Quadratic reciprocity and the Jacobi symbol

Stephen McAdam
Department of Mathematics
University of Texas at Austin
mcadam@math.utexas.edu

Abstract: We offer a proof of quadratic reciprocity that arises from looking at the Jacobi symbol in a non-standard way. We also give some non-standard proofs of some standard facts about the Jacobi symbol. We also prove that the Jacobi symbol always satisfies Gauss's Lemma, a fact which we have never seen mentioned.

Introduction: Recall that if p is an odd prime and GCD(m, p) = 1, then the Legendre symbol $(m / p)_L$ is defined to be +1 if there is a solution to $X^2 \equiv m \bmod p$, and is defined to be -1 otherwise. More generally, if n > 1 is odd with prime factorization $n = \prod_{r=1}^{c} p_r$, and if GCD(m, n) = 1, then the Jacobi symbol $(m / n)_J$ is defined to be $\prod_{r=1}^{c} (m/p_r)_L$, while $(m / 1)_J$ is defined as +1. The most important fact about the Jacobi symbol is that it satisfies quadratic reciprocity. That is, if m and n are relatively prime odd positive integers, then $(m / n)_J = (1)^{\frac{(m-1)(n-1)}{4}} (n / m)_J$.

In order to describe our work here, we need a bit of notation.

NOTATION: We assume n > 0 is odd and GCD(m, n) = 1.

For $1 \le i \le |m|$, let I_i be the interval $\left[(i - 1)n/2|m|, \quad in/2|m|\right)\Big]$.

We will call I_i an even (respectively odd) interval if i is even (respectively odd).

If m > 0, let t(m, n) be the number of integers contained in the union of the even intervals.

If m < 0, let t(m, n) be the number of positive integers contained in the union of the odd intervals. (We note that $0 \in I_1$. However, we canonically ignore it.)

Definition: Let $(m / n) = (-1)^{t(m,n)}$.

We will first show that some standard properties of the Jacobi symbol hold for our symbol, using non-standard proofs. We will then show that if n is an odd prime, then $(m / n) = (m / n)_L$. Next, we show that our symbol satisfies quadratic reciprocity. That will establish quadratic reciprocity for the Legendre symbol, which is our primary goal in this work. However, we will then give a non-standard proof that $(m_1m_2 / n) = (m_1 / n)(m_2 / n)$, and use that to show $(m / n) = (m / n)_J$.

Lemma 1: $(1 / n) = 1$ and $(m / 1) = 1$.

Proof: For $(1 / n)$, the only interval is I_1, which is odd. Thus $t(1, n) = 0$, and so $(1 / n) = 1$. For $(m / 1)$, we have $\bigcup_{i=1}^{|m|} I_i = [0, 1/2]$, and as that contains no nonzero integers, $t(m, 1) = 0$, so that $(m / 1) = 1$.

Lemma 2: $(-m / n) = (-1)^{\frac{n-1}{2}} (m /n)$.

Proof: $\bigcup_{i=1}^{|m|} I_i = [0, n/2]$. Thus the set of positive integers contained in the union of all the intervals is $\{1, 2, \ldots, (n - 1)/2.\}$ The only numbers contained in more than one interval have the form $in/2m$ with $1 \leq i \leq |m|$, and as $GCD(m, n) = 1$, none of those are integers. Thus each integer between 1 and $(n - 1)/2$ is in exactly one of our intervals.
Therefore, $t(m, n) + t(-m, n) = (n - 1)/2$, and so $t(-m, n) \equiv (n - 1)/2 + t(m , n) \bmod 2$.

Using that the Jacobi symbol satisfies quadratic reciprocity, it is not hard to show that Lemmas 3 and 5 below are true for the Jacobi symbol. However, we have never seen that stated, and they do not appear to be of great interest when the standard definition of the Jacobi symbol is used. However, for our work, with our non-standard definition, they are vital.

Lemma 3: If $m > 0$ is odd and $n - 2m > 0$, then $(m / n - 2m) = (-1)^{\frac{m-1}{2}} (m / n)$.

Proof: We have that $t(m, n)$ is the number of integers in the union of the even $I_i = \left[(i - 1)n/2m, \ in/2m\right)\Big]$, with $1 \le i \le m$. Now $t(m, n - 2m)$ is the number of integers in the union of the even intervals $J_i = \left[(i - 1)(n - 2m)/2m, i(n - 2m)/2m\right] =$ $\left[(i - 1)(n/2m) - (i - 1), i(n/2m) - i\right]$, with $1 \le i \le m$. The lower bound of J_i is less than the lower bound of I_i by exactly $(i - 1)$ (an integer), and the length, (namely $n/2m - 1 > 0$), of J_i is one less than the length of I_i. Thus, it is easily seen that J_i contains exactly one less integer than I_i. Therefore $t(m, n) - t(m, n - 2m)$ equals the number of even i, which is $(m - 1)/2$, and so $t(m, n - 2m) \equiv (m - 1)/2 + t(m, n) \bmod 2$.

We do not need the next corollary for our proof of quadratic reciprocity, but it is well known to hold for the Jacobi symbol. However, the only proof for the Jacobi symbol that this author has seen uses quadratic reciprocity. For our (m / n), it only needs Lemmas 2 and 3.

Corollary 4: If $r > 0$ and $n \equiv r \bmod 4m$, then $(m / n) = (m / r)$.

Proof: For the case $m > 0$, we may suppose $n > r$ and write $r = n - 4mk$. By Lemma 3 (used twice), we have $(m / n) = (-1)^{\frac{m-1}{2}} (m / n - 2m) = ((-1)^{\frac{m-1}{2}})^2 (m / n - 4m) = (m / n - 4m)$. That handles the case $k = 1$, and of course induction handles $k > 1$. When $m < 0$, since $n \equiv r \bmod 4(-m)$, we have $(-m / n) = (-m / r)$. Furthermore, since $n \equiv r \bmod 4$, we have $(-1)^{\frac{n-1}{2}} = (-1)^{\frac{r-1}{2}}$, so that Lemma 2 shows $(m / n) = (m / r)$.

Example: Using Corollary 4, it can easily be shown that $(-5 / n) = 1$ if and only if n is congruent to one of 1, 3, 7, or 9 mod 20. A similar rule (working mod 4m) holds for any (m / n).

Lemma 5: If $m > 0$ and $2m - n > 0$, then $(m / 2m - n) = (-1)^{\frac{m-1}{2}} (m / n)$.

Proof: As before, we have $I_i = \left[(i - 1)n/2m, \quad in/2m\right]$ with $1 \le i \le m$.

We let $K_i = \left[(i - 1)(2m - n)/2m, i(2m - n)/2m\right] = \left[(i - 1) - (i - 1)n/2m, i - in/2m\right]$.

Claim 1: We claim that for $2 \le i \le m$, there is exactly one integer in $K_i \cup I_i$, and furthermore, that integer is not in $K_i \cap I_i$. (Note that since $i > 1$, all integers under consideration are positive.)

Suppose claim 1 is true. Then since $t(m, n)$ counts the integers in the even I_i, while $t(m, 2m - n)$ counts the integers in the even K_i, and since there is no overlap of those two counts, $t(m, n) + t(m, 2m - n) = (m - 1)/2$, the number of even i. That shows $t(m, 2m - n) \equiv (m - 1)/2 + t(m, n) \bmod 2$, as required.

It remains to prove claim 1. We 'negate' the K_i, letting $-K_i = \left[in/2m - i, (i - 1)n/2m - (i - 1)\right]$.

Claim 2: For $2 \le i \le m$, $-K_i \cup I_i$ contains exactly one integer (necessarily non-zero).

We now show claim 2 implies claim 1. Suppose the number of integers in $I_i - K_i$ is x, the number of integers in $K_i - I_i$ is y, and the number of integers in $K_i \cap I_i$ is z. Then $-K_i$ contains $x + z$ negative integers and I_i contains $y + z$ positive integers, so that $-K_i \cup I_i$ contains $x + y + 2z$ integers. By claim 2, $x + y + 2z = 1$, and so $z = 0$ and one of x or y is 1, the other being 0. That proves claim 1.

It remains to prove claim 2. We will induct on i, first noting that when $i = 1$, $-K_1 \cup I_1 = [n/2m - 1, 0] \cup [0, n/2m]$ contains no nonzero integers (since $n/2m < 1$).

For $i > 1$, consider $\bigcup_{h=1}^{i}(-K_h \cup I_h) = [in/2m - i, in/2m]$. That interval has length i and has

non-integral end points, and so it contains exactly i integers, one of them being 0. Thus $\bigcup_{h=1}^{i}(-K_h \cup I_h)$ contains exactly i - 1 non-zero integers.

When i = 2, we know that $-K_2 \cup -K_1 \cup I_1 \cup I_2$ contains exactly 1 non-zero integer, and that integer is not in $-K_1 \cup I_1$. Therefore, it must be the only integer in $-K_2 \cup I_2$. In general, when moving from i to i + 1, we adjoin $-K_{i+1} \cup I_{i+1}$ to our previous union, and also add exactly one more nonzero integer (not contained in the previous union) to the count. That new integer must be the one and only integer in $-K_{i+1} \cup I_{i+1}$, proving claim 2, and also the lemma.

Before we can prove quadratic reciprocity for (m / n) (and for the Legendre symbol), we need one more property of (m / n). To prove it, we must reveal that the number t(m, n) defined above can also be described in a way that Gauss introduced. (We have so far hidden the connection, since we wished to stress how far our original description of t(m, n) could take us.)

.

NOTATION: We now take n > 1. We will let $S = \{1, \ldots, \frac{n-1}{2}\}$ and $T = \{\frac{n-1}{2} + 1, \ldots, n - 1\}$. We will say that r is reduced if $r \in S \cup T$. For $b \in S$, let r_b be the (unique) reduced number congruent to mb modulo n. (We will refer to the various r_b as 'the remainders'. Note that since GCD(m, n) = 1, and $1 \leq b \leq (n - 1)/2$, r_b is never 0.) Let $t'(m , n)$ be the number of r_b that are in T (as b varies over S).

Lemma 6: When n > 1, $t'(m, n)$ is the number of $b \in S$ such that $r_b \in T$.

Proof: It will suffice to show that distinct b give distinct remainders. To see that, if b and b' are both in S, with $r_b = r_b$, then $mb \equiv r_b = r_{b'} \equiv mb' \bmod n$, so that $b \equiv b' \bmod n$. As b and b' are both between 1 and (n - 1)/2, we have $b = b'$.

Lemma 7: $t(m, n) = t'(m, n)$.

Proof: We will do the slightly harder case that $m < 0$. In the proof of Lemma 2, we saw that S is exactly the set of nonzero integers contained in $\bigcup_{i=1}^{|m|} I_i$. Thus every integer in S is in exactly one of the I_i. We must show that for $b \in S$, with $b \in I_i$, we have i even if and only if $r_b \in T$. As $b \in I_i$, we have $(i - 1)n/2|m| < b < in/2|m|$. Since $m < 0$, we have

(*) $-in/2 < mb < -(i - 1)n/2$.

Suppose i is odd. Then $(i + 1)n/2$ is an integral multiple of n. Adding $(i + 1)n/2$ to each number in (*) shows that $n/2 < mb + (i + 1)n/2 < n$. That shows $r_b = mb + (i + 1)n/2 \in T$. On the other hand, if i is even, we add $in/2$ to the terms in (*), and see that $r_b = mb + in/2$ is in S.

Corollary 8: If n is an odd prime, $(m / n) = (m / n)_L$.

Proof: This follows from Lemma 7 and Gauss's Lemma [B, Theorem 9.5].

Remark: Lemma 7 shows that our symbol (m / n) always satisfies Gauss's Lemma, even when n is not prime. As we will later show $(m / n) = (m / n)_J$, we will have that the Jacobi symbol satisfies Gauss's Lemma. We have never seen that fact mentioned.

Lemma 9: If $m \equiv k \bmod n$, then $(m / n) = (m / k)$.

Proof: For $b \in S$, $mb \equiv kb \bmod n$. Thus the remainder r_b found for mb is the same as that found for kb. Therefore, $t(m, n) = t(k, n)$, and the lemma follows.

We have learned enough about our (m / n) that we can now give an easy (but slightly tedious) proof that it satisfies quadratic reciprocity. By Corollary 8, we will automatically get that the Legendre symbol satisfies quadratic reciprocity.

Theorem 10: If n and m are relatively prime positive odd integers,
then $(m / n) = (-1)^{\frac{(m-1)(n-1)}{4}} (n / m)$.

Proof: We are only concerned with odd $m > 0$. To help focus on them, we make a definition. For relatively prime odd positive integers m and n, let $\langle m / n \rangle = (m / n)$.
Our goal is now to show that $\langle m / n \rangle = (-1)^{\frac{(m-1)(n-1)}{4}} \langle n / m \rangle$.

Let $\{m / n\} = (-1)^{\frac{(m-1)(n-1)}{4}} \langle n / m \rangle$. Our goal is now to show $\{m / n\} = \langle m / n \rangle$.

We now list five facts about $\langle m / n \rangle$, along with their justifications.

Fact 1) If $m - 2n > 0$, then $\langle m - 2n / n \rangle = \langle m / n \rangle$. (Lemma 9.)

Fact 2) If $m - 2n > 0$, then $\langle n / m - 2n \rangle = (-1)^{\frac{n-1}{2}} \langle n / m \rangle$. (Lemma 3, with n and m reversed.)

Fact 3) If $2n - m > 0$, then $\langle 2n - m / n \rangle = (-1)^{\frac{n-1}{2}} \langle m / n \rangle$.
(By Lemmas 2 and 9, $(-1)^{\frac{n-1}{2}} \langle m / n \rangle = \langle -m / n \rangle = \langle 2n - m / n \rangle$.)

Fact 4) If $2n - m > 0$, then $\langle n / 2n - m \rangle = (-1)^{\frac{n-1}{2}} \langle n / m \rangle$. (Lemma 5, with n and m reversed.)

Fact 5: $\langle 1 / 1 \rangle = 1$. (Lemma 1.)

We will now show that $\{m / n\}$ also satisfies those five facts. Then we will use that to show $\{m / n\} = \langle m / n \rangle$, and be done.

For Fact 1, suppose m - 2n > 0. Then $\{m - 2n / n\} = (-1)^{\frac{(m-2n-1)(n-1)}{4}} \langle n / m - 2n \rangle =$ $(-1)^{\frac{(m-2n-1)(n-1)}{4}} (-1)^{\frac{n-1}{2}} \langle n / m \rangle$, using Fact 2 for < / >. We need that to equal $\{m / n\} = (-1)^{\frac{(m-1)(n-1)}{4}} \langle n / m \rangle$. That is an easy exercise.

For Fact 2, suppose m - 2n > 0. Then $\{n / m - 2n\} = (-1)^{\frac{(n-1)(m-2n-1)}{4}} \langle m - 2n / n \rangle =$ (by Fact 1) $(-1)^{\frac{(n-1)(m-2n-1)}{4}} \langle m / n \rangle$. That is easily seen to equal $(-1)^{\frac{n-1}{2}} \{n / m\} = (-1)^{\frac{n-1}{2}} (-1)^{\frac{(m-1)(n-1)}{4}} \langle m / n \rangle$.

For Fact 3, suppose 2n - m > 0. Then $\{2n - m / n\} = (-1)^{\frac{(2n-m-1)(n-1)}{4}} \langle n / 2n - m \rangle =$ $(-1)^{\frac{(2n-m-1)(n-1)}{4}} (-1)^{\frac{n-1}{2}} \langle n / m \rangle$, by Fact 4 applied to < / >. An easy exercise, using that n and m are odd, shows that equals $(-1)^{\frac{n-1}{2}} \{m / n\} = (-1)^{\frac{n-1}{2}} (-1)^{\frac{(m-1)(n-1)}{4}} \langle n / m \rangle$.

For Fact 4, suppose 2n - m > 0. We have $\{n / 2n - m\} = (-1)^{\frac{(n-1)(2n-m-1)}{4}} \langle 2n - m / n \rangle =$ (by Fact 3) $(-1)^{\frac{(n-1)(2n-m-1)}{4}} (-1)^{\frac{n-1}{2}} \langle m / n \rangle$. That is easily seen to equal $(-1)^{\frac{n-1}{2}} \{n / m\}$.

For Fact 5, we have $\{1 / 1\} = (-1)^{\frac{(1-1)(1-1)}{4}} \langle 1 / 1 \rangle = (1)(1) = 1$.

Remark: The above arguments show that Facts 1 and 2 are "reciprocals" of each other, as are Facts 3 and 4. That is what drives this proof of quadratic reciprocity.

In order to complete the proof of Theorem 10, we must only show $\{m / n\} = \langle m / n \rangle$. If false, consider a counter-example $\{m / n\} \neq \langle m / n \rangle$, with n minimal and (for that n) m minimal. We will get the contradiction that m < n and also n < m.

Suppose m - 2n > 0. By Fact 1, {m - 2n / n} = {m / n} ≠ <m / n> = <m - 2n / n>.
That contradicts the minimality of m. Thus 2n - m > 0. By Fact 3,
$\{2n - m / n\} = (-1)^{\frac{n-1}{2}} \{m / n\} \neq (-1)^{\frac{n-1}{2}} \langle m / n \rangle = \langle 2n - m / n \rangle$. Therefore, we must have
$m \leq 2n - m$. Now equality can only hold if m = n, and since GCD(m, n) = 1, that would require
m = 1 = n. However, Fact 5 shows {1 / 1} = <1 / 1>. Therefore, m < 2n - m, showing m < n.

Now suppose n - 2m > 0. Then reversing n and m in Fact 2, we have
$\{m / n - 2m\} = (-1)^{\frac{m-1}{2}} \{m / n\} \neq (-1)^{\frac{m-1}{2}} \langle m / n \rangle = \langle m / n - 2m \rangle$.
That violates the minimality of n. Thus 2m - n > 0. Reversing n and m in Fact 4, we have
$\{m / 2m - n\} = (-1)^{\frac{m-1}{2}} \{m / n\} \neq (-1)^{\frac{m-1}{2}} \langle m / n \rangle = \langle m / 2m - n \rangle$. Therefore, we must have
n < 2m - n (equality impossible by Fact 5), showing n < m, and completing the proof.

Combining Theorem 10 and Corollary 8 shows quadratic reciprocity holds for the Legendre symbol. We now turn to our second goal, showing (m / n) is actually the Jacobi symbol. There are two ways we could do that. The less interesting (pedagogically at least) is to use that it is known that the Jacobi symbol (like our symbol) satisfies quadratic reciprocity. Both symbols also satisfy Lemmas 1, 2, and 9. Using those facts, it is not hard to give a proof that they are equal, similar to our above argument that {m / n} = <m / n> in the proof of Theorem 10. However, we opt to give a proof that does not require any prior knowledge of the Jacobi symbol, other than its definitionn. We start with two more non-standard proofs.

Lemma 11: (2 / n) equals +1 if n is congruent to 1 or 7 mod 8,
and equals -1 if n is congruent to 3 or 5 mod 8.

Proof: We consider the m = 2 intervals $I_1 = [0, n/4]$ and $I_2 = [n/4, n/2]$. One can easily verify that t(2 / n), the number of integers in I_2, is even exactly when n is congruent to 1 or 7 mod 8.

In order to show that $(m / n) = (m / n)_J$, we need to show that $(m_1 m_2 / n) = (m_1 / n)(m_2 / n)$.

The proof of that fact for the Legendre symbol is well known. Our proof is markedly different. It uses the following lemma, which is also used in the proof of Gauss's Lemma.

LEMMA 12: $S = \{r_b \mid r_b \in S\} \cup \{n - r_b \mid r_b \in T\}$.

Proof: The union on the right is clearly a subset of S. Lemma 6 shows there are |S| distinct remainders, and so $|\{r_b \mid r_b \in S\}| + |\{n - r_b \mid r_b \in T\}| = |S|$. Therefore, it will suffice to show $\{r_b \mid r_b \in S\} \cap \{n - r_b \mid r_b \in T\}$ is empty. If $r_b = n - r_{b'}$, we have
$mb \equiv r_b = n - r_{b'} \equiv n - mb' \equiv - mb' \bmod n$, so that $b \equiv -b' \bmod n$.
But $1 \leq b + b' \leq n - 1$, giving a contradiction.

Lemma 13: $(m_1m_2 / n) = (m_1 / n)(m_2 / n)$.

Proof: Let $m_3 = m_2m_1$. For $b \in S$, and i = 1, 2, 3, let r_{ib} be the reduced remainder mod n of m_ib. Let t_i be the number r_{ib} in T, so that $(m_i / n) = (-1)^{t_i}$.

We want to show $(-1)^{t_1} (-1)^{t_2} = (-1)^{t_3}$. That is, we want $t_1 + t_2 \equiv t_3 \bmod 2$.

Let us say that b is of type 1 if $r_{1b} \in S$, and is of type 2 if $r_{1b} \in T$.
By definition of t_1, exactly t_1 of the $b \in S$ are of type 2.
Suppose that exactly x of the type 1 b have r_{3b} in T, and exactly y of the type 2 b have r_{3b} in T.
Then $t_3 = x + y$.

For $b \in S$, define $f(b) = r_{1b}$ for type 1 b, and $f(b) = n - r_{ib}$ for type 2 b.
By Lemma 12, f is a permutation of S. Thus, t_2 equals the number of $b \in S$ with $r_{2f(b)} \in T$.

CLAIM: For exactly x of the type 1 b, $r_{2f(b)}$ is in T, while for exactly $t_1 - y$ of the type 2 b, $r_{2f(b)}$ is in T, implying that $t_2 = x + (t_1 - y)$.

Suppose the claim is true. Then $t_1 + t_2 = t_1 + x + (t_1 - y)$ has the same parity as $t_3 = x + y$, and we are done.

In this proof of the claim, all congruences are mod n. If b is of type 1, then $r_{2f(b)} \equiv m_2 f(b) = m_2 r_{1b} \equiv m_2 m_1 b = m_3 b \equiv r_{3b}$. As all remainders lie between 1 and n - 1, we see that in this case, $r_{2f(b)} = r_{3b}$. As we are supposing that exactly x of the type 1 b have $r_{3b} \in T$, we have proven the first part of the claim. As for type 2 b, we have $r_{2f(b)} \equiv m_2 f(b) = m_2(n - r_{1b}) \equiv -m_2 r_{1b} \equiv -m_2 m_1 b = -m_3 b \equiv -r_{3b} \equiv n - r_{3b}$, the last step to have a remainder between 1 and n - 1. In this case, we have that $r_{2f(b)} = n - r_{3b}$. That last is in T exactly when r_{3b} is in S. We have assumed that r_{3b} is in T for exactly y of the type 2 b. We saw that there are exactly t_i b of type 2. Thus, exactly $t_1 - y$ of the type 2 b have $r_{3b} \in S$, and so have $r_{2b} = n - r_{3b} \in T$, completing the proof.

The next theorem is trivial if we use the standard definition of the Jacobi symbol, but (to the best of our knowledge) requires quadratic reciprocity (Theorem 10) using our non-standard definition.

Lemma 14. $(m / n_1 n_2) = (m / n_1)(m / n_2)$.

Proof: The cases m = -1 and m = 2 are easy, using Lemmas 2 and 11. For example, suppose $n_1 \equiv 3 \bmod 8$, and $n_2 \equiv 5 \bmod 8$, so that $n_1 n_2 \equiv 1 \bmod 8$. By Lemma 11, $(2 / n_1 n_2) = +1 = (-1)(-1) = (2 / n_1)(2 / n_2)$.

We claim that $(\frac{h}{n_1 n_2}) = (\frac{h}{n_1})(\frac{h}{n_2})$ whenever h > 0 is odd. Suppose that is true.
In general, say $m = (-1)^e (2)^d h$, with $e \in \{0, 1\}$, $d \geq 0$, and h > 0 and odd. By Lemma 13, we have $(m / n_1 n_2) = (-1 / n_1 n_2)^e (2 / n_1 n_2)^d (h / n_1 n_2)$. By the claim, we have $(k / n_1 n_2) = (k / n_1)(k / n_2)$ for $k \in \{-1, 2, h\}$, and we can then recombine those factors into $(m / n_1)(m / n_2)$.
Therefore, it only remains to prove the claim.

By Theorem 10 and Lemma 13, we have $(h / n_1n_1) = (-1)^{\frac{(h-1)(n_1n_2-1)}{4}}(n_1n_2 / h) =$
$(-1)^{\frac{(h-1)(n_1n_2-1)}{4}}(n_1 / h)(n_2 / h) = (-1)^{\frac{(h-1)(n_1n_2-1)}{4}}(-1)^{\frac{(h-1)(n_1-1)}{4}}(-1)^{\frac{(h-1)(n_2-1)}{4}}(h / n_1)(h / n_2)$.
Thus, it will suffice to show $(1/4)(h - 1)[n_1n_2 - 1 + n_1 - 1 + n_2 - 1]$ is even. As h -1 is even, we must show $(1/2)[n_1n_2 + n_1 + n_2 - 3]$ is even or equivalently, $n_1n_2 + n_1 + n_2 \equiv 3 \bmod 4$.
The four possible cases (mod 4) are easily checked.

Theorem 15: $(m / n) = (m / n)_J$.

Proof: They both when n = 1. For n > 1, suppose the factorization of n is $n = \prod_{r=1}^{c} p_r$.
By Lemmas 14 and Corollary 8, $(m / n) = \prod_{r=1}^{c}(m / p_r) = \prod_{r=1}^{c}(m / p_r)_L = (m / n)_J$.

Remark: It appears difficult to prove via our non-standard definition that if n is an odd prime, then there is an m with (m / n) = -1, without making use of Gauss's Lemma. If that could be done easily, it would lead to a pleasant proof of Gauss's Lemma, avoiding Euler's Criterion.

Reference

[B]: D. Burton, *Elementary Number Theory*, seventh edition, McGraw-Hill, New York, 2011.