7 Quadratic Residues

Recall our earlier discussion of k^{th} roots:

> If $\gcd(a,m) = 1 = \gcd\big(k, \varphi(m)\big)$, then $x^k \equiv a \pmod{m}$ has a unique solution.

This result contains an almost glaring omission: (when $m \geq 3$) $\varphi(m)$ is *always even*, so the simplest type of root, *square roots*, never fit the pattern! In this chapter we focus on the equation $x^2 \equiv a \pmod{p}$ where p is an odd prime, and consider the question of when a has a square root modulo p.

7.1 Squares Modulo an Odd Prime

Definition 7.1. Let p be an odd prime. A non-zero residue a is a *quadratic residue* (QR) modulo p if $x^2 \equiv a \pmod{p}$ has a solution. Otherwise it is a quadratic non-residue (QNR, or just NR).

Examples 7.2. Here are all possible equations modulo $p = 3, 5$ and 7, and whether each a is a quadratic residue modulo p.

a	equation	solutions	QR?
1	$x^2 \equiv 1 \pmod 3$	$x \equiv 1, 2$	✓
2	$x^2 \equiv 2 \pmod 3$	none	X

a	equation	solutions	QR?
1	$x^2 \equiv 1 \pmod 5$	$x \equiv 1, 4$	✓
2	$x^2 \equiv 2 \pmod 5$	none	X
3	$x^2 \equiv 3 \pmod 5$	none	X
4	$x^2 \equiv 4 \pmod 5$	$x \equiv 2, 3$	✓

a	equation	solutions	QR?
1	$x^2 \equiv 1 \pmod 7$	$x \equiv 1, 6$	✓
2	$x^2 \equiv 2 \pmod 7$	$x \equiv 3, 4$	✓
3	$x^2 \equiv 3 \pmod 7$	none	X
4	$x^2 \equiv 4 \pmod 7$	$x \equiv 2, 5$	✓
5	$x^2 \equiv 5 \pmod 7$	none	X
6	$x^2 \equiv 6 \pmod 7$	none	X

The first thing you should observe is that precisely half $\frac{p-1}{2}$ of the non-zero remainders are quadratic residues. This follows immediately from a simple calculation.

Lemma 7.3. *If p is an odd prime, then the numbers $0^2, 1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are distinct modulo p.*

Proof. $x^2 \equiv y^2 \implies (x-y)(x+y) \equiv 0 \pmod{p}$. By unique factorization, we have $x \equiv \pm y$. ∎

Partly in view of the Lemma, it is often useful when discussing quadratic residues to consider remainders as lying in the set of *least residues* $\{0, \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}\}$: i.e. with minimal absolute value.

Note also that the Lemma really requires a prime modulus (from which unique factorization follows). For composite moduli we don't expect distinct values from square: for instance

$$1^2 \equiv 3^2 \pmod 8$$

Indeed, modulo 8, the only equations $x^2 \equiv a$ with solutions are when $a \equiv 0, 1, 4$. Even for non-zero remainders, only two in seven have square roots modulo 8.

A second property that might take a little longer to spot is the *multiplicativity* of quadratic residues: for example 2 and 4 are quadratic residues modulo 7, as is $2 \cdot 4 \equiv 1$. With a proof of this in mind, we make a useful definition.

Definition 7.4. Given an odd prime p and an integer a, define the *Legendre symbol*

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } a \text{ is a QR modulo } p \\ -1 & \text{if } a \text{ is a QNR modulo } p \end{cases}$$

Examples 7.5. Look at the above tables: $\left(\frac{1}{3}\right) = \left(\frac{-1}{5}\right) = \left(\frac{2}{7}\right) = 1$ and $\left(\frac{-2}{3}\right) = \left(\frac{-2}{5}\right) = \left(\frac{3}{7}\right) = -1$

Legendre symbols will prove very useful for checking whether we have a quadratic residue. To see how, we develop a little algebra.

Theorem 7.6. *If p is an odd prime and $a, b \in \mathbb{Z}$, then:*

1. $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $p \nmid a \implies \left(\frac{a^2}{p}\right) = 1$
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$: *otherwise said QR×QR=QR, QR×NR=NR, NR×NR=QR.*

This follows as a corollary of a more complex result later, but for now it is worth a direct proof.

Proof. Parts 1 and 2 are immediate from the definition. In particular, note that

$$a \text{ is a QR} \iff \exists c \in \mathbb{Z}_p^\times \text{ such that } a \equiv c^2 \pmod{p}$$

For part 3, the statement is trivial if either or both $p \mid a$ or $p \mid b$. Otherwise, we treat the three cases separately: suppose throughout that c, d are units (non-zero modulo p).

(a) $c^2 d^2 \equiv (cd)^2$, so the product of QR's is a QR.

(b) By part (a), $c^2 n \equiv d^2 \implies n \equiv (dc^{-1})^2$ is a QR. The contrapositive says that if n is a NR, so also is $c^2 n$.

(c) Let n be a NR. Since $n \not\equiv 0$, we have a bijective map[a]

$$\mu : x \mapsto nx : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times \qquad \text{(the inverse is } \mu^{-1}(x) := n^{-1}x\text{)}$$

For any QR c^2, part (b) says that $\mu(c^2) = nc^2$ is an NR. Since (Lemma 7.3) the sets of QR's and NR's have equal cardinality, it follows that μ maps the QR's bijectively to the NR's and must therefore map NR's back to QR's. In particular, if m is a NR, then $\mu(m) = mn$ is a QR. ∎

[a] If you've done group theory, this argument should remind you of the comparison of even and odd cycles in the symmetric group S_n, where we see that the sets of such have the same cardinality. Indeed we are really proving that the function $f(a) = \left(\frac{a}{p}\right)$ is a homomorphism of multiplicative groups $f : \mathbb{Z}_p^\times \to \{\pm 1\}$.

Example 7.7. To check whether 27 is a QR modulo 61, we compute the Legendre symbol.

$$\left(\frac{27}{61}\right) = \left(\frac{3^2}{61}\right)\left(\frac{3}{61}\right) = \left(\frac{3}{61}\right)$$

We are left to decide whether 3 is a QR modulo 61; equivalently, we want to solve $x^2 \equiv 3 \pmod{61}$. By inspection, $x \equiv 8$ is a solution (as is $x \equiv -8 \equiv 53$), whence 27 is a QR modulo 61.
We can actually go further:

$$8^2 \equiv 3 \implies (3 \cdot 8)^2 \equiv 3^3 \implies 24^2 \equiv 27 \pmod{61}$$

It follows that the solutions to the original congruence are

$$x^2 \equiv 27 \pmod{61} \iff x \equiv \pm 24 \equiv 24,\ 37 \pmod{61}$$

While Legendre symbols were undoubtedly helpful for our example, they weren't quite enough. We still needed to be able to spot that 3 was a quadratic residue, though thankfully this was easy in the example. In general we can't rely on being able to spot a solution; we therefore need some method of computing a Legendre symbol directly.

Example 7.8. Suppose we want to find the value of $\left(\frac{2}{101}\right)$: equivalently we are asking whether $x^2 \equiv 2 \pmod{101}$ has a solution. Simply trying all possible values of x is a bad idea! Instead, suppose that there was a solution x: plainly it would have to be a unit modulo 101 and so we could apply Fermat's little theorem:

$$x^2 \equiv 2 \implies 1 \overset{\text{F}\ell\text{T}}{\equiv} x^{100} \equiv 2^{50} \pmod{101}$$

A short calculation (successive squaring?) should convince you that $2^{50} \equiv -1$, whence 2 is a non-residue and $\left(\frac{2}{101}\right) = -1$.

The approach works in general:

Theorem 7.9 (Euler's Criterion). *If p is an odd prime, then $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.*

Proof. If $p \mid a$, both sides are trivially zero.
If a is a QR, then $a \equiv b^2$ for some $b \in \mathbb{Z}_p^\times$, whence $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem.
Now consider the equation $y^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. By Lagrange, this has *at most* $\frac{p-1}{2}$ solutions. However, all $\frac{p-1}{2}$ quadratic residues (Lemma 7.3) are already solutions! Hence

$$a \text{ is a quadratic residue} \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

Finally observe that Fermat's little theorem may be factorized (*uniquely* modulo p):

$$0 \equiv a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \pmod{p}$$

We conclude that a is a non-residue $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ∎

Examples 7.10. 1. 3 is a QR modulo 13 since $3^{\frac{13-1}{2}} \equiv 3^6 \equiv 27^2 \equiv 1^2 \equiv 1 \mod 13$. It is easy to see that the solutions to $x^2 \equiv 3 \mod 13$ are $x \equiv 4, 9$.

2. Returning to Example 7.7 and applying successive squaring,

$$\left(\frac{3}{61}\right) \equiv 3^{\frac{61-1}{2}} \equiv 3^{30} \equiv 3^{2+4+8+16} \equiv 9 \cdot 20 \cdot (-27) \cdot (-3) \equiv 1 \pmod{61}$$

Is -1 a Quadratic Residue? Here is a straightforward application of Euler's criterion where we see for precisely which primes -1 is a quadratic residue.

Theorem 7.11. *If p is an odd prime, then -1 is a QR $\iff$ $p \equiv 1 \pmod 4$. Indeed*

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

As a surprising by-product, we obtain a proof of a result promised earlier in the course.

Theorem 7.12. *There are infinitely many primes congruent to 1 modulo 4.*

The idea is to construct an impossible solution to some $x^2 \equiv -1 \pmod q$ where $q \equiv 3 \pmod 4$.

Proof. Suppose that $p_1, \ldots, p_n$ constitute all primes congruent to 1 modulo 4. Define

$$x := 2p_1 \cdots p_n \text{ and } \Pi := x^2 + 1$$

Certainly Π is divisible by some prime q, which is plainly odd and cannot be one of the primes $p_1, \ldots, p_n$. We conclude that $q \equiv 3 \pmod 4$. However, we now have

$$\Pi \equiv 0 \implies x^2 \equiv -1 \pmod q$$

which contradicts Theorem 7.11. ∎

Is 2 a Quadratic Residue? This is harder than dealing with -1, though a nice answer is still available, based on a sneaky trick attributable to Gauss.[1]

Examples 7.13. 1. We multiply the even remainders modulo 23 in two ways:

$$2 \cdot 4 \cdot 6 \cdots 22 \equiv 2^{11} \cdot 11! \pmod{23}$$

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots 22 &\equiv 2 \cdot 4 \cdots 10 \cdot 12 \cdot 14 \cdots 22 \\ &\equiv 2 \cdot 4 \cdots 10 \cdot (-11) \cdot (-9) \cdots (-1) \\ &\equiv (-1)^6 \cdot 11! \pmod{23} \end{aligned}$$

It follows that $2^{11} \equiv 2^{\frac{23-1}{2}} \equiv (-1)^6 \equiv 1 \pmod{23}$, whence 2 is a quadratic residue modulo 23.

[1] Carl Friedrich Gauss (1777–1855) was arguably the most consequential mathematician in history, and a major contributor to number theory, which he considered the *Queen of Mathematics*.

2. Let $p = 37$. This time $\frac{p-1}{2} = 18$ so we we break the even remainders at 18:

$$\begin{aligned} 2^{18} \cdot 18! &\equiv 2 \cdot 4 \cdot 6 \cdots 36 \\ &\equiv 2 \cdot 4 \cdots 18 \cdot 20 \cdot 22 \cdots 36 \\ &\equiv 2 \cdot 4 \cdots 18 \cdot (-17) \cdot (-15) \cdots (-1) \\ &\equiv (-1)^9 \cdot 18! \pmod{37} \\ \implies 2^{\frac{37-1}{2}} &\equiv 2^{18} \equiv (-1)^9 \equiv -1 \pmod{37} \end{aligned}$$

We conclude that 2 is a non-residue modulo 37.

For the main result, we need only do this in the abstract!

Theorem 7.14. *If p is an odd prime, then 2 is a QR $\iff$ $p \equiv 1, 7 \pmod 8$. Otherwise said,*

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

Proof. Since p is odd, we may define the integer $P = \frac{p-1}{2}$. Multiply together the even remainders modulo p to obtain

$$2 \cdot 4 \cdot 6 \cdots (p-1) = 2^P \cdot 1 \cdot 2 \cdots P = 2^P P! \tag{$*$}$$

Now consider the same product, split at P:

$$\underbrace{2 \cdot 4 \cdot 6 \cdots}_{\leq P} \underbrace{\cdots (p-5)(p-3)(p-1)}_{> P} \equiv 2 \cdot 4 \cdot 6 \cdot \cdots \cdot (-5) \cdot (-3) \cdot (-1)$$

To finish the proof, we need to make sure that the right side has the form $(-1)^m \cdot P!$ and we need to *count the number of negative signs m*. There are two cases.

$P = 2k$ is even: Plainly $p = 2P + 1 = 4k + 1 \equiv 1 \pmod 4$. There are $P = 2k$ even remainders modulo p, whence the split is as follows:

$$\begin{aligned} 2 \cdot 4 \cdot 6 \cdots (p-1) &\equiv \underbrace{2 \cdot 4 \cdot 6 \cdots P}_{k \text{ terms} \leq P} \cdot \underbrace{(P+2) \cdots (p-5)(p-3)(p-1)}_{k \text{ terms} > P} \\ &\equiv 2 \cdot 4 \cdots P \cdot \big(-(P-1)\big) \cdots (-3) \cdot (-1) \\ &\equiv (-1)^k \cdot P! \pmod p \end{aligned}$$

where we used the fact that $(P+2) - p = P + 2 - 2P - 1 = -(P-1)$. Combined with $(*)$, we see that

$$2^{\frac{p-1}{2}} \equiv 2^P \equiv (-1)^k \equiv \begin{cases} 1 & \text{if } k \text{ is even} \iff p \equiv 1 \pmod 8 \\ -1 & \text{if } k \text{ is odd} \iff p \equiv 5 \pmod 8 \end{cases}$$

$P = 2k + 1$ is odd: This is similar and we leave it as an exercise. ∎

Example 7.15. To check whether $x^2 \equiv 95 \pmod{127}$ has any solutions, observe that

$$\left(\frac{95}{127}\right) = \left(\frac{-32}{127}\right) = \left(\frac{-1}{127}\right)\left(\frac{4^2}{127}\right)\left(\frac{2}{127}\right) = \left(\frac{-1}{127}\right)\left(\frac{2}{127}\right) = (-1)\cdot 1 = -1$$

where we used that fact that

$$127 = 15\cdot 8 + 7 \implies \begin{cases} 127 \equiv 3 \pmod 4 \\ 127 \equiv 7 \pmod 8 \end{cases}$$

We conclude that 95 is a non-residue modulo 127.

Similar results can be obtained for other values though, as we'll see, such aren't really necessary...

Exercises 7.1

1. Use the methods of this section to decide which are quadratic residues:
   (a) $7 \pmod{11}$ (b) $6 \pmod{31}$ (c) $39 \pmod{41}$
2. (a) Suppose that a is a quadratic residue modulo p, where $p \equiv 3 \pmod 4$. Check that the solutions of $x^2 \equiv a \pmod p$ are $x = \pm a^{\frac{p+1}{4}} \pmod p$.
   (b) Find all solutions to the congruence $x^2 \equiv 7 \pmod{31}$.
   (c) Still working with $p \equiv 3 \pmod 4$, if $p \nmid a$ and a is a quadratic non-residue modulo p, what is the value of $\left(a^{\frac{p+1}{4}}\right)^2$?
3. (a) Find the prime decomposition of 924.
   (b) Check that 37 is a quadratic residue modulo each odd prime dividing 924. Also check that $x^2 \equiv 37 \pmod{2^k}$ is solvable where 2^k is the largest power of 2 dividing 924.
   (c) How many solutions has the congruence $x^2 \equiv 37 \pmod{924}$? Why?
4. In the manner of question 3, decide whether the following have solutions and, if so, how many.
   (a) $x^2 \equiv 3 \pmod{143}$
   (b) $x^2 \equiv 2 \pmod{437}$
   (c) $x^2 \equiv 393 \pmod{1564}$
5. Suppose $p \nmid a$. Show that if $p \equiv 1 \pmod 4$, then both or neither of $\pm a$ are quadratic residues modulo p. Similarly, if $p \equiv 3 \pmod 4$, show that exactly one of $\pm a$ are quadratic residues.
6. Compute $2^{2048} \pmod{4097}$. What does this tell you about whether 4097 is prime?
   (*Hint: 4096 is a power of 2...*)
7. Complete the proof of Theorem 7.14 where p is an odd prime and $P = \frac{p-1}{2} = 2k+1$ is odd.
8. Show that if $p \nmid m$, then $\sum_{a=1}^{p-1} \left(\frac{ma}{p}\right) = 0$.
   (*Hint: show first that* $\sum \left(\frac{a}{p}\right) = 0$, *then recall that multiplication by m permutes residue classes...*)
9. Let a be given and suppose that n is a value assumed by the polynomial $f(x,y) = x^2 - ay^2$ where $x, y \in \mathbb{Z}$. Prove that, for every odd prime divisor p of n, either $p \mid x$ or $\left(\frac{a}{p}\right) = 1$.

7.2 Quadratic Reciprocity

For a result which is essentially unknown outside mathematics, the law of quadratic reciprocity has a surprising number of distinct proofs: around 200 are claimed, arguably more than any other result. Gauss himself gave at least *six* in his lifetime, the first when he was only 18, and the law is said to have been his favorite theorem. So why did he like it so much? Have a read and judge for yourself...

Theorem 7.16 (Quadratic Reciprocity). *If $p \neq q$ are prime, then*

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

Otherwise said, $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \iff$ both $p, q \equiv 3 \pmod 4$.

Reciprocity encompasses the idea that if q says something about p, then p says something about q:

> If we know whether (or not) $x^2 \equiv p \pmod q$ has a solution, then we know whether (or not) $x^2 \equiv q \pmod p$ has a solution.

That these equations should have anything to do with each other is surprising to say the least! We'll give a proof of the law later, but for now we start by seeing its utility.

Examples 7.17. 1. Suppose we are asked to decide whether -1500 is a QR modulo 997. We start to compute, using all our knowledge from the previous section:

$$\begin{aligned}
\left(\frac{-1500}{977}\right) &= \left(\frac{-1}{997}\right)\left(\frac{3}{997}\right)\left(\frac{2^2}{997}\right)\left(\frac{5^3}{997}\right) && \text{(Theorem 7.6, part 3)} \\
&= \left(\frac{-1}{997}\right)\left(\frac{3}{997}\right)\left(\frac{5}{997}\right) && \text{(Theorem 7.6, part 2)} \\
&= \left(\frac{3}{997}\right)\left(\frac{5}{997}\right) && \text{(Theorem 7.11, since } 997 \equiv 1 \pmod 4)
\end{aligned}$$

Without reciprocity, we'd be stuck with Euler's criterion (Theorem 7.9) and the nasty evaluation of $3^{498}5^{498} \pmod{997}$. Instead we simply flip the Legendre symbols and continue!

$$\begin{aligned}
\left(\frac{-1500}{977}\right) &= \left(\frac{997}{3}\right)\left(\frac{997}{5}\right) && \text{(reciprocity, since } 997 \equiv 1 \pmod 4) \\
&= \left(\frac{1}{3}\right)\left(\frac{2}{5}\right) = -1 && \text{(Theorem 7.14)}
\end{aligned}$$

We conclude that -1500 is a quadratic non-residue modulo 997.

2. We use reciprocity three times: note that $997 \equiv 1$ and $43, 563 \equiv 3 \pmod 4$:

$$\begin{aligned}
\left(\frac{563}{997}\right) = \left(\frac{997}{563}\right) = \left(\frac{-129}{563}\right) &= \left(\frac{-1}{563}\right)\left(\frac{3}{563}\right)\left(\frac{43}{563}\right) && \text{(factorize: Theorem 7.6)} \\
&= (-1)(-1)\left(\frac{563}{3}\right)(-1)\left(\frac{563}{43}\right) = -\left(\frac{2}{3}\right)\left(\frac{4}{43}\right) = 1 && \text{(Theorem 7.14)}
\end{aligned}$$

Note that this calculation doesn't help us solve the congruence $x^2 \equiv 563 \pmod{997}$: it only tells us that solutions[a] exist!

[a] In fact $x \equiv \pm 470 \equiv 470,\ 527 \pmod{997}$

Jacobi Symbols

Legendre symbols have a huge weakness: the reciprocity formula only applies when you have two primes. For large numbers you might need to do a lot of factorizing or perform several computations of the form $a^{\frac{p-1}{2}}$. With a small extension of the definition, however, this problem can be overcome and the computation of Legendre symbols becomes purely algorithmic.

Definition 7.18. Let a be an integer and n an odd positive integer. If $n = p_1^{\lambda_1} \cdots p_k^{\lambda_k}$ is the prime decomposition, then we define the *Jacobi Symbol* $\left(\frac{a}{n}\right)$ in terms of the Legendre symbols $\left(\frac{a}{p_i}\right)$

$$\left(\frac{a}{n}\right) := \left(\frac{a}{p_1}\right)^{\lambda_1} \cdots \left(\frac{a}{p_k}\right)^{\lambda_k}$$

If n is an odd prime, then $\left(\frac{a}{n}\right)$ is plainly a Legendre symbol. Moreover, the basic properties of Legendre symbols *and* the reciprocity results (Theorems 7.6, 7.11, 7.14 & 7.16) translate over almost immediately:

Theorem 7.19. *If $a, b \in \mathbb{Z}$ and m, n are odd positive integers, then;*

1. $a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\gcd(a, n) = 1 \implies \left(\frac{a^2}{n}\right) = 1$
3. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
4. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
5. $\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4} \\ -1 & \text{if } n \equiv 3 \pmod{4} \end{cases}$
6. $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1, 7 \pmod{8} \\ -1 & \text{if } n \equiv 3, 5 \pmod{8} \end{cases}$
7. *If* $\gcd(m, n) = 1$, *then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} = \begin{cases} 1 & \iff m \text{ or } n \equiv 1 \pmod{4} \\ -1 & \iff m \text{ and } n \equiv 3 \pmod{4} \end{cases}$$

The only real disadvantage of working modulo a composite n is that a Jacobi symbol being 1 doesn't correspond to the existence of solutions to a quadratic congruence.

Example 7.20. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, however $x^2 \equiv 2 \pmod{15}$ has no solution!

We won't pursue this further, instead using Jacobi symbols mainly to assist with the computation of Legendre symbols.

Proof. Arguments are barely required for parts 1–4: these follow from the corresponding propertied of Legendre symbols and the Definition. Parts 5 and 6 are exercises.

We content ourselves with a proof of the main reciprocity law (part 7).
Let $m = p_1 \cdots p_k$ and $n = q_1 \cdots q_l$ be the prime decompositions, where there are no primes in common between the lists and repeats are permitted. Then, by decomposing (parts 3, 4) and applying the quadratic reciprocity law,

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \left(\frac{p_1 \cdots p_k}{n}\right)\left(\frac{n}{p_1 \cdots p_k}\right) = \prod_{i=1}^{k}\left(\frac{p_i}{n}\right)\left(\frac{n}{p_i}\right) = \prod_{i=1}^{k}\left(\frac{p_i}{q_1 \cdots q_l}\right)\left(\frac{q_1 \cdots q_l}{p_i}\right) \\ &= \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}\end{aligned}$$

Since the only way a negative can appear is if *both* $p_i \equiv q_j \equiv 3 \pmod 4$, we count the number of such primes in each of m and n. Suppose there are s and t such primes in m and n respectively, then

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{st} = \begin{cases} 1 & \iff s \text{ or } t \text{ even} \iff m \text{ or } n \equiv 1 \pmod 4 \\ -1 & \iff s \text{ and } t \text{ odd} \iff m \text{ and } n \equiv 3 \pmod 4 \end{cases}$$

■

If you're unsure why the final implications hold, revisit the discussion of primes modulo 4 from earlier in the course.

The usefulness of Jacobi symbols is that we can apply the rules *without checking primality!* By combining the rules, we can easily compute the value of any Legendre (or Jacobi) symbol, where the only required factorizations are to divide out negatives and 2's.

Example 7.21. We know that 317 is prime, and we want to check whether 246 is a quadratic residue. We compute, indicating which part of the theorem we're using each time.

$$\begin{aligned}\left(\frac{246}{317}\right) &= \left(\frac{2}{317}\right)\left(\frac{123}{317}\right) = -\left(\frac{123}{317}\right) && \text{(parts 3, 6: since } 317 \equiv 5 \pmod 8\text{)} \\ &= -\left(\frac{317}{123}\right) && \text{(part 7: since } 317 \equiv 1 \pmod 4\text{)} \\ &= -\left(\frac{71}{123}\right) = \left(\frac{123}{71}\right) && \text{(parts 1, 7: since } 71, 123 \equiv 3 \pmod 4\text{)} \\ &= \left(\frac{31}{71}\right) = -\left(\frac{71}{31}\right) && \text{(parts 1, 7: since } 31, 71 \equiv 3 \pmod 4\text{)} \\ &= -\left(\frac{9}{31}\right) = -1 && \text{(parts 1 and 2)}\end{aligned}$$

Therefore 246 is a quadratic non-residue modulo 317.

It is easy to see how to state this algorithmically: to find $\left(\frac{a}{n}\right)$:

1. Reduce a modulo n, factor out any copies of $\left(\frac{-1}{n}\right)$, $\left(\frac{2}{n}\right)$ or $\left(\frac{b^2}{n}\right)$ and evaluate.
2. Apply the main reciprocity formula to each remaining factor.
3. Repeat steps 1 & 2 until all terms in step 1 are evaluated.

Primality Testing

Recall Euler's criterion: if n is an odd prime and $n \nmid a$, then $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$. If we are not sure whether n is prime, we could compute both sides of this for some a...

Definition 7.22 (Solovay–Strassen Primality Test). Let n be an odd positive integer. A *witness* to the compositeness of n is any unit $a \in \mathbb{Z}_n^\times$ for which

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n}$$

If n is composite, any unit a for which $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}$ is termed a *liar*, and n a *pseudoprime to base* a.

One witness is all you need to prove that n is composite! Even if n is very large, both sides of the congruence can be found rapidly with a computer. Moreover, if n is composite, *at least half* of the units modulo n can be shown to be witnesses, so you shouldn't have to try for long.

As a test for *primality*, Solovay–Strassen is only *probabilistic*. If you try four values of a and find no witnesses, then you have roughly a $\frac{1}{2^4} = \frac{1}{16}$ chance that n is composite; ten trials without a witness and the probability drops to roughly $\frac{1}{1024}$. Of course this is no good for *proving* that a large number is prime: you would have to try *half* the remainders without finding a witness before this could be your certain conclusion!

Examples 7.23. 1. We test to see if $n = 3599$ is composite by choosing $a = 2$. Use successive squaring to compute

$$2^{\frac{n-1}{2}} \equiv 2^{1799} \equiv 946 \pmod{3599}$$

Plainly this isn't ± 1 and so cannot be the value of a Lagrange/Jacobi symbol: $a = 2$ is therefore a witness and n is composite. For completion, since $8 \mid 200$ we can quickly verify that

$$n \equiv -1 \equiv 7 \pmod{8} \implies \left(\frac{2}{3599}\right) = 1$$

In fact $n = 59 \times 61$, but we did not need this information.

2. Given the 1000-digit number $n = 10^{999} + 7$, we have a computer verify that, modulo n,

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \text{ for each } a \in \{2, 3, 5, 7, 11\}$$

We conclude that n is likely prime with a probability of at least $1 - \frac{1}{2^5} = \frac{2047}{2048} = 99.95\%$ (this took the computer only 200 μs!). In fact n is prime; the smallest 1000-digit prime.

There are many other primality tests of varying degrees of complexity and predictive power. Computer packages are likely to rely on the Miller–Rabin test and its extension, the Baillie-PSW test. While neither test can prove conclusively that a given candidate is prime, no counter-examples (*pseudoprimes*) are known for the latter.

Gauss' Lemma and the Proof of Quadratic Reciprocity

With a view to proving the quadratic reciprocity law, we revisit the idea of least residues (page 1).

Definition 7.24. Let p be an odd prime and define $P = \frac{p-1}{2}$. Given $a \in \mathbb{Z}$, its *least residue modulo* p is the unique value r such that

$$a \equiv r \pmod{p} \text{ and } -P \leq r \leq P$$

If $r < 0$ we say that a has *negative least residue.* Now define a counting function; if $p \nmid a$ let,

$$\mu(a,p) = \left|\{x \in \{a, 2a, 3a, \ldots, Pa\} : x \text{ has negative least residue modulo } p\}\right|$$

Example 7.25. To find $\mu(8,13)$, start with $P = \frac{13-1}{2} = 6$ and compute

$$\{8k : 1 \leq k \leq \tfrac{13-1}{2}\} = \{8, 16, 24, 32, 40, 48\} \equiv \{-5, 3, -2, 6, 1, -4\} \implies \mu(8,13) = 3$$

One purpose of the function μ is to provide a general way of computing Legendre symbols.

Theorem 7.26 (Gauss' Lemma). $\left(\frac{a}{p}\right) = (-1)^{\mu(a,p)}$

Examples 7.27. 1. Continuing the previous example, we verify that

$$\left(\frac{8}{13}\right) = \left(\frac{2^2}{13}\right)\left(\frac{2}{13}\right) = -1 = (-1)^{\mu(8,13)}$$

2. To compute $\mu(17,11)$, note that $17 \equiv -5 \pmod{11}$ and build the set

$$\{17, \ldots, 5 \cdot 17\} \equiv \{-5, 1, -4, 2, -3\} \pmod{11} \implies \mu(17,11) = 3$$

Similarly, $11 \equiv -6 \pmod{17}$, whence

$$\{11, \ldots, 8 \cdot 11\} \equiv \{-6, 5, -1, -7, 4, -2, -8, 3\} \pmod{17} \implies \mu(11,17) = 5$$

By Gauss' Lemma, neither $x^2 \equiv 17 \pmod{11}$ nor $x^2 \equiv 17 \pmod{11}$ have solutions.

The proof is little more than a generalization of part of Theorem 7.14.

Proof. Since a is invertible modulo p, the (least) residues $a, 2a, 3a, \ldots, Pa$ are distinct. Moreover, for any $x, y \in \{1, \ldots, P\}$, if the least residues of ax, ay were negative each other,

$$ax \equiv -ay \implies x \equiv -y \pmod{p}$$

is a contradiction. We conclude that, modulo p, we have $\{a, 2a, 3a, \ldots, Pa\} = \{(\pm 1), (\pm 2), \ldots, (\pm P)\}$ where precisely one of each $\pm$ remainder appears. Plainly $\mu(a,p)$ is the number of negative signs appearing in the second representation. To finish, simply multiply together the remainders, cancel $P!$, and recall Euler's criterion (Theorem 7.9):

$$a^{\frac{p-1}{2}} P! \equiv a \cdot 2a \cdot 3a \cdot Pa \equiv (-1)^{\mu(a,p)} P! \implies a^{\frac{p-1}{2}} \equiv (-1)^{\mu(a,p)} \pmod{p}$$

■

In view of Gauss' Lemma, the quadratic reciprocity formula may now be rewritten as

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

To complete the proof, it suffices to show that

$$\mu(p,q) + \mu(q,p) \equiv \frac{p-1}{2}\cdot\frac{q-1}{2} \pmod 2$$

We do this somewhat sneakily: given distinct primes p, q construct the hexagon H as shown.

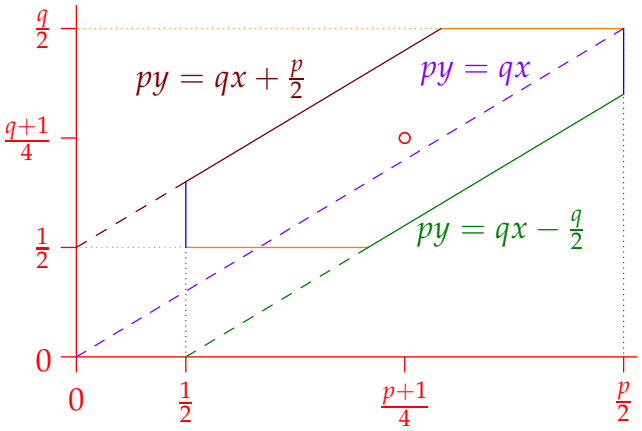
All points inside H satisfy four inequalities

$$\frac{1}{2} < x < \frac{p}{2} \qquad \frac{1}{2} < y < \frac{q}{2}$$

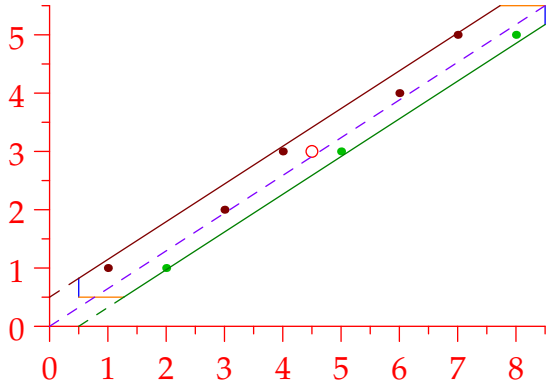
$$-\frac{q}{2} < py - qx < \frac{p}{2}$$

The circled point has co-ordinates $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$

We count the number of points with *integer* co-ordinates inside H in two ways, thereby recovering both sides of the desired congruence.

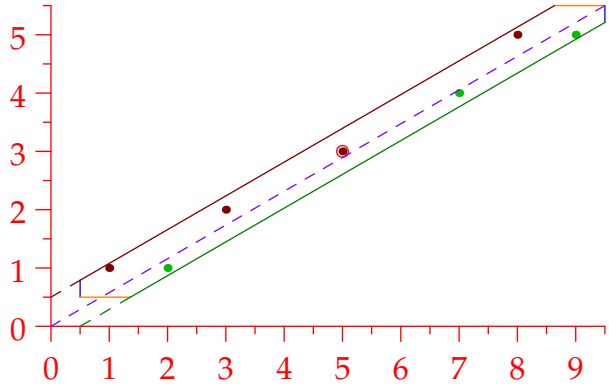


Here are two concrete examples where the integer points are plotted. We color the points differently depending on their location relative to the diagonal. Our goal is to relate the numbers of these points to values of Gauss' μ-function.



$p = 17,\ q = 11$

$\mu(p,q) + \mu(q,p) = 3 + 5$ is *even*



$p = 19,\ q = 11$

$\mu(p,q) + \mu(q,p) = 3 + 4$ is *odd*

The main result follows by observing some simple properties regarding the distribution of the integer points: see if you can make the relevant hypotheses *before* turning the page!

Lemma 7.28. *The integer points in H satisfy the following:*

1. *Symmetry around the circled point $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$. The number of integer points is odd precisely when the circled point has integer co-ordinates: when $p, q \equiv 3 \pmod 4$.*
2. *(a) No points lie on the boundaries or the diagonal of H.*
   (b) $\mu(p,q)$ points lie below the diagonal.
   (c) $\mu(q,p)$ points lie above the diagonal.

By part 2, the number of integer points in H is $\mu(p,q) + \mu(q,p)$. By part 1, this total is congruent to $\frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2$. The Lemma therefore establishes the required formula and completes the proof of the quadratic reciprocity law (Theorem 7.16).

Proof. 1. The reflection of (x,y) in the circled point is given by[a]

$$\left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$$

Since p, q are *odd*, this has integer co-ordinates if and only if (x,y) does.

It is moreover straightforward to check that the reflection maps opposite edges of H to each other: the circled point is therefore the centroid of H (and of the integer points therein).

2. (a) This is an easy exercise.

(b) Suppose $(x,y) \in H$ is an integer point lying below the diagonal. Since $(x,y) \in H$, we have

$$\frac{1}{2} < x < \frac{p}{2}, \quad \frac{1}{2} < y < \frac{q}{2}$$

To lie below the diagonal means

$$-\frac{q}{2} < py - qx < 0 \iff py \text{ has } \textit{negative least residue} \text{ modulo } q$$

Conversely, suppose y is an integer satisfying $\frac{1}{2} < y < \frac{q}{2}$ and such that py has negative least residue modulo q. Precisely one positive integer $x\,(> \frac{1}{2})$ satisfies the inequality $-\frac{q}{2} < py - qx < 0$. Moreover,

$$qx < py + \frac{q}{2} \implies x < \frac{p}{q}y + \frac{1}{2} < \frac{p}{q} \cdot \frac{q}{2} + \frac{1}{2} = \frac{p+1}{2} \implies x \leq \frac{p-1}{2} < \frac{p}{2}$$

since x is an *integer*. We therefore obtain a point $(x,y) \in H$ lying below the diagonal.
We conclude that there are precisely as many integer points below the diagonal as there are elements with negative least residue modulo q in the set

$$\left\{py : y = 1, \ldots, \tfrac{q-1}{2}\right\} = \left\{p, 2p, 3p, \ldots, \tfrac{q-1}{2}p\right\}$$

Otherwise said, there are $\mu(p,q)$ integer points below the diagonal.

(c) Being almost identical to part (b), we omit the argument. ∎

[a] If you're unsure why, observe that the midpoint of (x,y) and its reflection is $\left(\frac{p+1}{4}, \frac{q+1}{4}\right)$. Alternatively, think vector thoughts and compute $(x,y) + 2\left[\left(\frac{p+1}{4}, \frac{q+1}{4}\right) - (x,y)\right]\ldots$

Exercises 7.2 1. Recall Exercise 7.21. Compute the Legendre symbol $\left(\frac{246}{317}\right)$ *without* using Jacobi symbols: i.e. factorize 246 fully, and use reciprocity *only* if both terms are prime.

2. Evaluate the Legendre symbols $\left(\frac{503}{773}\right)$ and $\left(\frac{501}{773}\right)$ using any method you like.

3. (a) Pretend you don't know the prime factorization of 91. Compute $\left(\frac{9}{91}\right)$ and $9^{45} \pmod{91}$. What do you observe? Does this say anything about whether 91 is prime or composite?
   (b) Now compute $\left(\frac{2}{91}\right)$ and $2^{45} \pmod{91}$. What happens this time?

4. (a) Identify the witnesses and liars for the Solovay–Strassen test modulo 15.
   (b) Explain why there are *at least two* liars for every odd composite modulus n.
   (c) Let n be composite and suppose a is a witness and b a liar for n:

$$\gcd(a,n) = 1 = \gcd(b,n), \quad a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \text{ and } b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \pmod{n}$$

   By considering ab, prove there are at least as many witnesses as liars.
   (*This explains the $\frac{1}{2^k}$ probability estimation in the Solovay–Strassen test*)

5. A simpler primality test involves checking only that $a^{\frac{n-1}{2}} \equiv \pm 1$. Comment on your answer to question 3b, and compare what happens with the simple test and Solovay–Strassen for $a = 8$ modulo $n = 21$.

6. Compute the value of $\mu(12, 17)$ by finding the least residues of the set $\{12, 24, \ldots, 12 \cdot 8\}$. Confirm that your set of least residues and the value of μ fits with Gauss' Lemma.

7. Revisit Theorems 7.11 and 7.14, where we computed the values of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$. What are the values of $\mu(-1, p)$ and $\mu(2, p)$?

8. Use the law of quadratic reciprocity to prove that, for any prime $p \geq 5$, we have

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \iff p \equiv 1 \text{ or } 11 \pmod{12} \\ -1 & \iff p \equiv 5 \text{ or } 7 \pmod{12} \end{cases}$$

9. Verify the claim about the opposite sides of H being reflected to each other in the proof of Lemma 7.28. Also prove part 2(a) of the same result.

10. We prove parts 5 and 6 of Theorem 7.19.
    (a) Suppose that $n = p_1 \cdots p_k q_1 \cdots q_l$ is written as a product of primes where each $p_i \equiv 1$ and $q_j \equiv 3 \pmod{4}$. Prove that $n \equiv (-1)^l \pmod{4}$. Hence establish the formula for the Jacobi symbol $\left(\frac{-1}{n}\right)$.
    (b) (Harder) Prove the formula for the Jacobi symbol $\left(\frac{2}{n}\right)$.
    (*Hint: write n as a product of primes congruent to each of 1, 3, 5 and 7 modulo 8 and think about their products modulo 8*)

11. (For a bit of fun to end the term)
    (a) Find all the 2-digit integers x whose squares end in x (i.e. $10 \leq x \leq 99$).
    (b) Show that the only 3-digit integers x whose squares end in x are 376 and 625.
    (c) See how far you can generalize the problem…