin{aligned} \frac{p^2-1}{8} a &= p(q_1 + q_2 + \cdots + q_m) + r_1 + r_2 + \cdots + r_m \\ &\equiv p(q_1 + q_2 + \cdots + q_m) + \frac{p^2-1}{8} + t \pmod{2}, \end{aligned}$$

$$\text{so} \quad t \equiv \frac{p^2-1}{8} (a-1) - p(q_1 + q_2 + \cdots + q_m) \pmod{2},$$

$$\text{or} \quad t \equiv \frac{p^2-1}{8} (a-1) + q_1 + q_2 + \cdots + q_m = n \pmod{2}.$$

$$\text{Hence, } \left(\frac{a}{p}\right) = (-1)^t = (-1)^n.$$

Here is an important result that follows from the previous stuff:

$$\text{Corollary } \left(\frac{2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1, & \text{if } p \equiv 3 \text{ or } 5 \pmod{8} \end{cases} = (-1)^{\frac{p^2-1}{8}}.$$

**Proof 1.** I will give two proofs of this. First, using the technical lemma,  $\left(\frac{2}{p}\right) = (-1)^n$ ,

where  $n = \sum_{k=1}^{(p-1)/2} \lfloor 2k/p \rfloor + \frac{1}{8}(p^2-1)(2-1)$ . Since  $2k < p$  for all  $k$  between 1 and  $\frac{p-1}{2}$ , the sum contributes nothing, and we are left with  $n = \frac{p^2-1}{8}$ .

**Proof 2.** Alternatively, if we use Gauss's criterion directly, if  $p = 2m + 1$ . We must calculate  $2k \pmod{p}$  for each  $k \leq m$ . We get the numbers  $2, 4, 6, \dots, 2m$ . For example, when  $p = 11$ , our list is  $2, 4, 6, 8, 10$ . In this case, the last three numbers are greater than  $m$ . In general, the first bunch of numbers are  $\leq m$ , and the last bunch are  $> m$ . Since we want  $2k$

$> m$ , we have  $\frac{m}{2} < k \leq m$ . This gives a formula for the number of such  $k$ :

$$t = m - \lceil (m+1)/2 \rceil + 1.$$

To see what is going on here, look at  $p \pmod{8}$ :  $p = 8n + r$ , where  $r = 1, 3, 5, \text{ or } 7$ . In the first case,  $m = 4n$ , and  $t = 4n - (2n - 1) + 1 = 2n$ , which is even. If  $p = 8n + 3$ ,  $m = 4n + 1$ , and  $t = 4n + 1 - (2n + 1) + 1 = 2n + 1$ , which is odd, if  $p = 8n + 5$ ,  $m = 4n + 2$ , and  $t = 4n + 2 - (2n + 2) + 1 = 2n + 1$ , which is odd. Finally, if  $p = 8n + 7$ ,  $m = 4n + 3$ , so  $t = 4n + 3 - (2n + 2) + 1 = 2n + 2$ , which is even.  $\left(\frac{2}{p}\right) = 1$  when  $t$  is even. This happens when  $p = 8n + 1$  or  $p = 8n + 7$  and it is  $-1$  in the other two cases. Since  $\frac{p^2 - 1}{8}$  is also even for  $1, 7 \pmod{8}$  and odd for  $3, 5 \pmod{8}$ , the conclusion follows.

Gauss's criterion or the technical lemma could be used in general to determine  $\left(\frac{a}{p}\right)$  for all  $p$ , but this gets more and more tedious as  $a$  grows. Instead, Gauss used his criterion to prove a general, very powerful formula to handle these calculations with greater ease.

**Theorem** (The Law of Quadratic Reciprocity). Let  $p \neq q$  be two odd primes.

Then 
$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \text{ if } p \equiv 1 \pmod{4} \text{ or } q \equiv 1 \pmod{4},$$

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \text{ if both } p \text{ and } q \text{ are } \equiv 3 \pmod{4}.$$

If you like short formulas, this can be restated as:

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

For example, here are some calculations using the theorem:

$$\left(\frac{5}{19}\right) = \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2^2}{5}\right) = 1,$$

$$\left(\frac{37}{59}\right) = \left(\frac{59}{37}\right) = \left(\frac{12}{37}\right) = \left(\frac{4}{37}\right)\left(\frac{3}{37}\right) = \left(\frac{3}{37}\right) = \left(\frac{37}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

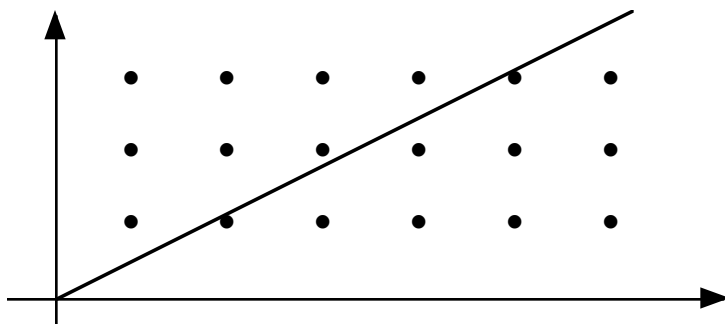
$$\left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{3^2-1}{8}} = -(-1)^1 = 1,$$

$$\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -1,$$

$$\begin{aligned} \left(\frac{53}{3581}\right) &= \left(\frac{3581}{53}\right) = \left(\frac{30}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{3}{53}\right)\left(\frac{5}{53}\right) = (-1)^{\frac{53^2-1}{2}} \left(\frac{53}{3}\right)\left(\frac{53}{5}\right) \\ &= -\left(\frac{2}{3}\right)\left(\frac{3}{5}\right) = (-1)(-1)(-1) = -1, \text{ etc.} \end{aligned}$$

Quadratic Reciprocity can be proved directly from Gauss's criterion. However, the introduction of the technical lemma speeds up the proof.

**Proof of theorem:** Let  $p = 2m_1 + 1$  and let  $q = 2m_2 + 1$ , and consider all ordered pairs of integers  $(x, y)$ , where  $1 \leq x \leq m_2$ ,  $1 \leq y \leq m_1$ . Obviously, there are  $m_1 m_2 = \frac{p-1}{2} \frac{p-1}{2}$  such pairs. We calculate how many of these pairs have  $px > qy$ . Geometrically,



if we plot the points in the  $xy$ -plane, and draw the line  $px = qy$ , this corresponds to the number of points below the line. Let's calculate this directly: We for each  $x$ , we want  $y$  with  $1 \leq y < \frac{px}{q}$ . The number of such  $y$  for a

specific  $x$  is  $\lfloor px/q \rfloor$ , so the total is  $\sum_{x=1}^{m_2} \lfloor px/q \rfloor$ . Similarly, the number of points  $(x, y)$  with  $px$

$< qy$  is the number of points above this line, and this evaluates to

$\sum_{y=1}^{m_1} \lfloor qy/p \rfloor$ . Since there are  $m_1 m_2$  total points, and no point is on the line, this means

that 
$$\sum_{x=1}^{m_2} \lfloor px/q \rfloor + \sum_{y=1}^{m_1} \lfloor qy/p \rfloor = m_1 m_2.$$

From the technical lemma,  $\left(\frac{p}{q}\right) = (-1)^{n_1}$ , where  $n_1 = \sum_{k=1}^{(q-1)/2} \lfloor pk/q \rfloor + \frac{1}{8}(q^2 - 1)(p - 1)$

and  $\left(\frac{q}{p}\right) = (-1)^{n_2}$  where  $n_2 = \sum_{k=1}^{(p-1)/2} \lfloor qk/p \rfloor + \frac{1}{8}(p^2 - 1)(q - 1)$ . Since  $p - 1$  and  $q - 1$  are

even, we can ignore the terms other than the sums. Hence,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{n_1 + n_2} \text{ where } n_1 + n_2 = \sum_{x=1}^{m_2} \lfloor px/q \rfloor + \sum_{y=1}^{m_1} \lfloor qy/p \rfloor = \frac{p-1}{2} \frac{q-1}{2}.$$

This completes the proof.

As an example, let's characterize all primes  $p$  for which 7 is a quadratic residue. Since

$$\left(\frac{7}{p}\right)\left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2} \frac{7-1}{2}} = (-1)^{\frac{p-1}{2}}, \text{ we have } \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right), \text{ if } p \equiv 1 \pmod{4}, \text{ and } \left(\frac{7}{p}\right) = -\left(\frac{p}{7}\right), \text{ if } p \equiv 3 \pmod{4}.$$

If we know  $p$  modulo 7, then we know  $\left(\frac{p}{7}\right)$ . Thus, to calculate  $\left(\frac{7}{p}\right)$ , we need to know  $p \pmod{7}$  and  $p \pmod{4}$ . That is, we really need  $p$  modulo 28. If  $p \equiv 1 \pmod{4}$ , then  $p$  is a quadratic residue of 7 if  $\left(\frac{p}{7}\right) = 1$ , or if  $p \equiv 1, 2, 4 \pmod{7}$ . This happens if  $p \equiv 1, 9, 25 \pmod{28}$ . If  $p \equiv 3 \pmod{4}$ , we need  $\left(\frac{p}{7}\right) = -1$ , so  $p \equiv 3, 5, 6 \pmod{7}$ . This leads to the additional cases  $p \equiv 3, 19, 27 \pmod{28}$ . Summarizing, 7 is a quadratic residue for those primes  $p$  such that  $p \equiv 1, 3, 9, 19, 25, \text{ or } 27 \pmod{28}$ , and a quadratic nonresidue for the other primes ( $p \equiv 5, 11, 13, 15, 17, \text{ or } 23 \pmod{28}$ ).

### The Jacobi symbol

As one final aid to calculating the Legendre symbol, we introduce a generalization, the Jacobi symbol. If  $m$  is a positive odd integer, with prime factorization  $m = p_1 p_2 \cdots p_k$  (primes

might be repeated), define  $\left(\frac{a}{m}\right)$  by a product of Legendre symbols:

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right).$$

One must be careful here:  $\left(\frac{a}{p}\right) = 1$  if and only if  $a$  is a quadratic residue modulo  $p$ . However, it is possible for  $\left(\frac{a}{m}\right) = 1$  even if  $a$  is not a quadratic residue modulo  $m$ . For example,  $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$ . If we look for squares modulo 15, we have a list:  $1^2 = 1$ ,  $2^2 = 4$ ,  $3^2 = 9$ ,  $4^2 = 1$ ,  $5^2 = 10$ ,  $6^2 = 6$ ,  $7^2 = 4$ . That is, the squares are 1, 4, 6, 9, and 10. Since 2 is not on the list, 2 is not a square modulo 15.

**Theorem.** (Properties of the Jacobi symbol) Let  $m$  and  $n$  be positive odd integers.

1.  $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right),$
2.  $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right),$
3. If  $a \equiv b \pmod{m}$ , then  $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right),$
4.  $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}},$
5.  $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}},$
6. If  $m$  and  $n$  are relatively prime, then  $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}}.$

**Proof.** The proofs of most of these are straight forward. For example, in 3, let  $m = p_1 p_2 \cdots p_k$ . If  $a \equiv b \pmod{m}$ , then  $a \equiv b \pmod{p_i}$  for each  $p_i$ . Thus,

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right) = \left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_k}\right) = \left(\frac{b}{m}\right).$$

For 5, induct on the number of prime divisors of  $m$ . What the rule translates to is that  $\left(\frac{2}{m}\right) =$

$$\begin{cases} 1, & \text{if } m \equiv 1 \text{ or } 7 \pmod{8}, \\ -1, & \text{if } m \equiv 3 \text{ or } 5 \pmod{8}. \end{cases}$$
 This is certainly the rule if  $m$  is prime. By way of induction,

suppose the result is true for  $m$ , and we wish to evaluate  $\left(\frac{2}{pm}\right)$ . We have  $\left(\frac{2}{pm}\right) = \left(\frac{2}{p}\right)\left(\frac{2}{m}\right)$ . If  $p \equiv 1, 7 \pmod{8}$  and  $m \equiv 1, 7 \pmod{8}$ , then this evaluates to 1. Also,  $pm \equiv 1, 7 \pmod{8}$ . If  $p \equiv 3, 5 \pmod{8}$  and  $m \equiv 3, 5 \pmod{8}$ , then the product is  $(-1)(-1) = 1$ , and  $pm \equiv 1, 7 \pmod{8}$ , so the result again holds. If one of  $p, m$  is  $1, 7 \pmod{8}$  and the other is  $3, 5 \pmod{8}$ , then the product is  $(1)(-1) = -1$ . In this case,  $pm \equiv 3, 5 \pmod{8}$ , and everything still works. You should check that all the arithmetic above is correct. To simplify things,  $x \equiv 1, 7 \pmod{8}$  is the same as  $x \equiv \pm 1$ . The other case is  $x \equiv \pm 3$ .

Finally, for (6), we also induct on the number of prime divisors of  $mn$ . The expression in (6) can be rewritten  $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$  if either  $m$  or  $n$  is  $\equiv 1 \pmod{4}$ , and  $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$  if both  $m$  and  $n$  are  $\equiv 3 \equiv -1 \pmod{4}$ . If  $m$  and  $n$  are both prime, the result is the Law of Quadratic Reciprocity for the Legendre symbol. Assuming the result works for some  $m, n$ , let one of these be multiplied by another prime  $p$ . By symmetry, we may reduce to the case of showing  $\left(\frac{pm}{n}\right) = \left(\frac{n}{pm}\right)$  if either  $n$  or  $pm$  is  $1 \pmod{4}$ , and  $\left(\frac{pm}{n}\right) = -\left(\frac{n}{pm}\right)$  if both  $pm$  and  $n$  are  $3 \pmod{4}$ . Suppose first, that  $n \equiv 1 \pmod{4}$ . Then

$$(*) \quad \left(\frac{pm}{n}\right) = \left(\frac{p}{n}\right)\left(\frac{m}{n}\right) = \left(\frac{n}{p}\right)\left(\frac{n}{m}\right) \text{ (by inductive hypothesis)} = \left(\frac{n}{pm}\right).$$

Next, suppose that  $n \equiv 3 \pmod{4}$ . If both  $p$  and  $m$  are  $1 \pmod{4}$ , then (\*) still is correct. If both  $p$  and  $m$  are  $3 \pmod{4}$ , then  $pm \equiv 1 \pmod{4}$ . Also,

$$\left(\frac{pm}{n}\right) = -\left(\frac{p}{n}\right)\left(-\left(\frac{m}{n}\right)\right) = \left(\frac{n}{p}\right)\left(\frac{n}{m}\right) = \left(\frac{n}{pm}\right).$$

Finally, if one of  $p, m$  is  $1 \pmod{4}$  and the other is  $3 \pmod{4}$ , then their product is  $3 \pmod{4}$ , and

$$\left(\frac{pm}{n}\right) = (-1)\left(\frac{p}{n}\right)\left(\frac{m}{n}\right) = -\left(\frac{n}{p}\right)\left(\frac{n}{m}\right) = -\left(\frac{n}{pm}\right).$$

All these cases are consistent with (6), and we have exhausted the possibilities.

Why introduce the Jacobi symbol rather than work strictly with Legendre symbols?

Here is one reason: Suppose we wish to calculate  $\left(\frac{a}{p}\right)$ , where  $a$  and  $p$  are both very large. In order to use Legendre symbols, we would need to know how  $a$  factors, whereas with Jacobi symbols, we don't. For example, suppose we wish to calculate  $\left(\frac{2^{257} - 1}{2^{521} - 1}\right)$ . Here the denominator is a Mersenne prime, but the numerator is not. Moreover, the numerator is a 78 digit number with no small prime divisors, so factoring it would be quite difficult. Thus, this would be a very hard exercise with just Legendre symbols to work with. With Jacobi symbols, we have  $\left(\frac{2^{257} - 1}{2^{521} - 1}\right) = -\left(\frac{2^{521} - 1}{2^{257} - 1}\right)$ . Now  $2^{521} - 1 = 2^{2 \cdot 257 + 7} - 1$ , and  $2^{257} \equiv 1 \pmod{2^{257} - 1}$ , so  $2^{521} - 1 \equiv 2^7 - 1 \pmod{2^{257} - 1}$ . Thus,  $-\left(\frac{2^{521} - 1}{2^{257} - 1}\right) = -\left(\frac{2^7 - 1}{2^{257} - 1}\right)$ . We employ (6) again to get  $\left(\frac{2^{257} - 1}{2^{521} - 1}\right) = -\left(-\left(\frac{2^{257} - 1}{2^7 - 1}\right)\right) = \left(\frac{2^{257} - 1}{2^7 - 1}\right)$ . Since  $2^7 \equiv 1 \pmod{2^7 - 1}$ , and  $2^{257} - 1 = 2^{36 \cdot 7 + 5} - 1$ ,  $2^{257} - 1 \equiv 2^5 - 1 \pmod{2^7 - 1}$ . We now have

$$\begin{aligned} \left(\frac{2^{257} - 1}{2^{521} - 1}\right) &= \left(\frac{31}{127}\right) \\ &= -\left(\frac{127}{31}\right) = -\left(\frac{3}{31}\right) = \left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1. \end{aligned}$$