SQUARES MODULO p, III

KEITH CONRAD

Such is the advantage of a well-constructed language that its simplified notation often becomes the source of profound theories. Laplace

We provide here me applications of quadratic reciprocity, ranging from explicit calculations to theoretical issues. One application will be a probabilistic primality test based on an attempt at extending Euler's congruence $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ to composite moduli.

1. Worked examples

Now we use the quadratic reciprocity law to make computations.

Example 1.1. Is $-7 \equiv \square \bmod 103$? We have

$$\left(\frac{-7}{103}\right) = \left(\frac{-1}{103}\right)\left(\frac{7}{103}\right).$$

Since $103 \equiv 3 \bmod 4$, $(\frac{-1}{103}) = -1$. Since $7 \equiv 3 \bmod 4$ and $103 \equiv 3 \bmod 4$, the main law says

$$\left(\frac{7}{103}\right) = -\left(\frac{103}{7}\right) = -\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1) = 1.$$

Therefore $(\frac{-7}{103}) = (-1)(1) = -1$, so $-7 \not\equiv \square \bmod 103$.

Example 1.2. Does the congruence $x^2 - 5x + 3 \equiv 0 \bmod 23$ have a solution? The discriminant is $5^2 - 4 \cdot 3 = 13$, so we compute $(\frac{13}{23})$. Since $13 \equiv 1 \bmod 4$,

$$\left(\frac{13}{23}\right) = \left(\frac{23}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{5}{13}\right).$$

Since $13 \equiv 5 \bmod 8$, $(\frac{2}{13}) = -1$. By the main law, $(\frac{5}{13}) = (\frac{13}{5}) = (\frac{3}{5}) = -1$, so

$$\left(\frac{13}{23}\right) = (-1)(-1) = 1,$$

so the discriminant is a square and there is a solution.

A brute force search shows the square roots of 13 mod 23 are 6 and 17. It is left to the reader to get solutions to the original quadratic congruence from this via the quadratic formula.

Example 1.3. For which primes $p \neq 2, 5$ is $5 \equiv \square \bmod p$? We need to describe those p with $(\frac{5}{p}) = 1$. By quadratic reciprocity, $(\frac{5}{p}) = (\frac{p}{5})$, so $(\frac{5}{p}) = 1$ is the same as $(\frac{p}{5}) = 1$, which says $p \equiv \square \bmod 5$, so it means $p \equiv 1, 4 \bmod 5$.

Example 1.4. For which primes $p \neq 2, 5$ is $-5 \equiv \square \bmod p$? We have

$$\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{5}\right).$$

This is 1 when both terms are 1 or both are -1. Since

$$(-1)^{(p-1)/2} = 1 \iff p \equiv 1 \bmod 4, \quad \left(\frac{p}{5}\right) = 1 \iff p \equiv 1, 4 \bmod 5,$$

we need to solve the pair of conditions $p \equiv 1 \bmod 4$ and $p \equiv 1 \bmod 5$ as well as $p \equiv 1 \bmod 4$ and $p \equiv 4 \bmod 5$. By the Chinese remainder theorem we can solve each pair as a congruence condition mod 20 and get the conditions

$$p \equiv 1, 9 \bmod 20.$$

Now we turn to the case $(-1)^{(p-1)/2} = -1$ and $(\frac{p}{5}) = -1$. This corresponds to the congruence constraints

$$p \equiv 3 \bmod 4, \quad p \equiv 2, 3 \bmod 5,$$

and by the Chinese remainder theorem these are the same as

$$p \equiv 3, 7 \bmod 20.$$

Therefore when p is not 2 or 5, $(\frac{-5}{p}) = 1 \iff p \equiv 1, 3, 7, 9 \bmod 20$.

Example 1.5. For which primes $p \neq 2, 5$ is $10 \equiv \square \bmod p$?

We need to solve $(\frac{10}{p}) = 1$. Since $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p})$, we need either $(\frac{2}{p}) = 1$ and $(\frac{5}{p}) = 1$ or $(\frac{2}{p}) = -1$ and $(\frac{5}{p}) = -1$.

Suppose first that both $(\frac{2}{p})$ and $(\frac{5}{p})$ are 1. From the supplementary law, $(\frac{2}{p}) = 1$ if and only if $p \equiv 1, 7 \bmod 8$. From Example 1.3, $(\frac{5}{p}) = 1$ if and only if $p \equiv 1, 4 \bmod 5$. The congruences

$$p \equiv 1, 7 \bmod 8, \quad p \equiv 1, 4 \bmod 5$$

can each be broken off into one mod 8 condition and one mod 5 condition, and these each combine into one mod 40 condition. Altogether the 4 ways of pairing off the conditions mod 8 and mod 5 combine to give the 4 congruences

$$p \equiv 1, 9, 31, 39 \bmod 40.$$

Now suppose that $(\frac{2}{p})$ and $(\frac{5}{p})$ equal -1. We have $(\frac{2}{p}) = -1$ if and only if $p \equiv 3, 5 \bmod 8$ and $(\frac{5}{p}) = -1$ if and only if $p \equiv 2, 3 \bmod 5$. The congruences

$$p \equiv 3, 5 \bmod 8, \quad p \equiv 2, 3 \bmod 5$$

combine in pairs (one mod 8 and one mod 5) to give the congruences

$$p \equiv 3, 13, 27, 37 \bmod 40.$$

Thus for $p \neq 2$ or 5, $10 \equiv \square \bmod p$ if and only if $p \equiv 1, 3, 9, 13, 27, 31, 37, 39 \bmod 40$.

2. Elementary applications

We begin with some applications of the formula for $(\frac{2}{p})$. Our first application involves Mersenne numbers $M_p = 2^p - 1$. For many primes p, M_p is composite. This happens for the first time at $p = 11$. (And then at $p = 23, 29, 37, 41$, and so on.) It turns out that the formula for $(\frac{2}{p})$ lets us prove compositeness of $2^p - 1$ for certain p.

Theorem 2.1. *Let p be a prime greater than 3 such that $p \equiv 3 \bmod 4$ and $2p+1$ is prime. Then $2^p - 1$ is composite.*

Note the theorem is false for $p = 3$, so we must exclude this case. Examples of p fitting the theorem are 11 and 89.

Proof. We will show $2p+1$ is a factor of 2^p-1. This shows 2^p-1 is composite since $2p+1 < 2^p-1$ when $p > 3$.

Set $q = 2p+1$, so q is prime. We look at $(\frac{2}{q})$:

$$\left(\frac{2}{q}\right) \equiv 2^{(q-1)/2} \equiv 2^p \bmod q. \tag{2.1}$$

When $p \equiv 3 \bmod 4$, we have $q = 2p+1 \equiv 7 \bmod 8$. Therefore $(\frac{2}{q}) = 1$, so (2.1) says

$$1 \equiv 2^p \bmod q,$$

so 2^p-1 is divisible by $q = 2p+1$, which is a *proper* factor when $p > 3$. □

The next application of the formula for $(\frac{2}{p})$ tells us 2 is a generator modulo certain primes.

Theorem 2.2. *Let q be a prime of the form $2p+1$, where p is a prime with $p \equiv 1 \bmod 4$. Then $2 \bmod q$ is a generator.*

The first prime q fitting the conditions of the theorem is 11. Others are 59 and 83.

Proof. The order of $2 \bmod q$ divides $q-1 = 2p$, so its order is 1, 2, p, or $2p$. Since $q \geq 11$, the order is not 1 or 2. Therefore we just have to eliminate the possibility that $2 \bmod q$ has order p in order to know that $2 \bmod q$ is a generator.

If $2 \bmod q$ has order p, then $2^p \equiv 1 \bmod q$. However, since $2^p = 2^{(q-1)/2}$, this condition says $2^{(q-1)/2} \equiv 1 \bmod q$, so

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

But $q = 2p+1 \equiv 3 \bmod 8$ since $p \equiv 1 \bmod 4$, so $(\frac{2}{q}) = -1$. We have a contradiction. □

Our final elementary application will use the rule for $(\frac{3}{p})$,

$$\left(\frac{3}{p}\right) = 1 \Longleftrightarrow p \equiv 1, 11 \bmod 12, \tag{2.2}$$

to prove a necessary and sufficient condition for primality of Fermat numbers, due to Pepin (1877).

Theorem 2.3 (Pepin)**.** *Let $F_n = 2^{2^n}+1$ be the n-th Fermat number. For $n \geq 1$, F_n is prime if and only if $3^{(F_n-1)/2} \equiv -1 \bmod F_n$.*

Proof. First we show $F_n \equiv 5 \bmod 12$ for $n \geq 1$. (In particular, $(3, F_n) = 1$ for $n \geq 1$; note $F_0 = 3$.) For any $k \geq 1$, $4^k \equiv 4 \bmod 12$. Therefore

$$F_n = 2^{2^n}+1 = 4^{2^{n-1}}+1 \equiv 5 \bmod 12$$

when $n \geq 1$.

Suppose $p := F_n$ is prime. Since $p \equiv 5 \bmod 12$, (2.2) tells us $3 \not\equiv \square \bmod p$, so $3^{(p-1)/2} \equiv -1 \bmod p$.

Now suppose, conversely, that $3^{(F_n-1)/2} \equiv -1 \bmod F_n$. Since $\frac{F_n-1}{2} = 2^{2^n-1}$, we have

$$3^{2^{2^n-1}} \equiv -1 \bmod F_n. \tag{2.3}$$

Squaring both sides,

$$3^{2^{2^n}} \equiv 1 \bmod F_n.$$

We now show the order of $3 \bmod F_n$ is 2^{2^n}. If the order is less, then it is 2^k where $0 \leq k \leq 2^n - 1$. But $k \leq 2^n - 1 \Rightarrow 2^k | 2^{2^n-1}$, so $3^{2^{2^n}-1} \equiv 1 \bmod F_n$, but this contradicts (2.3). Therefore $3 \bmod F_n$ has order 2^{2^n}. Since $F_n = 2^{2^n} + 1$, the order of $3 \bmod F_n$ is $F_n - 1$. Therefore $(F_n - 1) | \varphi(F_n)$. However, for any $m \in \mathbf{Z}^+$, $\varphi(m) \leq m - 2$ when m is composite (0 and a non-trivial factor of m are two non-units modulo m). Therefore the relation $(F_n - 1) | \varphi(F_n)$ forces F_n to be prime. □

Remark 2.4. Pepin's test is how Fermat numbers are checked to be composite. The test does not yield a non-trivial factor of F_n. For instance, Pepin's test was used in the 1960s to prove F_{14} is composite, but even today no nontrivial factor of F_{14} is known. The number F_{14} has 4933 decimal digits.

3. Advanced applications

We now use quadratic reciprocity to show for any nonzero integer a that whether or not $a \equiv \square \bmod p$ for odd positive primes p is determined by $p \bmod 4a$.

Theorem 3.1. *Let $a \in \mathbf{Z}$ be nonzero. For odd positive primes p and p' not dividing a,*

$$p \equiv p' \bmod 4a \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{a}{p'}\right). \tag{3.1}$$

Proof. Write $a = \varepsilon q_1 q_2 \cdots q_r$, where $\varepsilon = \pm 1$ and the q_i's are positive primes. (Some q_i's may be the same prime.) Then

$$\left(\frac{a}{p}\right) = \left(\frac{\varepsilon}{p}\right)\left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\cdots\left(\frac{q_r}{p}\right). \tag{3.2}$$

We know, from the supplementary laws, that $(\frac{-1}{p})$ is determined by $p \bmod 4$ and $(\frac{2}{p})$ is determined by $p \bmod 8$. For an odd prime q, the formula $(\frac{q}{p}) = (-1)^{(p-1)/2\cdot(q-1)/2}(\frac{p}{q})$ shows $(\frac{q}{p})$ is determined by $p \bmod q$ if $q \equiv 1 \bmod 4$ (then the power of -1 out front is 1) and by $p \bmod 4q$ if $q \equiv 3 \bmod 4$. Thus, in all cases, $(\frac{q}{p})$ is determined by $p \bmod 4q$ for any odd prime q. This is also true when $q = 2$ (a condition mod 8) and $q = -1$ (a condition mod 4).

Since each $(\frac{q_i}{p})$ is determined by $p \bmod 4q_i$, the Chinese remainder theorem tells us, by (3.2), that $(\frac{a}{p})$ is determined by $p \bmod 4a$, which is what we wanted to show. □

Equation (3.1) is striking: the Legendre symbol was defined to be periodic in its "numerator," and quadratic reciprocity tells us the Legendre symbol has a less obvious periodicity in its "denominator." In fact, (3.1) is essentially equivalent to the main law of quadratic reciprocity, and it was in the form (3.1) that Euler first discovered quadratic reciprocity.

If $a \in \mathbf{Z}$ is a perfect square, then obviously $(\frac{a}{p}) = 1$ for all odd primes p not dividing a. Does this property characterize perfect squares? Yes, and we'll now prove it with quadratic reciprocity. We will actually prove the contrapositive:

Theorem 3.2. *Let a be an integer which is not a perfect square. Then there are infinitely many primes p such that $(\frac{a}{p}) = -1$.*

Proof. Let $a = bc^2$, where b is a squarefree. Then $b \neq 1$. We have $(\frac{a}{p}) = (\frac{b}{p})$ for all p not dividing a, so we can work with b instead of a. That is, we can assume a is squarefree and $a \neq 1$. We consider four cases: $a = -1$, $a = 2$, $a = -2$, and a has an odd prime factor. The first three cases can be settled by the handout Square Applications I, which applies square patterns to primes in arithmetic progressions: each of the congruence conditions

$p \equiv 3 \bmod 4$, $p \equiv 3 \bmod 8$, and $p \equiv 7 \bmod 8$ is satisfied by infinitely many primes p, and that shows each of the Legendre symbols $(\frac{-1}{p})$, $(\frac{2}{p})$, and $(\frac{-2}{p})$ takes the value -1 at an infinite set of primes p.

Now we look at squarefree a with an odd prime factor:

$$a = (-1)^{e_0} 2^{e_1} \ell_1 \ell_2 \cdots \ell_r,$$

where e_0 and e_1 are 0 or 1, and the ℓ_i's are distinct odd positive primes with $r \geq 1$.

Let p be a prime not dividing $2a$. Then

$$\begin{aligned}
\left(\frac{a}{p}\right) &= \left(\frac{-1}{p}\right)^{e_0} \left(\frac{2}{p}\right)^{e_1} \left(\frac{\ell_1}{p}\right) \cdots \left(\frac{\ell_r}{p}\right) \\
&= (-1)^{e_0 \frac{p-1}{2}} (-1)^{e_1 \frac{p^2-1}{8}} (-1)^{\frac{p-1}{2}\frac{\ell_1-1}{2}} \left(\frac{p}{\ell_1}\right) \cdots (-1)^{\frac{p-1}{2}\frac{\ell_r-1}{2}} \left(\frac{p}{\ell_r}\right) \\
&= (-1)^{e_0 \frac{p-1}{2}} (-1)^{e_1 \frac{p^2-1}{8}} (-1)^{\frac{p-1}{2}\left(\frac{\ell_1-1}{2} + \cdots + \frac{\ell_r-1}{2}\right)} \left(\frac{p}{\ell_1}\right) \cdots \left(\frac{p}{\ell_r}\right) \\
&= (-1)^{\frac{p-1}{2}\left(e_0 + \frac{\ell_1-1}{2} + \cdots + \frac{\ell_r-1}{2}\right)} (-1)^{e_1 \frac{p^2-1}{8}} \left(\frac{p}{\ell_1}\right) \cdots \left(\frac{p}{\ell_r}\right),
\end{aligned}$$

where we used quadratic reciprocity (all parts of it) in the second equation.

For odd integers m, set

$$f(m) = (-1)^{\frac{m-1}{2}}, \quad g(m) = (-1)^{\frac{m^2-1}{8}}, \quad h(m) = \left(\frac{m}{\ell_1}\right) \cdots \left(\frac{m}{\ell_r}\right).$$

From early problem sets in the course, f is multiplicative (*i.e.*, $f(mn) = f(m)f(n)$ for odd m and n) and g is multiplicative. (Did you wonder what the point of those old homework problems was? Now you know) By the multiplicativity of the Legendre symbols, h is multiplicative. For odd m, let

$$k(m) = f(m)^{e_0 + \frac{\ell_1-1}{2} + \cdots + \frac{\ell_r-1}{2}} g(m)^{e_1} h(m).$$

Since f, g, and h are multiplicative, so is k and its values are ± 1. By our above work, $(\frac{a}{p}) = k(p)$ for positive primes p not dividing $2a$. We will show $k(p) = -1$ for infinitely many primes p.

Assume we have primes $p_1, \ldots, p_t$ such that $(\frac{a}{p_i}) = -1$ for $i = 1, \ldots, t$. We want to find a new prime with this property. (Initially, we have no such primes, so the reader could take $t = 0$.) Choose m such that

$$\left(\frac{m}{\ell_1}\right) = -1, \quad m \equiv 1 \bmod 8\ell_2 \cdots \ell_r p_1 \cdots p_t.$$

(When $t = 0$, interpret the empty product $p_1 \cdots p_t$ as 1.) Such m exist by the Chinese remainder theorem: the first condition is a congruence constraint on $m \bmod \ell_1$ and the second congruence constraint involves a modulus relatively prime to ℓ_1. We can adjust m by adding any multiple of $8\ell_1 \cdots \ell_r p_1 \cdots p_t$, so we may assume our m is positive.

Since $m \equiv 1 \bmod 8$, we have m odd, $f(m) = 1$, and $g(m) = 1$. Also, $(\frac{m}{\ell_j}) = 1$ for $j = 2, \ldots, r$, so

$$k(m) = \left(\frac{m}{\ell_1}\right) = -1.$$

Because k is multiplicative and its values are ± 1, that $k(m) = -1$ and $m > 0$ forces $k(p) = -1$ for some prime factor p of m. Since $m \equiv 0 \bmod p$ and $m \equiv 1 \bmod p_i$ by

construction, p is not one of $p_1, \ldots, p_t$. Thus p is a new prime such that $(\frac{a}{p}) = -1$, so we are done. □

Remark 3.3. It is natural to ask, given any $n \geq 2$, if the congruence $x^n \equiv a \bmod p$ is solvable for all primes p only when a is an nth power in $\mathbf{Z}$. We just used quadratic reciprocity to verify this when $n = 2$. It it is also true when $n = 3, 4, 5, 6$, and 7, but *not* when $n = 8$! Explicitly, the congruence $x^8 \equiv 16 \bmod p$ has a solution for all prime p, but 16 is not an 8th power in $\mathbf{Z}$.

Corollary 3.4. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be a 2-variable quadratic polynomial with integral coefficients a, b, and c. If the congruence $Q(x, y) \equiv 0 \bmod p$ has a solution $(x, y) \not\equiv (0, 0) \bmod p$ for all but finitely many primes p, then the equation $Q(x, y) = 0$ has an integral solution besides $(0, 0)$.*

Proof. We will basically show that the hypothesis of the theorem forces the "discriminant" $b^2 - 4ac$ to be a perfect square, so $Q(x, y)$ factors as a polynomial and then we will be able to read off an integral solution to $Q = 0$.

If $a = 0$ then $Q(1, 0) = 0$, so we may take $a \neq 0$.

Completing the square when $a \neq 0$,

$$Q(x, y) = \frac{(2ax + by)^2 + (4ac - b^2)y^2}{4a} = \frac{(2ax + by)^2 - (b^2 - 4ac)y^2}{4a}.$$

Let $d = b^2 - 4ac$ and $\widetilde{Q}(u, v) = u^2 - dv^2$, so $\widetilde{Q}(u, v)$ has integral coefficients and

$$Q(x, y) = \frac{1}{4a}\widetilde{Q}(2ax + by, y). \tag{3.3}$$

If we work over $\mathbf{Q}$, then a linear change of variables lets us turn solutions to $Q(x, y) = 0$ into solutions to $\widetilde{Q}(u, v) = 0$ and conversely: $(u, v) = (2ax + by, y)$ and $(x, y) = ((u - bv)/2a, v)$. The exact same ideas connect solutions to $Q(x, y) \equiv 0 \bmod p$ and $\widetilde{Q}(u, v) \equiv 0 \bmod p$ provided p does not divide $4a$. Why? Well, the point about $4a$ is that it is in a denominator on the right side of (3.3), so if we want to reduce modulo p we should avoid p dividing $4a$. Actually, it's a little easier to just clear the denominator and argue that way: multiplying (3.3) by $4a$ turns it into

$$4aQ(x, y) = \widetilde{Q}(2ax + by, y), \tag{3.4}$$

where both sides only involve integer coefficients. For p not dividing $4a$, reduce (3.4) modulo p. Since $4a \not\equiv 0 \bmod p$, $Q(x_0, y_0) \equiv 0 \bmod p$ if and only if $\widetilde{Q}(2ax_0 + by_0, y_0) \equiv 0 \bmod p$. The correspondence $(x_0, y_0) \bmod p \mapsto (2ax_0 + by_0, y_0) \bmod p$ is invertible, with inverse being $(u_0, v_0) \bmod p \mapsto c(u_0 - bv_0), v_0) \equiv 0 \bmod p$, where $c(2a) \equiv 1 \bmod p$. (That is, c is the mod p version of $1/2a$.) In this correspondence between solutions of $Q(x, y) \equiv 0 \bmod p$ and $\widetilde{Q}(u, v) \equiv 0 \bmod p$, the choice $(0, 0) \bmod p$ goes to itself in both directions. Therefore $Q(x, y) \equiv 0 \bmod p$ has a solution besides $(0, 0) \bmod p$ if and only if $\widetilde{Q}(u, v) \equiv 0 \bmod p$ does.

By hypothesis, there is a finite (perhaps empty) set S of primes such that for any prime $p \notin S$ the congruence $Q(x, y) \equiv 0 \bmod p$ has a solution besides $(0, 0) \bmod p$. Therefore if $p \notin S$ and p does not divide $4a$, $\widetilde{Q}(u, v) \equiv 0 \bmod p$ has a solution besides $(0, 0) \bmod p$. From the definition of $\widetilde{Q}$, this means $u^2 \equiv dv^2 \bmod p$ has a solution besides $(0, 0) \bmod p$. When $v \not\equiv 0 \bmod p$ we can divides both sides by v^2 to see that $d \equiv \square \bmod p$. Thus, for all p outside the finite set S together with the prime factors of $4a$, d is a square modulo p. It follows by Theorem 3.2 that d is a perfect square in $\mathbf{Z}$.

Write $d = n^2$. Then $\widetilde{Q}(u,v) = u^2 - n^2v^2$, so $\widetilde{Q}(n,1) = 0$. In terms of Q this becomes $Q((n-b)/2a, 1) = 0$, so $Q(n-b, 2a) = 0$. As $a \neq 0$, $(n-b, 2a) \neq (0,0)$, so we found an integral solution to $Q = 0$ besides $(0,0)$. □

4. The Jacobi symbol and Solovay–Strassen Test

Our next application of quadratic reciprocity is a description of the first "probabilistic" primality test. It is due to Solovay and Strassen (1976), and is based on a consideration of Euler's congruence for the Legendre symbol with a composite modulus, which we will have to define.

Recall that Fermat's little theorem let to a pseudo-probabilistic primality test: given an integer $n > 1$, pick random a from 1 to $n-1$ and see if Fermat's little congruence $a^{n-1} \equiv 1 \bmod n$ holds. If it ever fails for an a from 1 to $n-1$ then n has to be composite. If Fermat's little congruence works for many random choices of a, we may expect on probabilistic grounds that n is prime. In the Fermat's little theorem handout we showed that if n is composite then at least 50% of the integers modulo n will fail Fermat's little congruence as long as some unit fails the test. So there's a catch: n could be composite and all units a mod n satisfy $a^{n-1} \equiv 1 \bmod n$. Such n are called Carmichael numbers, there are infinitely many of them, and their existence is a reason that the Fermat little theorem test is not a true probabilistic primality test: for composite n we are not always assured that a large proportion of integers modulo n fail the test.

The Solovay-Strassen probabilistic primality test, which we will describe below, is a real probabilistic test: it involves testing a congruence modulo n which, if n is composite, is *guaranteed* to have at least 50% counterexamples. In other words, this test has no analogue of the Carmichael numbers. First we will explain the test and then we will use quadratic reciprocity to show the test has counterexamples for any (odd) composite n.

While Fermat's little congruence is an extension of $a^{p-1} \equiv 1 \bmod p$ to composite moduli, the Solovay-Strassen test uses an extension of Euler's congruence $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ to composite odd moduli. What does this mean? While we can replace the left side with $a^{(n-1)/2}$ for odd $n \in \mathbf{Z}^+$, what meaning should be given to $(\frac{a}{n})$ if n is a general odd number? We have given no definition yet of such a symbol with non-prime "denominator." We now provide a meaning for such a symbol by just extending the Legendre symbol in the denominator multiplicatively, by *fiat*.

Definition 4.1. Let n be an odd integer with $n > 1$. Factor n into primes as $n = p_1p_2\cdots p_r$, where the p_i's are odd positive primes (perhaps a prime appears more than once). For $a \in \mathbf{Z}$, define the *Jacobi symbol* $(\frac{a}{n})$ to be

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right).$$

In particular, $(\frac{a}{n}) = \pm 1$ if $(a,n) = 1$ and $(\frac{a}{n}) = 0$ if $(a,n) \neq 1$. Set $(\frac{a}{1}) = 1$ for all $a \in \mathbf{Z}$.

Example 4.2. $(\frac{8}{15}) = (\frac{8}{3})(\frac{8}{5}) = (\frac{2}{3})(\frac{3}{5}) = (-1)(-1) = 1$.

Example 4.3. $(\frac{37}{45}) = (\frac{37}{3})^2(\frac{37}{5}) = (\frac{1}{3})^2(\frac{2}{5}) = (1)(-1) = -1$.

Example 4.4. If $(a,9) = 1$, $(\frac{a}{9}) = (\frac{a}{3})^2 = 1$. If $3|a$, then $(\frac{a}{9}) = 0$.

While $(\frac{a}{n}) = \pm 1$ for $(a,n) = 1$, it is *false* that $(\frac{a}{n}) = 1 \Longleftrightarrow a \equiv \square \bmod n$. For instance, in Example 4.2 we found $(\frac{8}{15}) = 1$, but $8 \not\equiv \square \bmod 15$: the squares modulo 15 are $0, 1, 4, 6, 9$,

and 10. Similarly, $(\frac{2}{9}) = 1$, but $2 \not\equiv \square \bmod 9$. That $(\frac{a}{n}) = 1$ is not the same as $a \equiv \square \bmod n$ might at first seem strange, but there is nothing contradictory going on. Remember, we defined the Jacobi symbol $(\frac{a}{n})$ for composite odd $n > 0$ *not* in terms of squares or non-squares modulo n, but simply as a multiplicative extension of the Legendre symbol. That the value of $(\frac{a}{n})$ may or may not detect when $a \equiv \square \bmod n$ is something which has to be checked, and we see by examples that it does not work. (Exception: if $(\frac{a}{n}) = -1$, then some $(\frac{a}{p_i}) = -1$, so $a \not\equiv \square \bmod p_i$ and thus $a \not\equiv \square \bmod n$, so $(\frac{a}{n}) = -1$ does imply $a \not\equiv \square \bmod n$. The converse, however, is definitely false: when $(\frac{a}{n}) = 1$ we *can't* be sure that $a \equiv \square \bmod n$.)

While the Jacobi symbol does not have a simple quadratic interpretation like the Legendre symbol, the Jacobi symbol does satisfy many of the *computational rules* of the Legendre symbol:

- If $a \equiv b \bmod n$, then $(\frac{a}{n}) = (\frac{b}{n})$.
- For $a, b \in \mathbf{Z}$, $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$.
- $(\frac{-1}{n}) = (-1)^{(n-1)/2}$.
- $(\frac{2}{n}) = (-1)^{(n^2-1)/8}$
- For odd positive m and n,

$$\left(\frac{n}{m}\right) = (-1)^{(m-1)/2\cdot(n-1)/2}\left(\frac{m}{n}\right).$$

See the appendix for proofs of these rules, which largely proceed by induction on the number of prime factors in one of the terms inside the Jacobi symbol. The base case of the induction is the main law of quadratic reciprocity law for the Legendre symbol.[1] (There is a further extension of the Jacobi symbol, due to Kronecker, which allows $n < 0$ and n even, but we do not need this and don't discuss it.) The 3rd, 4th, and 5th properties are called Jacobi reciprocity, with the last one being the main law and the other two being the supplementary laws.

The importance of these computational rules holding for Jacobi symbols is that we can compute with a Jacobi symbol much like with a Legendre symbol, and thus we can avoid having to factor except for pulling out powers of 2. This leads to a fast method of computing Legendre symbols without factoring the "numerator" into primes.

Example 4.5. The number 101 is prime. We compute the Legendre symbol $(\frac{55}{101})$ in two ways, first by the usual quadratic reciprocity rules and then by viewing this as a Jacobi symbol.

For the first way, we factor $55 = 5 \cdot 11$ and get

$$\left(\frac{55}{101}\right) = \left(\frac{5}{101}\right)\left(\frac{11}{101}\right) = \left(\frac{101}{5}\right)\left(\frac{101}{11}\right) = \left(\frac{1}{5}\right)\left(\frac{2}{11}\right) = (1)(-1) = -1.$$

For the second way, we just note 55 is odd and compute

$$\left(\frac{55}{101}\right) = \left(\frac{101}{55}\right) = \left(\frac{46}{55}\right) = \left(\frac{2}{55}\right)\left(\frac{23}{55}\right) = -\left(\frac{55}{23}\right) = -\left(\frac{9}{23}\right) = -1.$$

For an even faster calculation by the second way,

$$\left(\frac{55}{101}\right) = \left(\frac{101}{55}\right) = \left(\frac{-9}{55}\right) = \left(\frac{-1}{55}\right) = (-1)^{(55-1)/2} = -1.$$

[1] This is an example of a proof by induction with a nontrivial base case!

Example 4.6. The number 127 is prime. We will compute $(\frac{105}{127})$, first using Legendre symbols and then using Jacobi symbols. To use Legendre symbols, we factor $105 = 3 \cdot 5 \cdot 7$, so

$$\left(\frac{105}{127}\right) = \left(\frac{3}{127}\right)\left(\frac{5}{127}\right)\left(\frac{7}{127}\right).$$

We calculate these three Legendre symbols separately. First,

$$\left(\frac{3}{127}\right) = -\left(\frac{127}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Second,

$$\left(\frac{5}{127}\right) = \left(\frac{127}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

Finally,

$$\left(\frac{7}{127}\right) = -\left(\frac{127}{7}\right) = -\left(\frac{1}{7}\right) = -1.$$

Therefore

$$\left(\frac{105}{127}\right) = (-1)(-1)(-1) = -1.$$

We now compute $(\frac{105}{127})$ as a Jacobi symbol:

$$\begin{aligned}
\left(\frac{105}{127}\right) &= \left(\frac{127}{105}\right) \\
&= \left(\frac{22}{105}\right) \\
&= \left(\frac{2}{105}\right)\left(\frac{11}{105}\right) \\
&= (1)\left(\frac{105}{11}\right) \text{ since } 105 \equiv 1 \bmod 8 \\
&= \left(\frac{6}{11}\right) \\
&= \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) \\
&= (-1)\cdot(-1)\left(\frac{11}{3}\right) \\
&= \left(\frac{2}{3}\right) \\
&= -1.
\end{aligned}$$

Example 4.7. For odd $n > 1$, $(\frac{2}{n}) = (\frac{-1}{n})(\frac{-2}{n}) = (\frac{-1}{n})(\frac{n-2}{n})$ since $-2 \equiv n-2 \bmod n$. Since n is odd, either n or $n-2$ is 1 mod 4, so $(\frac{n-2}{n}) = (\frac{n}{n-2})$ by the reciprocity for the Jacobi symbol. Therefore

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{n}{n-2}\right) = \left(\frac{-1}{n}\right)\left(\frac{2}{n-2}\right).$$

Thus we have a recursion linking the Jacobi symbols $(\frac{2}{n})$ and $(\frac{2}{n-2})$. Repeating this recursion,

$$\left(\frac{2}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{-1}{n-2}\right)\left(\frac{-1}{n-4}\right)\cdots\left(\frac{-1}{5}\right)\left(\frac{2}{3}\right).$$

Using the rule $(\frac{-1}{m}) = (-1)^{(m-1)/2}$ for odd $m > 0$, we obtain

$$\begin{aligned}\left(\frac{2}{n}\right) &= (-1)^{(n-1)/2}(-1)^{(n-3)/2}(-1)^{(n-5)/2}\cdots(-1)^{(5-1)/2}(-1)\\ &= (-1)^{(1/2)((n-1)+(n-3)+(n-5)+\cdots+4)}(-1).\end{aligned}$$

Since $n-1, n-3, n-5, \ldots, 4$ are consecutive even numbers from $n-1$ down to 4, their sum divided by 2 is the sum of the integers from $(n-1)/2$ down to 2, which is

$$2+3+\cdots+\frac{n-1}{2} = \frac{1}{2}\left(2+\frac{n-1}{2}\right)\left(\frac{n-1}{2}-1\right) = \frac{n^2-9}{8}.$$

Thus

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-9)/8}(-1) = (-1)^{(n^2-1)/8}.$$

Thus we have *derived* the supplementary law for $(\frac{2}{n})$ from the main law of Jacobi reciprocity, which is about odd numbers! In particular, from the main law of Jacobi reciprocity we have proved the supplementary law for $(\frac{2}{p})$ in ordinary quadratic reciprocity. (There is no circular argument here; the proof of the main law of Jacobi reciprocity does not depend on the supplementary law for the Legendre symbol $(\frac{2}{p})$. See the appendix.)

There is one rule for the Legendre symbol which we did not list for the Jacobi symbol: an analogue of Euler's congruence $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$ for $(a,p) = 1$. In fact, the analogue of this congruence for composite n always has counterexamples, and this is the basis for Solovay and Strassen's probabilistic primality test.

Example 4.8. Let $n = 2821$. While $2^{n-1} \equiv 1 \bmod n$, we have $2^{(n-1)/2} = 2^{1410} \equiv 1520 \bmod 2821$, so $2^{(n-1)/2} \not\equiv (\frac{2}{2821}) \bmod 2821$.

Theorem 4.9 (Solovay-Strassen)**.** *Let n be a positive odd composite number. There is some a with $(a,n) = 1$ and $a^{(n-1)/2} \not\equiv (\frac{a}{n}) \bmod n$.*

The crucial point is that there is a *unit* mod n which violates Euler's congruence.

Proof. We take two cases: n is squarefree and n has a multiple prime factor.

Suppose $n = p_1p_2\cdots p_r$ is squarefree, with $r \geq 2$ (n is not prime!). Pick $b \not\equiv 0 \bmod p_1$ such that $b \not\equiv \square \bmod p_1$. There is such b since only half the nonzero numbers mod p_1 are squares. Use the Chinese remainder theorem to select $a \in \mathbf{Z}$ satisfying

$$a \equiv b \bmod p_1, \quad a \equiv 1 \bmod p_2\cdots p_r.$$

Then $(a,n) = 1$ and

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right) = \left(\frac{b}{p_1}\right) = -1.$$

We will show by contradiction that $a^{(n-1)/2} \not\equiv (\frac{a}{n}) \bmod n$. If $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ then $a^{(n-1)/2} \equiv -1 \bmod n$. Since $a \equiv 1 \bmod p_2\cdots p_r$, if we reduce the congruence $a^{(n-1)/2} \equiv -1 \bmod n$ to the modulus $p_2\cdots p_r$, which divides n, we get

$$1 \equiv -1 \bmod p_2\cdots p_r,$$

which is a contradiction since $p_2 \cdots p_r > 2$.

For the second part of the proof, suppose n has a multiple prime factor, say $n = p^k m$ with $k \geq 2$ and $(p, m) = 1$. By the Chinese remainder theorem, there is an $a \in \mathbf{Z}$ satisfying

$$a \equiv 1 + p \bmod p^k, \quad a \equiv 1 \bmod m.$$

That means a is relatively prime to p^k and to m, so $(a, n) = 1$. If $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$ then squaring gives us $a^{n-1} \equiv 1 \bmod n$. We can reduce modulo p^k (a factor of n) and obtain $a^{n-1} \equiv 1 \bmod p^k$, so $(1+p)^{n-1} \equiv 1 \bmod p^k$. We are going to show this last congruence is false, so $a^{(n-1)/2} \not\equiv (\frac{a}{n}) \bmod n$.

It is left as an exercise for the reader to show that for any $x, y \in \mathbf{Z}$ and prime p,

$$x \equiv y \bmod p^t \Longrightarrow x^p \equiv y^p \bmod p^{t+1}$$

for any integer $t \geq 1$. So starting from $1 + p \equiv 1 \bmod p$ we get $(1+p)^p \equiv 1 \bmod p^2$. Then raising to the pth power again, $(1+p)^{p^2} \equiv 1 \bmod p^3$. Continuing in this pattern (use induction),

$$(1+p)^{p^{k-1}} \equiv 1 \bmod p^k.$$

Therefore the order of $1 + p \bmod p^k$ divides p^{k-1}, so the order is a power of p. The order is not 1 since $1 + p \not\equiv 1 \bmod p^k$ (as $k \geq 2$!).

If $(1+p)^{n-1} \equiv 1 \bmod p^k$, then $n - 1$ is divisible by the order of $1 + p \bmod p^k$, so $n - 1$ is divisible by a power of p greater than 1. That means $n \equiv 1 \bmod p$, but by definition n is divisible by p, so we have a contradiction. (Notice this second part of the proof was really not a serious use of Jacobi symbols, but the first part of the proof was.) □

Now we can explain why at least half the numbers $a \bmod n$ do not satisfy $(a, n) = 1$ and

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n \tag{4.1}$$

when n is odd and composite. Set

$$A = \left\{a \in (\mathbf{Z}/(n))^\times : a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n\right\},$$

$$B = \left\{a \in (\mathbf{Z}/(n))^\times : a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \bmod n\right\},$$

$$C = \{a \in \mathbf{Z}/(n) : (a, n) \neq 1\}.$$

So A, B, and C are disjoint and fill up $\mathbf{Z}/(n)$. We want to show $\#B + \#C \geq n/2$.

We know there is some $b_0 \in B$. We will show $Ab_0 = \{ab : a \in A\} \subset B$. For any $a \in A$, the product ab_0 is a unit modulo n, so $ab_0 \in A$ or $ab_0 \in B$. To show $ab_0 \in B$ we argue by contradiction: if $ab_0 \in A$ then $(ab_0)^{(n-1)/2} \equiv (\frac{ab_0}{n}) \bmod n$. Also

$$(ab_0)^{(n-1)/2} = a^{(n-1)/2} b_0^{(n-1)/2} \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \bmod n,$$

so

$$\left(\frac{ab_0}{n}\right) \equiv \left(\frac{a}{n}\right) b_0^{(n-1)/2} \bmod n.$$

Since $(\frac{ab_0}{n}) = (\frac{a}{n})(\frac{b_0}{n})$, we can cancel the common factor $(\frac{a}{n}) = \pm 1$ from both sides and we are left with $(\frac{b_0}{n}) \equiv b_0^{(n-1)/2} \bmod n$. But this isn't true, since it violates the meaning of b_0 lying in B. Therefore $ab_0 \notin A$, so $ab_0 \in B$.

Now that we know $Ab_0 \subset B$, we have $\#B \geq \#(Ab_0) = \#A$. Therefore

$$n = \#A + \#B + \#C \geq \#A + \#A + 0 = 2\#A,$$

so $\#A \leq n/2$. Hence

$$\#B + \#C = n - \#A \geq n - \frac{n}{2} = \frac{n}{2}.$$

This means the set of counterexamples to (4.1) is at least half the integers modulo n. Let's state this officially, as a means of pinning down how the Jacobi symbol distinguishes primes and composites.

Theorem 4.10 (Solovay, Strassen)**.** *Let n be a positive odd integer. If n is prime then $\#\{a \bmod n : a^{(n-1)/2} \equiv (\frac{a}{n})\} = n$. If n is composite then $\#\{a \bmod n : a^{(n-1)/2} \equiv (\frac{a}{n})\} \leq n/2$.*

Thus, we can deservedly say, for odd composite n, that we have at least a 50% chance of discovering n is composite by testing (4.1) for a random choice of a. Doing this test for, say, 20 choices of a and finding no counterexamples to (4.1) suggests n is prime with a "probability" of $1/2^{20}$ that we are incorrect. This is what Solovay and Strassen's test is.

Although the Solovay-Strassen test was, historically, the first probabilistic primality test, it was soon eclipsed by the Miller-Rabin test, which is easier to implement than the Solovay-Strassen test and more effective: the proportion of counterexamples is at least 75%. However, it is not as easy to understand the Miller-Rabin test (or where the 75% comes from).

5. Using Jacobi Reciprocity for the Legendre Symbol

In Theorem 3.1 we proved that for fixed nonzero $a \in \mathbf{Z}$, whether or not $a \equiv \square \bmod p$, for $(p, 2a) = 1$, only depends on $p \bmod 4a$. Our earlier numerical data suggested several refinements of this:

(1) If $p \equiv 1 \bmod 4a$ then $a \equiv \square \bmod p$.
(2) For $a > 0$, if $p \equiv -1 \bmod 4a$ then $a \equiv \square \bmod p$.
(3) For $a < 0$, if $p \equiv -1 \bmod 4a$ then $a \not\equiv \square \bmod p$.
(4) If p, p', and p'' are odd positive primes such that $pp' \equiv p'' \bmod 4a$, $a \equiv \square \bmod p$, and $a \equiv \square \bmod p'$, then $a \equiv \square \bmod p''$.
(5) If $a \equiv 1 \bmod 4$ then $(\frac{a}{p})$ is determined by $p \bmod a$, not just $p \bmod 4a$, and the four previous refinements are true with modulus $4a$ replaced by modulus a.

We will now prove all of these using Jacobi reciprocity, even though they are all about Legendre symbols. We will formulate these results more generally for Jacobi symbols to streamline the proofs (Jacobi reciprocity does not require factoring into primes besides powers of 2), and then the versions for Legendre symbols just fall out as special cases. The Jacobi symbol versions of the above results will concern the value of $(\frac{a}{n})$, which is not telling us whether or not $a \equiv \square \bmod n$ unless n is a prime.

Theorem 5.1. *Let a and b be nonzero integers with b odd and positive. If $b \equiv 1 \bmod 4a$ then $(\frac{a}{b}) = 1$. In particular, for prime p if $p \equiv 1 \bmod 4a$ then $a \equiv \square \bmod p$.*

Proof. Since $b \equiv 1 \bmod 4a$, $(a, b) = 1$. Write $a = (-1)^{e_0} 2^{e_1} a'$, where a' is odd and positive. Then

$$\left(\frac{a}{b}\right) = \left(\frac{-1}{b}\right)^{e_0} \left(\frac{2}{b}\right)^{e_1} \left(\frac{a'}{b}\right).$$

We will use Jacobi reciprocity to show every term on the right equals 1.

Since $b \equiv 1 \bmod 4$, $(\frac{-1}{b}) = (-1)^{(b-1)/2} = 1$. If a is even then 8 is a factor of $4a$, so $b \equiv 1 \bmod 8$, which implies $(\frac{2}{b}) = 1$, so $(\frac{2}{b})^{e_1} = 1$. If a is odd then $e_1 = 0$ so we still have $(\frac{2}{b})^{e_1} = 1$. Finally, since a' is a factor of a we have $b \equiv 1 \bmod 4a'$, so the main law of

Jacobi reciprocity gives us $(\frac{a'}{b}) = (-1)^{(a'-1)/2\cdot(b-1)/2}(\frac{b}{a'})$. The exponent on -1 is even since $b \equiv 1 \bmod 4$, and $(\frac{b}{a'}) = 1$ since $b \equiv 1 \bmod a'$.

The interpretation of this result for $b = p$ a prime comes from the interpretation of $(\frac{a}{p})$ in terms of squares mod p. □

Theorem 5.2. *Let a and b be nonzero integers with b odd, positive, and $b \equiv -1 \bmod 4a$. Then $(\frac{a}{b}) = 1$ if and only if $a > 0$. In particular, for prime p with $p \equiv -1 \bmod 4a$, $a \equiv \square \bmod p$ if and only if $a > 0$.*

Proof. Since $b \equiv -1 \bmod 4a$, $(a, b) = 1$. First suppose $a > 0$. Write $a = 2^{e_1}a'$ where a' is odd and positive. Then

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^{e_1}\left(\frac{a'}{b}\right).$$

If a is even then 8 is a factor of $4a$, so $b \equiv -1 \bmod 8$, which implies $(\frac{2}{b}) = 1$ by the supplementary law of Jacobi reciprocity, so $(\frac{2}{b})^{e_1} = 1$. If a is odd then $e_1 = 0$ and we still have $(\frac{2}{b})^{e_1} = 1$. Either way, we get $(\frac{a}{b}) = (\frac{a'}{b})$. Since a' is a factor of a, $b \equiv -1 \bmod 4a'$, so the main law of Jacobi reciprocity tells us

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

Since $b \equiv -1 \bmod 4$, $(b-1)/2$ is odd, so the power of -1 is $(-1)^{(a'-1)/2}$. Since $b \equiv -1 \bmod a'$, $(\frac{b}{a'})$ equals $(\frac{-1}{a'}) = (-1)^{(a'-1)/2}$. Thus $(\frac{a}{b}) = (-1)^{(a'-1)/2}(-1)^{(a'-1)/2} = 1$.

Next suppose $a < 0$. Then $a = -|a|$ with $|a| > 0$ and $b \equiv -1 \bmod 4|a|$, so from the previous paragraph $(\frac{|a|}{b}) = 1$. Therefore $(\frac{a}{b}) = (\frac{-1}{b})(\frac{|a|}{b}) = (\frac{-1}{b}) = (-1)^{(b-1)/2}$. Since $b \equiv -1 \bmod 4$, $(-1)^{(b-1)/2} = -1$. □

Theorem 5.3. *If b, b', and b'' are odd, positive, relatively prime to a and $bb' \equiv b'' \bmod 4a$ then $(\frac{a}{b})(\frac{a}{b'}) = (\frac{a}{b''})$. In particular, if p, p', and p'' are odd positive primes not dividing a such that $pp' \equiv p'' \bmod 4a$, $a \equiv \square \bmod p$, and $a \equiv \square \bmod p'$ then $a \equiv \square \bmod p''$.*

Proof. Write $a = (-1)^{e_0}2^{e_1}a'$, where a' is odd and positive. By Jacobi reciprocity,

$$\begin{aligned}\left(\frac{a}{b}\right) &= \left(\frac{-1}{b}\right)^{e_0}\left(\frac{2}{b}\right)^{e_1}\left(\frac{a'}{b}\right)\\ &= (-1)^{e_0(b-1)/2}(-1)^{e_1(b^2-1)/8}(-1)^{(a'-1)/2\cdot(b-1)/2}\left(\frac{b}{a'}\right)\\ &= (-1)^{(e_0+(a'-1)/2)(b-1)/2}(-1)^{e_1(b^2-1)/8}\left(\frac{b}{a'}\right).\end{aligned}$$

There is a similar formula for $(\frac{a}{b'})$, so

$$\left(\frac{a}{b}\right)\left(\frac{a}{b'}\right) = (-1)^{(e_0+(a'-1)/2)((b-1)/2+(b'-1)/2)}(-1)^{e_1((b^2-1)/8+(b'^2-1)/8)}\left(\frac{b}{a'}\right)\left(\frac{b'}{a'}\right).$$

The two Jacobi symbols on the right multiply together to $(\frac{bb'}{a'})$, which equals $(\frac{b''}{a'})$ since $bb' \equiv b'' \bmod a$. Since

$$(-1)^{(b-1)/2+(b'-1)/2} = (-1)^{(bb'-1)/2}$$

and $bb' \equiv b'' \bmod 4$, $(-1)^{(b-1)/2+(b'-1)/2} = (-1)^{(b''-1)/2}$. Supposing a is even, so 8 is a factor of $4a$, from

$$(-1)^{(b^2-1)/8+(b'^2-1)/8} = (-1)^{((bb')^2-1)/8}$$

and $bb' \equiv b'' \bmod 8$ we have $(-1)^{(b^2-1)/8+(b'^2-1)/8} = (-1)^{(b''^2-1)/8}$, so

$$\left(\frac{a}{b}\right)\left(\frac{a}{b'}\right) = (-1)^{(e_0+(a-1)/2)(b''-1)/2}(-1)^{e_1(b''^2-1)/8}\left(\frac{b''}{a'}\right) = \left(\frac{a}{b''}\right).$$

If a is odd the whole $(\frac{2}{b})$ term just drops out of consideration and we get the same result. □

Theorem 5.4. *For $a \equiv 1 \bmod 4$ and odd positive b with $(a,b) = 1$, the value of $(\frac{a}{b})$ is determined by $b \bmod a$. In particular, for odd positive primes p whether or not $a \equiv \square \bmod p$ is determined by $p \bmod a$.*

Proof. We take cases for $a > 0$ and $a < 0$.

If $a > 0$ then by the main law of Jacobi reciprocity, $(\frac{a}{b}) = (\frac{b}{a})$ because the condition $a \equiv 1 \bmod 4$ implies $(-1)^{(a-1)/2\cdot(b-1)/2} = 1$ for any b. Obviously $(\frac{b}{a})$ only depends on $b \bmod a$.

Now suppose $a < 0$. Write $a = -a'$, so a' is odd, positive, and $a' \equiv 3 \bmod 4$. Then the main law of Jacobi reciprocity says $(\frac{a}{b}) = (\frac{-1}{b})(\frac{a'}{b}) = (-1)^{(b-1)/2}(-1)^{(a'-1)/2\cdot(b-1)/2}(\frac{b}{a'})$. Since $a' \equiv 3 \bmod 4$, $(a'-1)/2$ is odd, so $(-1)^{(a'-1)/2\cdot(b-1)/2} = (-1)^{(b-1)/2}$. Therefore $(\frac{a}{b}) = (\frac{b}{a'})$, and this last Jacobi symbol only depends on $b \bmod a'$, which is the same thing as $b \bmod a$ since $a' = |a|$. □

It is left as an exercise for the reader to reprove Theorems 5.1, 5.2, and 5.3 for congruences with modulus a rather than $4a$ when $a \equiv 1 \bmod 4$.

Appendix A. Proof of Jacobi Reciprocity

This appendix gives a proof of the reciprocity law for Jacobi symbols. It is based on notes of Neal Lima.

We begin with two properties of the Jacobi symbol which are computationally important but are not part of the law itself.

Theorem A.1. *For an odd positive integer n and integers a and b,*

1. *if $a \equiv b \bmod n$, then $(\frac{a}{n}) = (\frac{b}{n})$,*
2. *$(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$.*

Proof. If $n = 1$ then both results are obvious (all symbols equal 1). If $n > 1$, write $n = p_1p_2\cdots p_r$ where the p_i's are (not necessarily distinct) prime numbers. Since $a \equiv b \bmod n$, $a \equiv b \bmod p_i$ for all p_i, so $(\frac{a}{p_i}) = (\frac{b}{p_i})$. Then

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

That takes care of (1). For (2), $(\frac{ab}{p_i}) = (\frac{a}{p_i})(\frac{b}{p_i})$ for all p_i, so

$$\begin{aligned}\left(\frac{ab}{n}\right) &= \left(\frac{ab}{p_1}\right)\left(\frac{ab}{p_2}\right)\cdots\left(\frac{ab}{p_r}\right)\\ &= \left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)\\ &= \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_1}\right)\left(\frac{b}{p_2}\right)\cdots\left(\frac{b}{p_r}\right)\\ &= \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).\end{aligned}$$

□

Lemma A.2. *For any odd integers a and b,*

$$(-1)^{(a-1)/2}(-1)^{(b-1)/2} = (-1)^{(ab-1)/2}, \qquad (-1)^{(a^2-1)/8}(-1)^{(b^2-1)/8} = (-1)^{((ab)^2-1)/8}.$$

Proof. We have

$$(a-1)(b-1) \equiv 0 \bmod 4,$$

so expanding the product and rearranging gives

$$(a-1)+(b-1) \equiv ab-1 \bmod 4.$$

Now divide through by 2 to get

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \bmod 2.$$

Raising -1 to both sides gives the first result. Starting from

$$(a^2-1)(b^2-1) \equiv 0 \bmod 16,$$

and expanding and rearranging in a similar way, the second formula falls out. □

Theorem A.3 (Jacobi Reciprocity)**.** *For odd positive integers m and n,*

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

$$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} 1, & \text{if } n \equiv 1,7 \bmod 8, \\ -1, & \text{if } n \equiv 3,5 \bmod 8, \end{cases}$$

and

$$\left(\frac{n}{m}\right) = (-1)^{(m-1)/2\cdot(n-1)/2}\left(\frac{m}{n}\right) = \begin{cases} \left(\frac{m}{n}\right), & \text{if } m \text{ or } n \equiv 1 \bmod 4, \\ -\left(\frac{m}{n}\right), & \text{if } m \text{ and } n \equiv 3 \bmod 4. \end{cases}$$

Proof. All parts are trivial if m or n is 1, so we may take $m > 1$ and $n > 1$. The explicit formulas for $(-1)^{(n-1)/2}$ and $(-1)^{(n^2-1)/8}$ in terms of n mod 4 and n mod 8 are straightforward to check case-by-case, and are left to the reader.

To show

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2},$$

we argue by induction on the number of prime factors of n. For our base case of one prime factor, $n = p$ is an odd prime. Then

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{(n-1)/2}$$

by a supplementary law of quadratic reciprocity for the Legendre symbol. For our inductive step, assume that the formula for $(\frac{-1}{n})$ holds for all odd positive n having k (possibly repeated) prime factors for some $k \geq 1$. Then when $n = p_1 p_2 \dots p_k p_{k+1}$ is an odd positive integer with $k+1$ prime factors,

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)\cdots\left(\frac{-1}{p_k}\right)\left(\frac{-1}{p_{k+1}}\right) = \left(\frac{-1}{p_1\cdots p_k}\right)\left(\frac{-1}{p_{k+1}}\right) \tag{A.1}$$

from the definition of the Jacobi symbol. Because $p_1 \cdots p_k$ has k prime factors and p_{k+1} is prime, we can apply our inductive hypothesis to the right side and get

$$\begin{aligned}\left(\frac{-1}{p_1\cdots p_k}\right)\left(\frac{-1}{p_{k+1}}\right) &= (-1)^{(p_1\cdots p_k-1)/2}(-1)^{(p_{k+1}-1)/2},\\ &= (-1)^{(p_1\cdots p_k-1)/2+(p_{k+1}-1)/2}. \end{aligned} \tag{A.2}$$

By the first formula in Lemma A.2, this is $(-1)^{(p_1\cdots p_kp_{k+1}-1)/2} = (-1)^{(n-1)/2}$, so our induction is complete.

To prove the formula for $(\frac{2}{n})$, carry out induction on the number of prime factors of n as done in the proof of the formula for $(\frac{-1}{n})$. At the end of the inductive step, the second formula in Lemma A.2 will be useful.

For the main law of Jacobi reciprocity, we may assume $(m,n) = 1$, since otherwise both sides of the desired formula are 0 (both Jacobi symbols vanish). We will proceed by leaving n fixed and inducting on the number of prime factors of m. For the base case of one prime factor, $m = q$ is an odd prime. Write $n = p_1p_2\dots p_k$ where all p_i are prime and none of these primes equal q (since $(m,n) = 1$). Using the definition of the Legendre symbol and quadratic reciprocity for the Legendre symbol,

$$\begin{aligned}\left(\frac{n}{q}\right) &= \left(\frac{p_1}{q}\right)\cdots\left(\frac{p_k}{q}\right)\\ &= (-1)^{(p_1-1)/2\cdot(q-1)/2}\left(\frac{q}{p_1}\right)\cdots(-1)^{(p_k-1)/2\cdot(q-1)/2}\left(\frac{q}{p_k}\right)\\ &= (-1)^{(p_1-1)/2\cdot(q-1)/2}\cdots(-1)^{(p_k-1)/2\cdot(q-1)/2}\left(\frac{q}{p_1}\right)\cdots\left(\frac{q}{p_k}\right).\end{aligned}$$

By the definition of the Jacobi symbol,

$$\left(\frac{q}{p_1}\right)\cdots\left(\frac{q}{p_k}\right) = \left(\frac{q}{n}\right),$$

so

$$\begin{aligned}\left(\frac{n}{q}\right) &= (-1)^{(p_1-1)/2\cdot(q-1)/2}\cdots(-1)^{(p_k-1)/2\cdot(q-1)/2}\left(\frac{q}{n}\right)\\ &= (-1)^{(p_1-1)/2\cdot(q-1)/2+\cdots+(p_k-1)/2\cdot(q-1)/2}\left(\frac{q}{n}\right)\\ &= \left((-1)^{(p_1-1)/2+\cdots+(p_k-1)/2)}\right)^{(q-1)/2}\left(\frac{q}{n}\right).\end{aligned} \tag{A.3}$$

Using an extended form of Lemma A.2 with several odd parameters rather than just two,,

$$(-1)^{(p_1-1)/2+\cdots+(p_k-1)/2} = (-1)^{(p_1\cdots p_k-1)/2} = (-1)^{(n-1)/2},$$

so

$$\left(\frac{n}{q}\right) = \left((-1)^{(n-1)/2}\right)^{(q-1)/2}\left(\frac{q}{n}\right) = (-1)^{(n-1)/2\cdot(q-1)/2}\left(\frac{q}{n}\right),$$

which completes the base case (of m being an odd prime).

For the inductive step, assume the main law of Jacobi reciprocity holds when m has k prime factors (counted with multiplicity). Now suppose $m = q_1\dots q_kq_{k+1}$, where all q_i are odd primes and not necessarily distinct. We want to show the main law of Jacobi reciprocity holds for this value of m.

We know that

$$\left(\frac{n}{m}\right) = \left(\frac{n}{q_1}\right)\cdots\left(\frac{n}{q_k}\right)\left(\frac{n}{q_{k+1}}\right) = \left(\frac{n}{q_1\cdots q_k}\right)\left(\frac{n}{q_{k+1}}\right)$$

by the definition of the Jacobi symbol. By the base case and inductive hypothesis, we can evaluate the two terms in the last expression to get

$$\begin{aligned}\left(\frac{n}{m}\right) &= (-1)^{(n-1)/2\cdot(q_1\cdots q_k-1)/2}\left(\frac{q_1\cdots q_k}{n}\right)(-1)^{(n-1)/2\cdot(q_{k+1}-1)/2}\left(\frac{q_{k+1}}{n}\right)\\ &= (-1)^{(n-1)/2\cdot(q_1\cdots q_k-1)/2+(n-1)/2\cdot(q_{k+1}-1)/2}\left(\frac{q_1\cdots q_kq_{k+1}}{n}\right)\\ &= \left((-1)^{(q_1\cdots q_k-1)/2+(q_{k+1}-1)/2)}\right)^{(n-1)/2}\left(\frac{m}{n}\right). \qquad \text{(A.4)}\end{aligned}$$

By Lemma A.2,

$$(-1)^{(q_1\cdots q_k-1)/2+(q_{k+1}-1)/2} = (-1)^{(q_1\cdots q_kq_{k+1}-1)/2} = (-1)^{(m-1)/2}.$$

Feed this into (A.4) to conclude

$$\left(\frac{n}{m}\right) = \left((-1)^{(m-1)/2}\right)^{(n-1)/2}\left(\frac{m}{n}\right) = (-1)^{(m-1)/2\cdot(n-1)/2}\left(\frac{m}{n}\right).$$

Therefore we have shown that Jacobi reciprocity holds for all odd relatively prime positive integers m and n. □