7 Quadratic Reciprocity

We are now ready to work towards the major result of this course, Euler's famous law of Quadratic Reciprocity.

7.1 Power residues

For further reading on the material in this subsection, consult **Rosen 9.4, 11.1, PMF 11.1, Stein 4.1, Shoup 2.8**.

Definition 7.1. Let m be a natural number. We say a is a *kth power residue of m* if the congruence $x^k \equiv a \mod n$ has a solution, or in other words if a has a kth root modulo m. Otherwise we say a is a *nonresidue*.

Remark 7.2. Some sources, including Rosen, claim a residue has to be relatively prime to m by definition. This convention makes some theorems more awkward and others less.

Example 7.3. Under our convention, 0 is a kth power residue modulo m for any $k, m \in \mathbb{N}$. Under either convention, 1 is a kth power residue modulo m for any $k, m \in \mathbb{N}$.

Example 7.4. We can find the kth power residues modulo m simply by raising every element to the kth power. For instance, we can compute

$$\begin{array}{llll} 0^2 \equiv 0 \mod 7 & 1^2 \equiv 1 \mod 7 & 2^2 \equiv 4 \mod 7 & 3^2 \equiv 2 \mod 7 \\ & 4^2 \equiv 2 \mod 7 & 5^2 \equiv 4 \mod 7 & 6^2 \equiv 1 \mod 7 \end{array}$$

thus the second-power residues (or quadratic residues) modulo 7 are 0, 1, 2, 4. The nonresidues are 3, 5, 6,

Similarly, we can compute

$$\begin{array}{llll} 0^3 \equiv 0 \mod 7 & 1^3 \equiv 1 \mod 7 & 2^3 \equiv 1 \mod 7 & 3^3 \equiv 6 \mod 7 \\ & 4^3 \equiv 1 \mod 7 & 5^3 \equiv 6 \mod 7 & 6^3 \equiv 6 \mod 7 \end{array}$$

thus the third-power (or cubic) residues modulo 7 are 0, 1, 6, and the nonresidues are 2, 3, 4, 5.

Notice that it's easier to prove that something is a residue than to prove that it isn't: to prove something is a residue, we just need to provide a root, but to prove something is not a residue, we need to compute a power of every possible base.

This is an awful lot of computation, so we'd like to determine the set of residues more easily.

Lemma 7.5. *Let m be a positive integer with a primitive root, and let a be relatively prime to m. Then a is a kth power residue modulo m if and only if $a^{\phi(m)/d} \equiv 1 \mod m$, where $d = (k, \phi(m))$.*

Furthermore, if a is a kth power residue modulo m, then $x^k \equiv a \mod m$ has exactly d incongruent solutions modulo m.

Proof. Let r be a primitive root modulo m. Then $x^k \equiv a \mod m$ if and only if $k \cdot \operatorname{ind}_r x \equiv \operatorname{ind}_r a \mod \phi(m)$.

If we set $y = \operatorname{ind}_r x$ then our congruence is $ky \equiv \operatorname{ind}_r a \mod \phi(m)$, and by our results on linear congruences this has a solution if and only if $d | \operatorname{ind}_r a$, and if $d | \operatorname{ind}_r a$ then there are exactly d incongruent solutions.

But $d | \operatorname{ind}_r a$ if and only if $\phi(m)/d(\operatorname{ind}_r a) \equiv 0 \mod \phi(m)$, which by lemma 6.10 holds if and only if

$$a^{\phi(m)/d} \equiv a^{\phi(m)/d \operatorname{ind}_r a} \equiv 1 \mod \phi(m).$$

And this proves the lemma. □

Corollary 7.6. *If p is a prime and $p \nmid a$, then a is a kth power residue modulo p if and only if $a^{(p-1)/d} \equiv 1 \mod p$.*

Example 7.7. Is 5 a sixth-power residue modulo 17?

We see that $(6, 16) = 2$, so we compute

$$5^{16/2} = 5^8 \equiv 25^4 \equiv 8^4 \equiv 64^2 \equiv (-4)^2 \equiv -1 \mod 17.$$

We see that $2 \nmid -1$ and thus 5 is not a sixth-power residue modulo 17.

We'd like an even more precise statement, but making that in the most general case is quite difficult. So we will now focus on one particular special case.

7.2 Quadratic Residues

For further reading on the material in this subsection, consult **Rosen 11.1, PMF 11.2, Stein 4.1, Shoup 12.1**.

Definition 7.8. If m is a positive integer, we say a is a *quadratic residue of m* if the congruence $x^2 \equiv a \mod m$ has a solution. You will notice that this is just the definition of a 2nd-power residue again.

We can get an initial result purely from counting. We recall a result from homework 5:

Lemma 7.9. *Suppose p is an odd prime and a is a positive integer with $(a,p)=1$. Then the congruence $x^2 \equiv a \mod p$ either has no solution, or has exactly two solutions moduo p.*

Using this we can prove:

Lemma 7.10. *If p is an odd prime, then there are exactly $(p+1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues modulo p in the set $\{0,\dots,p-1\}$.*

Proof. First notice that 0 is always a quadratic residue modulo p. So we need to prove that of the $p-1$ integers relatively prime to p, then $(p-1)/2$ of them are residues and $(p-1)/2$ are not.

But each congruence $x^2 \equiv a \mod p$ has either two solutions or zero solutions, and the total set of solutions has size $p-1$, since every number has exactly one square and thus solves exactly one of these congruences.

So it must be the case that $(p-1)/2$ of these congruences have 2 solutions each, and the other $(p-1)/2$ of them have no solutions, proving our lemma. □

We can also use indices and the results of subsection 7.1 to make statements about quadratic residues.

Lemma 7.11. *Let p be a prime and let r be a primitive root of p. If $p \nmid a$, then a is a quadratic residue of p if and only if $\operatorname{ind}_r a$ is even.*

Proof. Suppose $\operatorname{ind}_r a$ is even. Then

$$(r^{\operatorname{ind}_r a/2})^2 = r^{\operatorname{ind}_r a} \equiv a \mod p$$

and thus a is a square and thus a quadratic residue modulo p.

Now suppose a is a quadratic residue modulo p. Then there is an integer x such that $x^2 \equiv a \mod p$. Taking indices to the base r for some primitive root r, we have

$$\begin{aligned} \operatorname{ind}_r x^2 &\equiv \operatorname{ind}_r a \mod \phi(p) \\ 2\operatorname{ind}_r x &\equiv \operatorname{ind}_r a \mod p-1 \end{aligned}$$

and since $2\operatorname{ind}_r x$ and $p-1$ are both even, so is $\operatorname{ind}_r a$. □

Corollary 7.12. *If r is a primitive root modulo an odd prime p. Then r is a quadratic nonresidue modulo p.*

Proof. We know that $\operatorname{ind}_r r = 1$ is not even. □

7.3 Quadratic residues modulo primes

For further reading on the material in this subsection, consult **Rosen 11.1, PMF 11.2, Stein 4.2, Shoup 12.1**.

Since we'll be discussing this a great deal more, it will be useful to introduce some notation for it. We want to attack this question exactly like we attack all our other number theoretic questions: we solve it for primes, then generalize.

Since we'll be talking about this a lot, we introduce some new notation.

Definition 7.13. Let p be an odd prime, and a an integer. Then we define the *Legendre symbol* by

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ is a nonzero quadratic residue modulo } p \\ -1 & a \text{ is a quadratic nonresidue modulo } p \\ 0 & a \equiv 0 \mod p \end{cases}$$

The symbol is named after Legendre, who repeatedly attempted to prove Euler's conjectured reciprocity law, until it was finally proven by Gauss.

Theorem 7.14 (Euler's Criterion)**.** *Let p be an odd prime and a an integer. Then*

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

Proof. If $(a,p) \neq 1$ then $p|a$, so both sides are equivalent to 0 modulo p. So we can assume $(a,p) = 1$.

Suppose $\left(\frac{a}{p}\right) = 1$. Then there is some x such that $x^2 \equiv a \mod p$. Then we compute that

$$a^{(p-1)/2} = x^{(p-1)} \equiv 1 \mod p$$

by Euler's theorem.

Now suppose $\left(\frac{a}{p}\right) = -1$. Then the congruence $x^2 \equiv a \mod p$ has no solutions. Now consider the numbers $1, \dots, p-1$. We know that for each $1 \leq i \leq p-1$ there is a unique $1 \leq j \leq p-1$ such that $ij \equiv a \mod p$; and since a is a quadratic nonresidue, each pairing is distinct. (That is, we never have $i^2 \equiv a \mod p$).

Thus the product of all the numbers from 1 to $p-1$ is equivalent to $a^{(p-1)/2}$ modulo p. Thus we have

$$a^{(p-1)/2} \equiv (p-1)! \equiv -1 \mod p$$

by Wilson's theorem. □

Example 7.15. Let $p = 23$ and $a = 5$. We can compute that $5^{11} \equiv -1 \mod 23$, so by Euler's criterion we have $\left(\frac{5}{23}\right) = -1$ and thus 5 is a quadratic residue modulo 23.

Proposition 7.16. *Let p be an odd prime and let a, b be integers. then*

1. *If $a \equiv b \mod p$ then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*
2. *$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.*
3. *$\left(\frac{a^2}{p}\right) = 1$ if $p \nmid a$.*

Proof. 1.

2. By Euler's criterion, we have

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p \qquad \left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \mod p$$

$$\begin{aligned}\left(\frac{ab}{p}\right) &\equiv (ab)^{(p-1)/2} \mod p \\ &\equiv a^{(p-1)/2} b^{(p-1)/2} \\ &\equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \mod p.\end{aligned}$$

   Since the two values are equivalent modulo p and both must be ± 1 we conclude they are equal.

3.

□

Remark 7.17. This tells us that the product of two quadratic residues is a quadratic residue, which is obvious. It tells us that the product of a residue and a non-residue is not a residue, which seems reasonable. And it tells us the product of two non-residues is a residue.

We now want to figure out when any number is a quadratic residue modulo a prime. We start, as usual, with studying the primes, but we need to also check one other case.

Lemma 7.18. *If p is an odd prime then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv -1 \mod 4. \end{cases}$$

Proof. By Euler's criterion we know that

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

If $p \equiv 1 \mod 4$ then $(p-1)/2$ is even and thus $(-1)^{(p-1)/2} = 1$. But if $p \equiv 3 \mod 4$ then $(p-1)/2 = 2k+1$ is odd, and thus $(-1)^{(p-1)/2} = -1$. □

In order to sort out the other primes, we need one more major tool. It is awkward to state, so we almost never want to use it directly; but it is quite useful in proofs.

Lemma 7.19 (Gauss's lemma)**.** *Let p be an odd prime and let a be an integer with $(a,p) = 1$. If s is the number of least positive residues of the integers $a, 2a, \dots, a(p-1)/2$ that are greater than $p/2$, then $\left(\frac{a}{p}\right) = (-1)^s$.*

Proof. Consider the list of integers $a, 2a, \dots, a(p-1)/2$. Relabel them so that $u_1, \dots, u_s$ are the elements of the list greater than $p/2$, and $v_1, \dots, v_t$ are the elements less than $p/2$. (No element can be equal to $p/2$ since it is not an integer).

First we claim that the set $\{p-u_1, \dots, p-u_s, v_1, \dots, v_t\}$ is equal to the set $\{1, 2, \dots, (p-1)/2\}$. We just need to show that none of the integers are congruent, since it is a list of $(p-1)/2$ elements between 1 and $(p-1)/2$.

So we can check that $u_i \not\equiv u_j$ and $v_i \not\equiv v_j$ if $i \neq j$, since otherwise we'd have $ma \equiv na \mod p$ and thus $m \equiv n \mod p$ and thus $m = n$.

So suppose $p - u_i \equiv v_j \mod p$. Then $ma \equiv p - na \mod p$, so $ma \equiv -na \mod p$ and $m = -n \mod p$. But this can't happen since m and n are both between 1 and $(p-1)/2$. So we have proven that our set is the set of integers from 1 to $(p-1)/2$.

So now consider the product of the whoel set. We have

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &\equiv (p-u_1)(p-u_2)\dots(p-u_s)v_1v_2\dots v_t \\
&\equiv (-1)^s u_1u_2\dots u_sv_1v_2\dots v_t \\
&\equiv (-1)^s a(2a)(3a)\dots(a(p-1)/2) \\
&\equiv (-1)^s a^{(p-1)/2}\left(\frac{p-1}{2}\right)! \mod p
\end{aligned}$$

and by cancellation, we have

$$\begin{aligned}
1 &\equiv (-1)^s a^{(p-1)/2} \mod p \\
(-1)^s \equiv a^{(p-1)/2} &\equiv \left(\frac{a}{p}\right) \mod p
\end{aligned}$$

by Euler's criterion. □

We can now use Gauss's lemma to figure out what happens in some additional cases.

Lemma 7.20. *If p is an odd prime, then*

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

Remark 7.21. We can rephrase this to say that 2 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 8$.

Proof. By Gauss's lemma 7.19, we just need to determine the number of least positive residues in the set $\{1 \cdot 2, 2 \cdot 2, \dots, 2(p-1)/2\}$ which are greater than $p/2$. But since all of these numbers are between 1 and p, we just need to check the number of set elements that are bigger than $p/2$.

If $1 \leq j \leq (p-1)/2$, then $2j < p/2$ if and only if $j \leq p/4$. Thus the number of integers less than $p/2$ is $\lfloor p/4 \rfloor$, and so we have

$$\left(\frac{2}{p}\right) = (-1)^{(p-1)/2 - \lfloor p/4 \rfloor}.$$

So we just want to show that if p is an odd integer, then

$$\frac{p-1}{2} - \lfloor p/4 \rfloor \equiv \frac{p^2-1}{8} \mod 2.$$

We claim that this formula holds for an odd integer n if and only if it holds for $n+8$. For

$$\begin{aligned}\frac{p+8-1}{2} - \lfloor (p+8)/4 \rfloor &= \frac{p-1}{2} + 4 - \lfloor p/4 + 2 \rfloor = \frac{p-1}{2} - \lfloor p/4 \rfloor + 2 \\ &\equiv \frac{p-1}{2} - \lfloor p/4 \rfloor \mod 2 \\ \frac{(p+8)^2-1}{8} &= \frac{p^2-1}{8} + 2p + 8 \equiv \frac{p^2-1}{8} \mod 2.\end{aligned}$$

Thus by induction we only need to check the formula for $p = \pm 1$ and $p = \pm 3$. Checking these by hand, we see the theorem is proved. □

7.4 The Law of Quadratic Reciprocity

For further reading on the material in this subsection, consult **Rosen 11.2, PMF 11.3-4, Stein 4.1,4.3 Shoup 12.1**.

We've figured out when -1 is a quadratic residue, and when 2 is a quadratic residue. Now we want to look at the other prime numbers.

Unfortunately there is not a good formula for telling whether one odd prime is a quadratic residue modulo another. However, we have a very powerful result which is almost as good, known as the Law of Quadratic Reciprocity. A reciprocity law is a law like this that does *not* give a formula, but does relate two unknown things in a way that often gives us information about them.

Theorem 7.22 (Quadratic Reciprocity)**.** *Let p and q be distinct odd primes. Then*

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

We can use this law, combined with the properties of the Legendre symbol, to compute whther most numbers are quadratic residues.

Example 7.23. Let $p = 13$ and $q = 17$. By quadratic reciprocity, we know that

$$\left(\frac{13}{17}\right)\left(\frac{17}{13}\right) = (-1)^{12/2\cdot 16/2} = 1$$

and thus $\left(\frac{13}{17}\right) = \left(\frac{17}{13}\right)$. But we know that

$$\left(\frac{17}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{2}{13}\right)^2 = 1.$$

Thus we know that $\left(\frac{13}{17}\right) = 1$ and thus 13 is a quadratic residue modulo 17.

Example 7.24. Suppose we want to determine if 7 is a quadratic residue modulo 19. Then quadratic reciprocity tells us that

$$\left(\frac{7}{19}\right)\left(\frac{19}{7}\right) = (-1)^{6/2\cdot 18/2} = (-1)^{27} = -1.$$

Thus

$$\left(\frac{7}{19}\right) = -\left(\frac{19}{7}\right) = -\left(\frac{5}{7}\right).$$

We could check this by hand, but we can also see that

$$\left(\frac{5}{7}\right)\left(\frac{7}{5}\right) = (-1)^{6/2\cdot 4/2} = 1$$

so

$$-\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = -(-1)^{(5^2-1)/8} = -(-1)^3 = 1.$$

Thus 7 is a quadratic residue modulo 19.

If we want to determine whether a composite number is a quadratic residue modulo a prime, we can factor it into primes and use the complete multiplicativity of the Legendre symbol.

Example 7.25. Is 15 a quadratic residue modulo 31?

We compute that $\left(\frac{15}{31}\right) = \left(\frac{5}{31}\right)\left(\frac{3}{31}\right)$. Then quadratic reciprocity tells us that

$$\begin{aligned}\left(\frac{5}{31}\right)\left(\frac{31}{5}\right) &= (-1)^{4/2\cdot 30/2} = 1\\ \left(\frac{5}{31}\right) &= \left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1\\ \left(\frac{3}{31}\right)\left(\frac{31}{3}\right) &= (-1)^{2/2\cdot 30/2} = -1\\ \left(\frac{3}{31}\right) &= -\left(\frac{31}{3}\right) = -\left(\frac{1}{3}\right) = -1.\end{aligned}$$

Thus we see that

$$\left(\frac{15}{31}\right) = 1\cdot(-1) = -1$$

so 15 is not a quadratic residue modulo 31.

Now we should prove the law of quadratic reciprocity, which will take a bit of work.

Lemma 7.26 (Eisenstein)**.** *If p is an odd prime and a is an odd integer with $p \nmid a$, then*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$$

where

$$T(a,p) = \sum_{j=1}^{(p-1)/2} \lfloor ja/p \rfloor .$$

Proof. We reduce this to Gauss's lemma 7.19. As before, consider the set $a, 2a, \ldots, a(p-1)/2$, and let $u_1, \ldots, u_s$ be the elements whose least positive residues are greater than $p/2$, and $v_1, \ldots, v_t$ be those whose least positive residues are less than $p/2$. We know by Gauss's lemma that

$$\left(\frac{a}{p}\right) = (-1)^s$$

so we just need to prove that $s \equiv T(a,p) \mod 2$.

For each ja, we can use the division algorithm to divide by $\lfloor ja/p \rfloor$ to get

$$ja = p\lfloor ja + p \rfloor + r_j$$

where the remainder is one of the u_i or v_i (since it is the least positive residue of ja). If we add these equations together for each $1 \leq j \leq (p-1)/2$, we get

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\lfloor ja/p \rfloor + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j.$$

But as before we have that the integers from 1 to $(p-1)/2$ are the integers $p-u_i, v_j$ in some order, so

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_t = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j.$$

Subtracting the second equation from the first gives

$$\begin{aligned}
\sum_{j=1}^{(p-1)/2} j(a-1) &= \sum_{j=1}^{(p-1)/2} p\lfloor ja/p \rfloor - ps + 2\sum_{j=1}^{s} u_j \\
&= T(a,p) - ps + 2\sum_{j=1}^{s} u_j \\
(a-1)\sum_{j=1}^{(p-1)/2} j &= T(a,p) - ps + 2\sum_{j=1}^{s} u_j \\
0 &\equiv T(a,p) - s \mod 2.
\end{aligned}$$

□

Proof of Quadratic Reciprocity. Let p and q be odd primes. Let S be the set of pairs of integers $\{(x,y) : 1 \leq x \leq (p-1)/2, 1 \leq y \leq (q-1)/2\}$. Notice that S has $(p-1)(q-1)/4$ elements, and that we can draw it as the "lattice points" or integer-valued points in a $(p-1)/2 \times (q-1)/2$ rectangle in the real plane.

We draw a diagonal line $x = (p/q)y$ or $qx = py$ *almost* through the corners of this rectangle, and we count the points above and below it. We first note that no point is on this line, since if $qx = py$ then $q|py$ and thus either $q|p$ (which is not true since both are prime), or $q|y$, which is not true since $1 \leq y \leq (q-1)/2$. So every point is above or below the line.

A point $(x,y) \in S$ is below the line if and only if $py < qx$, if and only if $1 \leq y \leq qx/p$. For a fixed x, the number of points we get this way is $\lfloor qx/p \rfloor$, thus the total number of points below the line is $\sum_{x=1}^{(p-1)/2} \lfloor qj/p \rfloor$. Notice this is exactly $T(q,p)$ from lemma 7.26.

Similarly, the number of points *above* the line is $\sum_{y=1}^{(p-1)/2} \lfloor pj/q \rfloor = T(p,q)$. In particular, the sum of these sums is $(p-1)(q-1)/4$ because every point is counted exactly once, and

thus we have

$$T(q,p) + T(p,q) = \frac{p-1}{2} \cdot \frac{q-1}{2}$$
$$(-1)^{T(q,p)}(-1)^{T(p,q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

But from lemma 7.26 we know that $(-1)^{T(q,p)} = \left(\frac{q}{p}\right)$ and $(-1)^{T(p,q)} = \left(\frac{p}{q}\right)$, which completes our proof. □

7.5 Bonus Material: the Jacobi Symbol

For further reading on the material in this subsection, consult **Rosen 11.3, PMF 11.6, Stein 4.3, Shoup 12.2-3**.

So far we've only dealt with determining quadratic residues modulo a prime. We'd like to be able to answer this question about composites as well.

Definition 7.27. Let $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ be an odd positive integer. We define the *Jacobi symbol* by

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{t_1} \dots \left(\frac{a}{p_k}\right)^{t_k}.$$

If $(a,n) = 1$ then $\left(\frac{a}{n}\right) = \pm 1$. If $(a,n) \neq 1$ then $\left(\frac{a}{n}\right) = 0$. When n is prime then this is just the Legendre symbol.

We can see that if $\left(\frac{a}{n}\right) \neq 1$ then a is not a quadratic residue modulo n. For if a is a residue modulo n it must be a residue modulo p_i for each i, since its square root modulo n will also be a square root modulo p_i.

Unfortunately, the converse is not true; if $\left(\frac{a}{n}\right) = 1$ that does not imply that a is a quadratic residue modulo n. For instance, if $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$ then $\left(\frac{a}{pq}\right) = 1$ but a is not a quadratic residue modulo pq.

We can carry over or reprove many results from our section on primes.

Proposition 7.28 (Facts about the Jacobi Symbol)**.** *Let n be an odd positive integer, and a, b integers. Then*

1. *If $a \equiv b \mod n$ then $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
3. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
4. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

Theorem 7.29 (Quadratic Reciprocity for the Jacobi Symbol)**.** *If n and m are relatively prime odd integers greater than 1, then*

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

Our Jacobi symbol computations do make it easier for us to compute Legendre symbols, however. The one difficulty we had using quadratic reciprocity earlier was that to compute $\left(\frac{a}{p}\right)$ when a was composite, we had to factor it into primes–which is in general difficult. But now we can use the same algorithm without ever having to factor.

Example 7.30. Let us determine whether 93 is a quadratic residue modulo 179. Since 179 is prime, we just need to compute $\left(\frac{93}{179}\right)$. By quadratic reciprocity we have

$$\begin{aligned}
\left(\frac{93}{179}\right)\left(\frac{179}{93}\right) &= (-1)^{92/2\cdot 178/2} = 1\\
\left(\frac{93}{179}\right) = \left(\frac{179}{93}\right) &= \left(\frac{-7}{93}\right) = \left(\frac{7}{93}\right)\left(\frac{-1}{93}\right)\\
\left(\frac{-1}{93}\right) &= (-1)^{(93-1)/2} = (-1)^{46} = 1\\
\left(\frac{7}{93}\right)\left(\frac{93}{7}\right) &= (-1)^{6/2\cdot 92/2} = 1\\
\left(\frac{7}{93}\right) = \left(\frac{93}{7}\right) &= \left(\frac{2}{7}\right) = (-1)^{(7^2-1)/8} = (-1)^6 = 1
\end{aligned}$$

and thus $\left(\frac{93}{179}\right) = 1 \cdot 1 = 1$.