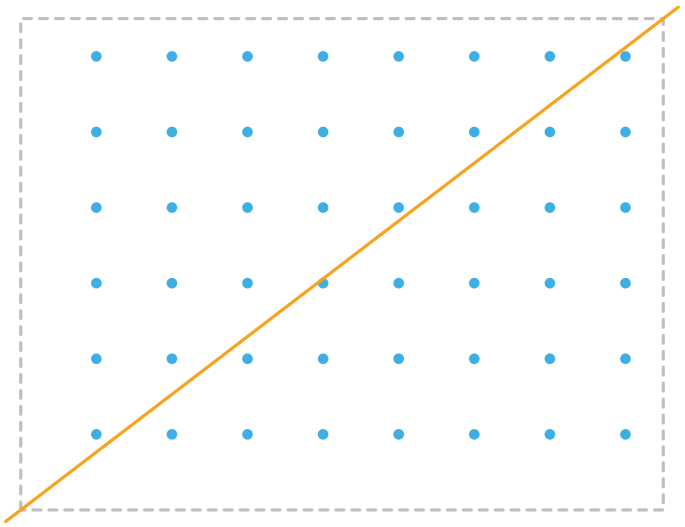
Johns Hopkins University

Egbert Rijke



The Arithmetic of Quadratic Forms

Book III

of

The Great Story of Numbers

Version: 0.261124-vol-3
Primary font: Libertinus
Supporting fonts: EB Garamond, GFS Artemisia, Noto Sans Cuneiform, STIX Two Math, Theano Didot
TeX engine: LuaHBTeX, Version 1.24.0 (TeX Live 2026); development id 7724
LaTeX format: LaTeX2e 2026-11-01
Document language: en-US
PDF version: 2.0
Accessibility standard: PDF/UA-2
Archival standard: PDF/A-4f
Tagging setup: MathML structure elements (math/setup=mathml-SE)

© 2025 Egbert Rijke.
All rights reserved.

Citing this work:

```
@book{rijke-0.261124-vol-3,
  author = {Egbert Rijke},
  title = {Book III of The Great Story of Numbers: The Arithmetic of
    Quadratic Forms},
  year = {2026},
  month = nov,
  note = {Version 0.261124-vol-3},
  url = {https://egbertrijke.github.io/notes/number-theory/}
}
```

Contents

27 Quadratic Residues · 379
27.1 Quadratic Congruences · 379
27.2 Quadratic Residues · 381
27.3 Legendre Symbols · 382
27.4 Euler's Criterion · 384
27.5 Euler's Prime-Generating Polynomial · 385
Exercises · 388

28 Quadratic Reciprocity · 393
28.1 The Quadratic Character of 2 · 393
28.2 The Statement of Quadratic Reciprocity · 398
28.3 Gauss's Lemma · 402
28.4 Eisenstein's Proof · 406
Exercises · 410

29 Primality Testing · 413
29.1 Pépin's Primality Test for the Fermat Numbers · 413
29.2 The Carmichael Numbers · 413
29.3 The Lucas–Lehmer Primality Test · 417
29.4 Pocklington's Criteria · 417
29.5 Mersenne Primes · 418
Exercises · 420

References · 421



Illustrations

28.1 Quadratic residues and nonresidues · 395
28.2 The least absolute residue bijection · 404
28.3 Gauss's lemma · 405
28.4 Eisenstein's proof of quadratic reciprocity · 408

Chapter 27

Quadratic Residues

27.1 Quadratic Congruences

A *quadratic congruence* is a congruence of the form

$$ax^2 + bx + c \equiv 0 \pmod{n},$$

where a is assumed to be relatively prime to n. To build intuition for such quadratic congruences, let's first recall how to solve a quadratic equation

$$ax^2 + bx + c = 0,$$

where $a \neq 0$. Since we have assumed that a is nonzero, we may divide through by a to obtain the equation

$$x^2 + \frac{b}{a}x = -\frac{c}{a}.$$

Completing the square, gives us the equation

$$\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a^2} - \frac{c}{a} = \frac{b^2 - 4ac}{4a^2}.$$

This equation has the familiar solutions

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

The number $\Delta := b^2 - 4ac$ is called the *discriminant* of the quadratic equation $ax^2 + bx + c = 0$. For example, the quadratic equation $x^2 - x - 1$ has discriminant 5, and therefore its solutions are

$$x = \frac{1 \pm \sqrt{5}}{2}.$$

Since the square root $\sqrt{k}$ of an integer k is an integer if and only if k is a perfect square, we obtain the following theorem:

THEOREM 27.1.1. *Consider the quadratic equation with integer coefficients*

$$ax^2 + bx + c = 0,$$

where $a \neq 0$. This equation has a rational solution if and only if the discriminant $\Delta = b^2 - 4ac$ is a perfect square.

Now consider an odd prime p. Recall from Theorem 20.3.2 (Lagrange's Theorem) that a polynomial congruence

$$f(x) \equiv 0 \pmod{p}$$

has at most n solutions, where n is the degree of f. It follows that a quadratic congruence modulo a prime has at most two solutions. In the following theorem, which is analogous to the previous theorem, we show that a quadratic congruence modulo an odd prime is solvable if and only if its discriminant is a perfect square.

The situation is slightly different for the prime $p = 2$, since the quadratic congruence

$$x^2 + x + 1 \equiv 0 \pmod{2}$$

has no solutions, even though the discriminant is a perfect square. Indeed, as we will see in the proof below, we will rely on the invertibility of 2 modulo p to solve general quadratic congruences modulo p, which is not possible if $p = 2$.

THEOREM 27.1.2. *Consider a quadratic congruence*

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

modulo an odd prime p, where $a \not\equiv 0 \pmod{p}$. This quadratic congruence is solvable if and only if the discriminant $\Delta = b^2 - 4ac$ is congruent to a square modulo p.

PROOF. Given that p is an odd prime and that $a \not\equiv 0 \pmod{p}$, it follows that $4a$ is invertible modulo p. The quadratic congruence in the statement of the theorem is therefore solvable if and only if the quadratic congruence

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$$

is solvable. Given a solution of this quadratic congruence, we calculate

$$\begin{aligned}(2ax + b)^2 &= 4a^2x^2 + 4abx + b^2 \\ &= 4a^2x^2 + 4abx + 4ac + b^2 - 4ac \\ &\equiv b^2 - 4ac\end{aligned}$$

modulo p. This shows that the discriminant is congruent to a square modulo p.

On the other hand, if the discriminant is congruent to a square modulo p, as in

$$y^2 \equiv b^2 - 4ac \pmod{p},$$

then we find, entirely analogous to the case of quadratic equations, that

$$x = \frac{-b \pm y}{2a}$$

solves the quadratic congruence modulo p. We leave the verification that such x is indeed a solution to the reader. □

27.2 Quadratic Residues

We have seen in the previous section that in order to solve a quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

modulo an odd prime p, we need to determine whether the discriminant $\Delta = b^2 - 4ac$ is congruent to a square modulo p. In other words, we need to determine whether the discriminant is a quadratic residue modulo p, which is defined as follows:

Definition 27.2.1. An integer a is said to be a *quadratic residue* modulo n if there is an integer x such that the congruence

$$x^2 \equiv a \pmod{n}$$

holds. If no such x exists, we say that a is a *quadratic nonresidue* modulo n.

For example, 0 and 1 are always quadratic residues modulo any natural number n. The number 0 is called the *trivial quadratic residue*, and we will mostly be interested in the nontrivial quadratic residues.

Modulo 3, the only quadratic residues are 0 and 1, since the quadratic congruence $x^2 \equiv 2 \pmod{3}$ does not have solutions. In other words, every square is either divisible by 3 or congruent to 1 modulo 3.

Similarly, 0 and 1 are the only quadratic residues modulo 4; that is, no square number can be congruent to 2 or 3 modulo 4. Indeed, the square of an even number is divisible by 4 and the square of an odd number is congruent to 1 modulo 4.

Modulo 5 we find that 0, 1, and 4 are quadratic residues, and we can similarly list all the quadratic. The following table lists the nontrivial quadratic residues modulo n from 4 to 10, where 0 is included as a quadratic residue if it is the square of a nonzero integer modulo n:

n	4	5	6	7	8	9	10
quadratic residues	0, 1	1, 4	1, 3, 4	1, 2, 4	0, 1, 4	0, 1, 4, 7	1, 4, 5, 6, 9

If we have access to a primitive root g of a prime p, then it is easy to characterize the nontrivial quadratic residues of p as the even powers of g. This has the immediate corollary that exactly half of the nonzero integers modulo p are quadratic residues.

PROPOSITION 27.2.2. *Consider a prime p with a primitive root g. An integer $a \not\equiv 0 \pmod{p}$ is a nontrivial quadratic residue modulo a p if and only if it is an even power of g.*

PROOF. Consider a primitive root g modulo p. If $a \equiv g^{2k} \pmod{p}$, then a is clearly a quadratic residue modulo p. On the other hand, if $x^2 \equiv a \pmod{p}$, and $x \equiv g^k \pmod{p}$, then we have $a \equiv g^{2k} \pmod{p}$. □

COROLLARY 27.2.3. *There are exactly $(p-1)/2$ nontrivial quadratic residues modulo p in the set $\{1, \ldots, p-1\}$, and exactly $(p-1)/2$ quadratic nonresidues.*

We now turn our attention to the quadratic congruence $x^2 \equiv 1 \pmod{n}$. When n is not a prime number, this congruence can have more solutions than its degree. For example, the quadratic congruence $x^2 \equiv 1 \pmod{8}$ has four distinct solutions. Similarly, the quadratic congruence $x^2 \equiv 1 \pmod{15}$ we have the four solutions

$$1^2 \equiv 1 \pmod{15}, \quad 4^2 \equiv 1 \pmod{15}, \quad 11^2 \equiv 1 \pmod{15}, \quad \text{and} \quad 14^2 \equiv 1 \pmod{15}.$$

In the following theorem we give a precise count of the number of solutions to this quadratic congruence.

THEOREM 27.2.4. *Consider a positive integer n, and let $\omega(n)$ be the number of its prime divisors. Then the number of integers $0 < x < n$ such that $x^2 \equiv 1 \pmod{n}$ is $2^{\omega(n)+\varepsilon(n)}$, where*

$$\varepsilon(n) := \begin{cases} 0 & \text{if } n \text{ is odd,} \\ -1 & \text{if } n \text{ is even but not divisible by } 4, \\ 0 & \text{if } n \text{ is divisible by } 4 \text{ but not by } 8, \\ 1 & \text{if } n \text{ is divisible by } 8. \end{cases}$$

27.3 Legendre Symbols

The fact that the integers $1, 2, \ldots, p-1$ can be split into the sets of quadratic residues and quadratic nonresidues, which are both of size $(p-1)/2$, suggests there is an interesting dichotomy between them. We can explore this further using primitive roots. If g is a primitive root modulo p, then the quadratic residues are precisely those integers modulo p that can be written as an even power of g, and the quadratic nonresidues are precisely those integers modulo p that can be written as an odd power of g. Now recall that

$$g^m g^k = g^{m+k},$$

and that the parity of the sum of two integers can be expressed in terms of the parity of the summands: The summands m and k have the same parity if and only if $m + k$ is

even, and likewise they have distinct parity if and only if $m + k$ is odd. This leads to the following multiplication rule of quadratic residues:

Proposition 27.3.1. *Consider two integers a and b modulo a prime p, both not divisible by p. Then we have*

(i) *If both a and b are quadratic residues, or both are quadratic nonresidues, then ab is a quadratic residue.*

(ii) *If one of a and b is a quadratic residue and the other is a quadratic nonresidue, then ab is a quadratic nonresidue.*

The previous proposition was also observed by Adrien-Marie Legendre, who published his findings in *Essai sur la théorie des nombres* in 1798 [Leg1798]. In this work, he also formulated the quadratic reciprocity theorem, and attempted to prove it. His approach, however, relied on unproven assumptions about certain functions, and was therefore incomplete.

Definition 27.3.2. The *Legendre symbol* of an integer a modulo a prime p, such that $p \nmid a$, is defined by

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

An immediate consequence of Proposition 27.2.2 is that

$$\left(\frac{a}{p}\right) = (-1)^{\operatorname{ind}_g(a)}$$

for any primitive root g modulo p. Using Legendre symbols, we can reformulate Proposition 27.3.1 succinctly as the *multiplicative law of Legendre symbols*: For any two integers a and b, both not multiples of p, the equality

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

holds. In fact, the Legendre symbol is the unique surjective function from the integers $\{1, \dots, p-1\}$ to $\{1, -1\}$ with this property.

Theorem 27.3.3. *Consider an odd prime p. Then the function $a \mapsto \left(\frac{a}{p}\right)$ is the unique surjective function $f : \{1, \dots, p-1\} \to \{1, -1\}$ preserving multiplication, in the sense that*

$$f(ab) = f(a)f(b)$$

for every two nonzero integers a and b modulo p.[1]

[1] In the language of group theory: The Legendre symbol is the unique surjective group homomorphism from the group $(\mathbb{Z}/p\mathbb{Z})^\times$ of invertible elements modulo p to the 2-element group S_2.

PROOF. We have already seen that the Legendre symbol is a surjective function preserving multiplication. Thus, our task is now to show that if $f : \{1, \dots, p-1\} \to \{1, -1\}$ is any surjective function preserving multiplication, then f is the Legendre symbol. Notice that for any primitive root g modulo p, we have

$$f(g^m) = f(g)^m.$$

since every element is of the form g^m, this implies that $f(g) = -1$. Then it follows that $f(g^m) = 1$ if and only if m is even, i.e., $f(a) = 1$ if and only if a is a quadratic residue modulo p. □

EXAMPLE 27.3.4. Recall that 2 is a primitive root of the prime 13, and is therefore a quadratic nonresidue. Using that the square of a Legendre symbol is always 1, we can compute the Legendre symbol $\left(\frac{8}{13}\right)$ as follows:

$$\left(\frac{8}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{2}{13}\right)\left(\frac{2}{13}\right) = \left(\frac{2}{13}\right) = -1.$$

Thus, 8 is a quadratic nonresidue modulo 13.

Similarly, using that $5 \equiv 18 \pmod{13}$ we can compute the Legendre symbol $\left(\frac{5}{13}\right)$ as follows:

$$\left(\frac{5}{13}\right) = \left(\frac{18}{13}\right) = \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{2}{13}\right) = -1.$$

We see that 5 is also a quadratic nonresidue modulo 13.

On the other hand, again using that the square of a Legendre symbol is always 1, we can compute the Legendre symbol $\left(\frac{3}{13}\right)$ as follows:

$$\left(\frac{3}{13}\right) = \left(\frac{3}{13}\right)\left(\frac{3}{13}\right)\left(\frac{3}{13}\right) = \left(\frac{27}{13}\right) = \left(\frac{1}{13}\right) = 1.$$

Thus we see that 3 is a quadratic residue modulo 13. In fact, we can readily verify that $3 \equiv 4^2 \pmod{13}$. The set of all nontrivial quadratic residues modulo 13 is

$$\{1, 3, 4, 9, 10, 12\}.$$

27.4 Euler's Criterion

Euler had a deep understanding of numbers that are congruent to a square modulo a prime. In 1748 he had published a result now known as *Euler's criterion*, which characterized precisely the squares modulo a prime.

THEOREM 27.4.1 (Euler's Criterion). *Consider an integer a and an odd prime p. Then we have*

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

Proof. First note that Theorem 16.1.1 (Fermat's Little Theorem) gives that if $b := a^{\frac{p-1}{2}}$, then

$$b^2 \equiv 1 \pmod{p}.$$

This implies that $b \equiv \pm 1 \pmod{p}$.

To prove the congruence in Euler's Criterion, consider a primitive root g modulo p, and suppose that $g^m \equiv a \pmod{p}$. Then a is a quadratic residue if and only if m is even. Also, we note that

$$\frac{m(p-1)}{2}$$

is a multiple of $p-1$ if and only if m is even. Thus we see that

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

if and only if a is a quadratic residue, and it is congruent to -1 otherwise. □

Using Euler's Criterion, we can give a new proof of Theorem 16.5.1. In the language of quadratic residues, Theorem 16.5.1 states that -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \pmod{4}$. In other words,

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

This description of the quadratic character of -1 is also called the *first supplement* of the law of quadratic reciprocity.

Proof of Theorem 16.5.1 using Euler's criterion. By Theorem 27.4.1 (Euler's Criterion), it follows that -1 is a quadratic residue modulo p if and only if

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Since $(-1)^m \equiv 1 \pmod{p}$ if and only if m is even, it follows that -1 is a quadratic residue modulo p if and only if $\frac{p-1}{2}$ is even, which holds if and only if

$$p \equiv 1 \pmod{4}.$$ □

27.5 Euler's Prime-Generating Polynomial

In the early 1770s, Leonhard Euler devised his famous prime-generating polynomial

$$n^2 + n + 41.$$

This polynomial produces prime numbers for any $0 \leq n \leq 39$. Note that

$$40^2 + 40 + 41 = 40(40+1) + 41 = 41^2$$



isn't prime anymore. We could easily imagine Euler pondering one day over the question of creating a quadratic polynomial that returns a surprising amount of primes, and it would be natural to wonder how he might have approached the problem.

Of course, there is no polynomial $f(x)$ other than a constant polynomial such that $f(x)$ is a prime number for every integer x.

PROPOSITION 27.5.1. *If every value of a polynomial $f(x)$ is prime, then $f(x)$ is constant.*

PROOF. Suppose $f(x)$ is a polynomial, all of whose values are prime. Then in particular $p := f(0)$ is prime. Then $p \mid f(kp)$ for every integer k. Since each value of f is prime, it follows that $f(kp) = p$ for every integer k. This implies that $f(x) - p$ has infinitely many roots, i.e., $f(x)$ is the constant polynomial with value p. □

As a reasonable starting point for our search, we take three consecutive primes of the form

$$q,\ q+2,\ \text{and}\ q+6.$$

By Theorem 20.4.2 (Lagrange's Interpolation Theorem), there is only one polynomial f such that $f(n)$ assumes those values for $n = 0, 1, 2$:

$$f(n) = n^2 + n + q.$$

Thus we are faced with the task of finding a prime q such that $n^2 + n + q$ is prime for $0 \le n \le q - 2$. One thing to note is that if the number

$$n^2 + n + q$$

is composite for some $0 \le n \le q - 2$, then it must have a prime factor below q. Indeed, we have $n^2 + n + q < q^2$ for such n, so if $n^2 + n + q$ is composite for any $0 \le n \le q - 2$ then it has an odd prime factor $p < q$. In other words, we want to find an odd prime q such that

$$n^2 + n + q \not\equiv 0 \pmod{p}$$

for any odd prime $p < q$. Recall from Theorem 27.1.2 that such an incongruence holds if and only if the discriminant $\Delta = 1 - 4q$ is a quadratic nonresidue modulo p for any odd prime $p < q$. By Theorem 27.4.1 (Euler's Criterion), this observation finally narrows our search: We are looking for a prime q such that

$$(1 - 4q)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

for any odd prime $p < q$.

We can now discover prime-generating polynomials of the form $n^2 + n + q$ by computing the integer $1 - 4q \pmod{p}$ for all odd primes $3 < p < q$. If we can find a prime p such that $1 - 4q$ is a quadratic residue mod p, we may discard that prime from the remainder of the search. This process resulted in Table 27.1, which reveals that the

$q \setminus p$	3	5	7	11	13	17	19	23	29	31	37
5	2										
7	0	-									
11	2	2	6								
13	0	-	-	-							
17	2	3	3	10	11						
19	0	-	-	-	-	-					
23	2	4	-	-	-	-	-				
29	2	0	-	-	-	-	-	-			
31	0	-	-	-	-	-	-	-	-		
37	0	-	-	-	-	-	-	-	-	-	
41	2	2	5	2	6	7	8	21	11	23	22

Table 27.1: Residues of the discriminant $\Delta = 1 - 4q$ modulo an odd prime $p < q$, for the polynomial $n^2 + n + q$.
Computations of residues for $q \leq p$ are omitted. A dash indicates that it was not necessary to compute this residue, because a quadratic residue has been encountered earlier.

following polynomials are prime-generating polynomials, in the sense that they yield prime numbers for all inputs $0 \leq n \leq q - 2$:

$$n^2 + n + 2 \qquad\qquad n^2 + n + 11$$
$$n^2 + n + 3 \qquad\qquad n^2 + n + 17$$
$$n^2 + n + 5 \qquad\qquad n^2 + n + 41.$$

A deep theorem, the Baker–Heegner–Stark Theorem, shows that these are the only prime-generating polynomials of the form $n^2 + n + q$. In other words, Euler had in fact found the quadratic polynomial of this kind with the longest streak of primes! For this reason, the number 41 is sometimes called Euler's lucky prime.



Exercises

Starter Exercises

27.1 Find all the quadratic residues modulo:

(a) 23,
(b) 29,
(c) 31,
(d) 37.

Confirm in each case that the number of quadratic residues is $(p-1)/2$.

27.2 Compute the Legendre symbols

(a) $\left(\frac{5}{11}\right)$,
(b) $\left(\frac{7}{17}\right)$,
(c) $\left(\frac{3}{19}\right)$.

27.3 Compute the Legendre symbols

(a) $\left(\frac{6}{11}\right)$,
(b) $\left(\frac{12}{17}\right)$,
(c) $\left(\frac{15}{19}\right)$.

27.4 List all the odd primes below 100 of which:

(a) 2 is a quadratic residue,
(b) 3 is a quadratic residue,
(c) 5 is a quadratic residue,
(d) 7 is a quadratic residue.

27.5 Show that the system of congruences

$$\begin{aligned} x + y &\equiv 0 \pmod{p}, \\ xy &\equiv 1 \pmod{p} \end{aligned}$$

is solvable if and only if $p \equiv 1 \pmod{4}$.

Routine-Building Exercises

27.6 Show that for any prime p, the polynomial $x^2 + x + 1$ has a root modulo p if and only if the polynomial $x^2 + x + 7$ has a root modulo p.

27.7 Consider an integer a and a prime p. Show that $-a$ is a quadratic residue modulo p if and only if p divides a number of the form $x^2 + ay^2$.

27.8 (a) Consider a prime $p \equiv 1 \pmod{4}$. Show that g is a primitive root modulo p if and only if $-g$ is a primitive root modulo p.
(b) Consider a prime $p \equiv 3 \pmod{4}$. Show that g is a primitive root modulo p if and only if $-g$ has order $(p-1)/2$ modulo p.

(f)

$p\backslash q$	3	5	7	11	13	17	19	23	29	31
3	-	1	2	1	2	1	2	1	1	2
5	1	-	1	4	1	1	2	1	2	4
7	1	1	-	2	3	1	1	2	6	1
11	2	2	1	-	1	1	1	10	1	2
13	4	3	1	1	-	2	1	2	4	3
17	1	1	1	1	4	-	2	1	1	1
19	1	2	6	6	1	2	-	2	1	3
23	2	1	1	1	2	1	1	-	2	2
29	1	2	4	1	2	7	1	4	-	1
31	1	10	2	1	1	1	2	3	3	-

Table 27.2: The value $(p-1)/\operatorname{ord}_p(q)$, with p and q ranging over the first ten odd primes. Note that the value 1 indicates that q is a primitive root modulo p.

27.9 Consider an odd prime p and an integer a.

(a) Show that if $\operatorname{ord}_p(a)$ is odd, then $\left(\frac{a}{p}\right) = 1$.

(b) Show that if $\left(\frac{a}{p}\right) = -1$, then $\operatorname{ord}_p(a)$ is even.

(c) Give an example where $p \equiv 1 \pmod 4$ and where a is an integer of even order modulo p, such that $\left(\frac{a}{p}\right) = 1$.

(d) Show that if $p \equiv 3 \pmod 4$ and $\operatorname{ord}_p(a) = 2k$ is an even number, then we have

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

and $a^k \equiv -1 \pmod p$. Thus, in the case where $p \equiv 3 \pmod 4$, the quadratic residues are precisely the integers of odd order, and the quadratic nonresidues are precisely the integers of even order.

(e) Show that if $p \equiv 1 \pmod 4$ and $\operatorname{ord}_p(a)$ is even, then $\left(\frac{a}{p}\right) = 1$ if and only if $\operatorname{ord}_p(a) \mid \frac{p-1}{2}$.

Combine the previous parts to show that for any odd prime p and for any integer $a \not\equiv 0 \pmod p$, we have the identity

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\operatorname{ord}_p(a)}}.$$

Table 27.2 lists the values of $\frac{p-1}{\operatorname{ord}_p(a)}$, where p and q range over the first ten primes.

(g) Using Exercise 21.7, give a direct proof of the identity

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\operatorname{ord}_p(a)}}.$$

27.10 Consider an odd prime p, an integer a, and an integer m. Show that

$$a^m \equiv \left(\frac{a}{p}\right) \pmod{p} \quad \Leftrightarrow \quad m \equiv \frac{p-1}{2} \pmod{\operatorname{ord}_p(a)}.$$

Challenge Exercises

27.11 Recall that a Fermat prime is a prime of the form $F_n := 2^{2^n} + 1$. Show that the following are equivalent for a prime number p:

(i) The prime p is a Fermat prime.

(ii) Every quadratic nonresidue modulo p is a primitive root.

27.12 (a) Show that $\left(\frac{-3}{p}\right) = 1$ if and only if $p \equiv 1 \pmod{3}$.

(b) For any finite set $p_1, \ldots, p_k$ of primes congruent to 1 modulo 3, use the prime divisors of

$$n = (p_1 \cdots p_k)^2 + 3$$

to show that there is a prime $q \equiv 1 \pmod{3}$ that is not already among the primes $p_1, \ldots, p_k$. Conclude that there are infinitely many primes congruent to 1 modulo 3.

27.13 (a) Show that $\left(\frac{5}{q}\right) = \left(\frac{q}{5}\right)$ holds for every prime $q \neq 5$. In other words, which two congruence classes 1, 2, 3, or 4 modulo 5 contain the primes q such that 5 to be a quadratic residue modulo q?

(b) For any finite set of primes $p_1, \ldots, p_k$ congruent to 1 modulo 5, use the prime divisors of

$$(2p_1 \cdots p_k)^4 + 5$$

to show that there is a prime $q \equiv 1 \pmod{5}$ that is not already among the primes $p_1, \ldots, p_k$. Conclude that there are infinitely many primes congruent to 1 modulo 5.

27.14 Consider an odd prime p.

(a) For any positive integer m and any integer a, show that a is a quadratic residue modulo p^m if and only if a is a quadratic residue modulo p.

(b) Conclude that there are exactly

$$\frac{(p-1)p^m}{2}$$

quadratic residues modulo p^{m+1} that are not divisible by p.

27.15 Recall that a prime p is said to be a Sophie Germain prime if the number $q = 2p + 1$ is prime.

(a) Show that p is a Sophie Germain prime if and only if every quadratic nonresidue modulo q apart from -1 is a primitive root modulo q.

(b) Show that if $p \equiv 1 \pmod 4$ is a Sophie Germain prime, then 2 is a primitive root modulo q.

(c) Show that if $p \equiv 3 \pmod 4$ is a Sophie Germain prime, then -2 is a primitive root modulo q.

27.16 Consider the Fibonacci sequence (F_n). For parts (a) and (b) assume that $p \neq 2, 5$ is a prime, and define

$$h := \frac{p - \left(\frac{5}{p}\right)}{2}.$$

(a) Show that

$$F_{n+2h} \equiv \left(\frac{5}{p}\right) F_n \pmod p.$$

(b) Show that

$$F_{h+n} \equiv (-1)^{n+1} \left(\frac{-1}{p}\right) F_{h-n} \pmod p.$$

(c) Show that there does not exist an odd prime p such that for all $0 \leq k \leq p-1$, we have $k \equiv s^2$ for some s if and only if $k \equiv F_n \pmod p$ for some Fibonacci number n.

Chapter 28

Quadratic Reciprocity

28.1 The Quadratic Character of 2

In this section we consider the question for which odd primes p we have that 2 is a quadratic residue. By Exercise 27.9, this is equivalent to the question for which primes p we have

$$\frac{p-1}{\operatorname{ord}_p(2)} \equiv 0 \pmod{2}.$$

In the following table we list the quantity $\frac{p-1}{\operatorname{ord}_p(2)}$ for the odd primes below 50:

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\frac{p-1}{\operatorname{ord}_p(2)}$	1	1	2	1	1	2	1	2	1	6	1	2	3	2.

This table shows that 2 is a quadratic residue modulo p for the primes

$$7,\ 17,\ 23,\ 31,\ 41,\ 47,\ \ldots.$$

Unlike the case where we were seeking to characterize the primes for which -1 is a primitive root, these primes are not organized according to their residue class modulo 4. The pattern is slightly more complicated. However, we may observe that the primes for which 2 is a quadratic residue all happen to be close to a multiple of 8, while the primes for which 2 is a quadratic nonresidue are further from the multiples of 8. This turns out to be the right idea: The number 2 is a quadratic residue modulo p if and only if p is of the form $8k \pm 1$.

Note also that 2 is a primitive root if and only if $\operatorname{ord}_p(2) = p-1$, so we see from the previous table that 2 is a primitive root modulo p for the primes

$$3,\ 5,\ 11,\ 13,\ 19,\ 29,\ 37,\ \ldots.$$

However, it is not quite true that 2 is a primitive root modulo p whenever it is a quadratic nonresidue modulo p: The first prime for which 2 is neither a quadratic residue nor a primitive root is 43.

THEOREM 28.1.1. *The Legendre symbol of 2 modulo an odd prime p satisfies the identity*

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

In other words, 2 is a quadratic residue if and only if $p \equiv \pm 1 \pmod 8$, and it is a quadratic nonresidue if and only if $p \equiv \pm 3 \pmod 8$.

Before we start the proof, recall that one of the proofs of Theorem 16.1.1 (Fermat's Little Theorem) was obtained by multiplying all the numbers $1, \ldots, p-1$ with an integer a to obtain the congruence

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

Since $(p-1)!$ isn't divisible by p, it is invertible modulo p and thus we found that $a^{p-1} \equiv 1 \pmod p$.

PROOF. In this proof, we will write $P := \frac{p-1}{2}$ so that $2P = p-1$. By Theorem 27.4.1 (Euler's Criterion) we have $\left(\frac{2}{p}\right) \equiv 2^P \pmod p$, which gives us the congruences

$$\left(\frac{2}{p}\right)P! \equiv 2^P P! \equiv 2 \cdot 4 \cdot \cdots \cdot (2P) \pmod p$$

We proceed by carefully analyzing this product of all the even positive integers below p. If we define the numbers

$$s := \left\lfloor \frac{p-1}{4} \right\rfloor \qquad \text{and} \qquad t := \left\lfloor \frac{p+1}{4} \right\rfloor,$$

so that $s + t = P$, then we can partition the set of all even positive integers below p into two subsets

$$S := \{2k \mid 1 \le k \le s\} \qquad \text{and} \qquad T := \{2k \mid s+1 \le k \le P\},$$

so that S consists precisely of all the even positive integers up to and possibly including P, and T consists of all the larger even integers up to and including $2P$. Note that the set S has s elements and the set T has exactly t elements.

The key observation is that for every integer y in T there is a unique *odd* integer $1 \le x \le P$ so that $y = p - x$, which determines a bijection. Thus, taking the product

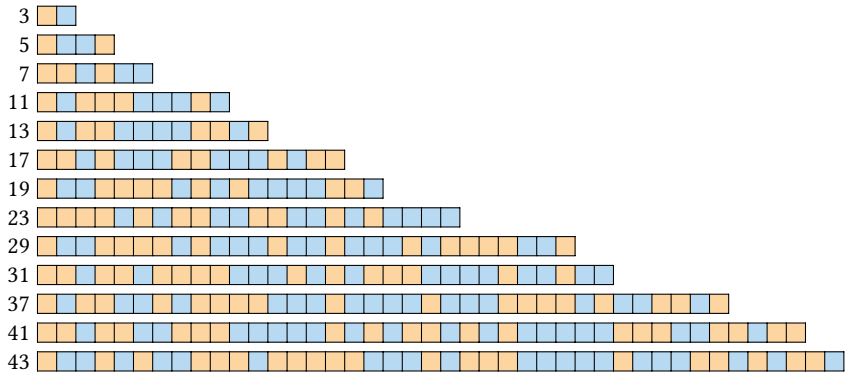


Figure 28.1: Quadratic residues (orange) and nonresidues (blue) among the integers $1, \dots, p-1$, for odd primes $3 \leq p \leq 43$.

modulo p of all the even integers up to p amounts to taking the product of all the integers $1 \leq x \leq P$ with a sign change for every odd integer, of which there are t. In other words, we have the congruence

$$\left(\frac{2}{p}\right) P! \equiv 2 \cdot 4 \cdot \cdots \cdot 2P \equiv (-1)^t P! \pmod{p}.$$

Since $P!$ is not divisible by p we apply the cancellation law to obtain

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

We conclude the proof by observing that the parity of t is determined according to the following cases:

$$t \equiv \begin{cases} 0 \pmod 2 & \text{if } p \equiv \pm 1 \pmod 8 \\ 1 \pmod 2 & \text{if } p \equiv \pm 3 \pmod 8. \end{cases}$$

□

We will present a second combinatorial proof, due to Thomas Joannes Stieltjes [Sti1884].

Proof. We will write $P := \frac{p-1}{2}$. Call a number $1 \leq k \leq p-2$ a **variation** if one of k and $k+1$ is a residue and the other is a nonresidue. That is, if we color the residues orange and the nonresidues blue, as we did in Figure 28.1, then k is a variation if k and $k+1$ have distinct colors. We first claim that there are exactly P variations.

To see this, note that k is a variation if and only if $k(k+1)$ is a nonresidue. Defining $r_k := \frac{k+1}{k}$, so that $k^2 r_k \equiv k(k+1)$, we see that k is a variation if and only if r_k is a nonresidue. Furthermore, the map $k \mapsto r_k$ is a bijection

$$\{1, \dots, p-2\} \cong \{2, \dots, p-1\}$$

with inverse $k \mapsto \frac{1}{k-1}$. Since there are exactly P nonresidues in the latter set, the claim follows. Consequently, we observe that since the sequence $1, \dots, p-1$ begins with a residue and contains exactly P variations, it follows that $-1 \equiv p-1 \pmod{p}$ is a residue if and only if P is even. That is, -1 is a residue if and only if $p \equiv 1 \pmod{4}$.

Observe that k is a variation if and only if $p-k-1$ is a variation. Ideed, multiplying by -1 either preserves the residuosity of both members of a consecutive pair of numbers or reverses the residuosity of both. This implies that variations occur in pairs

$$\{k, p-k-1\}$$

Each of these sets has exactly two elements, except the set $\{P, p-P-1\} = \{P\}$. Since the number of variations is P, we see that P is a variation if and only if P is odd. It also follows that the number of variations in the set $\{1, \dots, P-1\}$ is

$$\begin{cases} \frac{p-1}{4} & \text{if } p \equiv 1 \pmod{4}, \\ \frac{p-3}{4} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

There are now two cases, each of which splits in two further cases. If $p \equiv 1 \pmod{4}$, then the congruence $2P \equiv -1 \pmod{p}$ shows that 2 is a residue if and only if P is. Furthermore, P is a residue if and only if P is preceeded by an even number of variations. The number of variations preceeding P is $(p-1)/4$, so we conclude that 2 is a residue if $p \equiv 1 \pmod{8}$, and a nonresidue if $p \equiv 5 \pmod{8}$.

If $p \equiv 3 \pmod{4}$, then the congruence $2P \equiv -1 \pmod{p}$ shows that 2 is a residue if and only if P is a nonresidue. As before, P is a residue if and only if P is preceeded by an even number of variations, which is $(p-3)/4$, so we conclude that 2 is a residue if $p \equiv 7 \pmod{8}$ and a nonresidue if $p \equiv 3 \pmod{8}$. □

The previous theorem is also known as the *Second Supplement* of the law of Quadratic Reciprocity. An immediate corollary of the second supplement is that

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

Since primitive roots are always quadratic nonresidues, we obtain the following corollary. Artin conjectured that there are infinitely many primes p for which 2 is a primitive root. More generally, he conjectured that for any integer a that is neither -1 nor a perfect square, there are infinitely many primes for which a is a primitive root.

COROLLARY 28.1.2. *If 2 is a primitive root modulo p, then* $p \equiv \pm 3 \pmod{8}$.

The second supplement can be used to show that there are infinitely many primes of the form $8k+r$ for any odd number $0 < r < 8$. We have already seen in Theorem 16.6.1 that there are infinitely many primes congruent to 1 modulo 2^n. In particular, there are infinitely many primes of the form $8k+1$. It remains prove the analogous claims for the residue classes 3, 5, and 7 modulo 8. We will be following Sierpiński [SIE1988]. The first ten primes congruent to r moduo 8 for each odd residue class r are given in Table 28.1.

	1st	2nd	3rd	4th	5th	6th	7th	8th	9th	10th
$r = 1$	17	41	73	89	97	113	137	193	233	241
$r = 3$	3	11	19	43	59	67	83	107	131	139
$r = 5$	5	13	29	37	53	61	101	109	149	157
$r = 7$	7	23	31	47	71	79	103	127	151	167

Table 28.1: The first ten primes congruent to r modulo 8, for $r = 1, 3, 5, 7$.

Theorem 28.1.3. *There are infinitely many primes congruent to* 3 *modulo* 8.

Proof. If a is an odd integer, then $a^2 \equiv 1 \pmod 8$ so that

$$N_a := a^2 + 2$$

is congruent to 3 modulo 8. Not all prime divisors of N_a can be congruent to ± 1 modulo 8, since if they were, then N_a would likewise be congruent to ± 1 modulo 8. Therefore N_a has a prime divisor q so that

$$q \equiv \pm 3 \pmod 8.$$

Since $q \mid a^2 + 2$, it follows that -2 is a quadratic residue modulo q, so $q \not\equiv -3 \pmod 8$. Thus it follows that $q \equiv 3 \pmod 8$.

For a suitable choice of a, let p_n be the nth prime number, so that $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ and so forth. Then we define

$$a = p_2 p_3 \cdots p_n,$$

so that any prime divisor of N_a is larger than p_n. Since N_a has a prime divisor congruent to 3 modulo 8, it follows that there are arbitrarily large such primes. □

Theorem 28.1.4. *There are infinitely many primes congruent to* 5 *modulo* 8.

Proof. If a is an odd integer, then $a^2 \equiv 1 \pmod 8$ so that

$$N_a := a^2 + 4$$

is congruent to 5 modulo 8. As before, there must be a prime divisor q of N_a so that

$$q \equiv \pm 3 \pmod 8.$$

Since $q \mid a^2 + 4$, it follows that -4 is a quadratic residue modulo q. This implies that -1 is a quadratic residue modulo q, so that $q \equiv 1 \pmod 4$. Since we assumed that $q \not\equiv 1 \pmod 8$, it follows that $q \equiv -3 \pmod 8$.

For a suitable choice of a, define

$$a = p_2 p_3 \cdots p_n$$

so that any prime divisor of N_a is larger than p_n. Since N_a has a prime divisor congruent to 5 modulo 8, it follows that there are arbitrarily large such primes. □

THEOREM 28.1.5. *There are infinitely many primes congruent to* 7 *modulo* 8.

PROOF. The idea of the proof is to find a natural number N of the form

$$N = 2a^2 - b^2,$$

so that $N \equiv -1 \pmod 8$ and N is relatively prime to any $m \leq n$. Assuming that $n > 1$, a suitable choice of a and b is $a := n!$ and $b := 1$. Indeed, in this case a is even, so that $2a^2 - 1 \equiv -1 \pmod 8$.

Under these assumptions, N will have a prime factor $q \not\equiv 1 \pmod 8$, and furthermore we will have

$$2a^2 \equiv b^2 \pmod q.$$

Since a^2 and b^2 are clearly quadratic residues modulo q, it follows that 2 is a quadratic residue, implying that $q \equiv \pm 1 \pmod 8$. However, since we have chosen q so that $q \not\equiv 1 \pmod 8$, it follows that $q \equiv -1 \pmod 8$. Furthermore, since q is relatively prime to any $m \leq n$, it follows that $n < q$, which shows that there are arbitrarily large primes $q \equiv -1 \pmod 8$. □

28.2 The Statement of Quadratic Reciprocity

We have already established several facts about Legendre symbols. The Legendre symbol is multiplicative, meaning that

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

The Legendre symbol $\left(\frac{-1}{p}\right)$ can be computed according to whether p is congruent to 1 or 3 modulo 4:

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

The Legendre symbol $\left(\frac{2}{p}\right)$ can likewise be computed according to whether p is congruent to ± 1 or ± 3 modulo 8:

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

We need one final piece to effectively compute Legendre symbols: a way to determine the Legendre symbol $\left(\frac{q}{p}\right)$ when q is an odd prime. The recipe for determining $\left(\frac{q}{p}\right)$ is given by the law of quadratic reciprocity.

To build some intuition for what the law of quadratic reciprocity should assert, we recall from Exercise 27.9 that the Legendre symbol of a modulo p can be computed by

$$\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\operatorname{ord}_p(a)}}.$$

$p\backslash q$	3	5	7	11	13	17	19	23	29	31
3		−	+	−	+	−	+	−	−	+
5	−		−	+	−	−	+	−	+	+
7	−	−		+	−	−	−	+	+	−
11	+	+	−		−	−	−	+	−	+
13	+	−	−	−		+	−	+	+	−
17	−	−	−	−	+		+	−	−	−
19	−	+	+	+	−	+		+	−	−
23	+	−	−	−	+	−	−		+	+
29	−	+	+	−	+	−	−	+		−
31	−	+	+	−	−	−	+	−	−	

Table 28.2: The sign of the Legendre symbol $\left(\frac{q}{p}\right)$, ranging over pairs of distinct odd primes p and q.

Thus, the Legendre symbol of a modulo p depends only of the parity of the quantity

$$\frac{p-1}{\operatorname{ord}_p(a)},$$

which gives us a fairly quick way of determining the Legendre symbol $\left(\frac{q}{p}\right)$ for small odd primes p and q. We listed signs of the Legendre symbols of q modulo p in Table 28.2.

The patterns in this table might not be immediately apparent. However, those who did Exercise 27.13 might spot that column 5 is identical to row 5. Looking for more identical columns and rows, we create a new table by comparing the entry in row i and column j in Table 28.2 with the entry in row j and column i. When these two entries are equal, we mark it with a solid black circle (●), and if they are different we mark it with an open circle (○). This results in the following table:

Using this table, we quickly spot that columns 5, 13, 17, and 29 are identical to rows 5, 13, 17, and 29, respectively, which means that these columns were also identical to their respective rows in Table 28.2. Something special is going on with the primes

$$5,\ 13,\ 17,\ 29,$$

and something seems to be off about the primes

$$3,\ 7,\ 11,\ 19,\ 23,\ 31.$$

We are very familiar with this grouping of the primes by now: The first set of primes are all congruent to 1 modulo 4, while the second set of primes are all congruent to 3 modulo 4. These observations suggest the following:

$p\backslash q$	3	5	7	11	13	17	19	23	29	31
3		●	○	○	●	●	○	○	●	○
5	●		●	●	●	●	●	●	●	●
7	○	●		○	●	●	○	○	●	○
11	○	●	○		●	●	○	○	●	○
13	●	●	●	●		●	●	●	●	●
17	●	●	●	●	●		●	●	●	●
19	○	●	○	○	●	●		○	●	○
23	○	●	○	○	●	●	○		●	○
29	●	●	●	●	●	●	●	●		●
31	○	●	○	○	●	●	○	○	●	

(i) If at least one of p and q is congruent to 1 modulo 4, then we have

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

(ii) If both p and q are congruent to 3 modulo 4, then we have

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

Legendre and Gauss spotted these patterns towards the end of the 18th century. They formulated it succinctly as follows:

THEOREM 28.2.1 (The Law of Quadratic Reciprocity). *For any two distinct odd primes p and q we have*

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

EXAMPLE 28.2.2. The law of quadratic reciprocity is incredibly effective in computations of Legendre symbols. For example, since 17 and 101 are congruent to 1 modulo 4, we have

$$\left(\frac{17}{101}\right) = \left(\frac{101}{17}\right) = \left(\frac{16}{17}\right) = \left(\frac{4}{17}\right)\left(\frac{4}{17}\right) = 1.$$

Indeed, it turns out that $44^2 \equiv 17$ and $57^2 \equiv 17$ modulo 101.

On the other hand, both 23 and 43 are congruent to 3 modulo 4, so the law of quadratic reciprocity tells us that

$$\left(\frac{23}{43}\right) = -\left(\frac{43}{23}\right) = -\left(\frac{20}{23}\right) = -\left(\frac{4}{23}\right)\left(\frac{5}{23}\right) = -\left(\frac{5}{23}\right) = -\left(\frac{23}{5}\right) = -\left(\frac{3}{5}\right) = 1.$$

In this case, it turns out that $18^2 \equiv 23$ and $25^2 \equiv 23$ modulo 43.

As a final example, for good measure, note that 31 and 83 are both congruent to 3 modulo 4. Using the law of quadratic reciprocity we obtain that

$$\left(\frac{31}{83}\right) = -\left(\frac{83}{31}\right) = -\left(\frac{21}{31}\right) = -\left(\frac{3}{31}\right)\left(\frac{7}{31}\right) = -\left(\frac{31}{3}\right)\left(\frac{31}{7}\right) = -\left(\frac{1}{3}\right)\left(\frac{3}{7}\right) = \left(\frac{7}{3}\right) = 1.$$

The quadratic residuosity of an odd prime q modulo a distinct odd prime p determines some important restrictions on the form of the prime p. We spell these out in the following theorem, which is essentially a reformulation of the law of quadratic reciprocity.

Theorem 28.2.3. *Consider two distinct odd primes p and q. The following two statements hold:*

(i) *If $p \equiv 1 \pmod 4$, then q is a quadratic residue modulo p if and only if there exists an odd integer $0 < a < q$ such that*

$$p \equiv a^2 \pmod{4q}.$$

(ii) *If $p \equiv 3 \pmod 4$, then q is a quadratic residue modulo p if and only if there exists an odd integer $0 < a < q$ such that*

$$p \equiv -a^2 \pmod{4q}.$$

Proof. Before proving each statement, we note that for any $u \not\equiv 0 \pmod q$, if the quadratic congruence

$$x^2 \equiv u \pmod q$$

is solvable, then it has two solutions. Of these two solutions, one is even and the other is odd. Thus, if it is solvable, we can always pick an odd solution.

For the first claim of the theorem, assume that $p \equiv 1 \pmod 4$. By the law of quadratic reciprocity, it follows that

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

Furthermore, $\left(\frac{p}{q}\right) = 1$ if and only if there exists an odd integer $0 < a < q$ such that $p \equiv a^2 \pmod q$. Furthermore, since a is odd and $p \equiv 1 \pmod 4$, it also follows that $p \equiv a^2 \pmod 4$. Thus we see that $\left(\frac{q}{p}\right) = 1$ if and only if there exists an odd integer $0 < a < q$ such that

$$p \equiv a^2 \pmod{4q}.$$

For the second claim, assume that $p \equiv 3 \pmod 4$. By the law of quadratic reciprocity, it follows that

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

By rearranging the terms, we find that $\left(\frac{q}{p}\right) = \left(\frac{-p}{q}\right)$, and thus there is an odd integer a such that

$$p \equiv -a^2 \pmod{q}.$$

Since a is assumed to be odd and $p \equiv 3 \pmod{4}$, we find furthermore that $-a^2 \equiv p \pmod{4}$. We conclude that $\left(\frac{q}{p}\right) = 1$ if and only if there is an odd integer $0 < a < q$ such that

$$p \equiv -a^2 \pmod{4q}.$$ □

The previous theorem can be used at once to characterize the primes p for which 3 is a quadratic residue modulo p. Taking $q = 3$ in the previous theorem, we find that 3 is a quadratic residue modulo p if and only if p is of the form $12k \pm 1$, since the only odd quadratic residue modulo 3 is 1. For any odd prime $p \neq 3$, we have thus shown that

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{12}, \\ -1 & \text{if } p \equiv \pm 5 \pmod{12}. \end{cases}$$

Likewise, we can characterize the primes p for which 5 is a quadratic residue modulo p. Taking $q = 5$ in the previous theorem, we find that 5 is a quadratic residue modulo p if and only if p is of the form $20k \pm 1$ or $20k \pm 9$, since the two odd squares modulo 5 are 1^2 and 3^2. For any odd prime $p \neq 5$, we have thus shown that

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}. \end{cases}$$

28.3 Gauss's Lemma

While it is customary to consider the standard residue classes modulo an odd prime p to be the integers $0 \leq r < p$, we have now the occasion to consider the complete residue system of integers between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$.

DEFINITION 28.3.1. The *least absolute residue* of an integer a modulo a natural number n is the unique integer

$$-\frac{n}{2} < x \leq \frac{n}{2}$$

such that $x \equiv a \pmod{n}$. We will write $\lfloor a \rceil_n$ for the least absolute residue of a modulo n, and we will write $\lVert a \rVert_n$ for its absolute value.

Thus, the least absolute residue of an integer a modulo an odd prime p, which is what we will be using this concept for, is the unique integer

$$-\frac{p-1}{2} \leq x \leq \frac{p-1}{2}$$

such that $x \equiv a \pmod{p}$. For example, the least absolute residue of 4 modulo 7 is -3, the least absolute residue of 6 modulo 13 is 6, and the least absolute residue of 12 modulo 13 is -1. In the following table, we list the least absolute residues modulo 11:

a	0	1	2	3	4	5	6	7	8	9	10
$\lfloor a \rceil_{11}$	0	1	2	3	4	5	-5	-4	-3	-2	-1.

If we consider an integer a relatively prime to an odd prime p, then multiplication by a defines a bijection on $\mathbb{Z}/p\mathbb{Z}$. It follows that the function

$$x \mapsto \lfloor ax \rceil_p : \{0, \dots, p-1\} \to \{-\tfrac{p-1}{2}, \dots, \tfrac{p-1}{2}\}$$

is also a bijection. Restricting this bijection to the set $\{1, \dots, \frac{p-1}{2}\}$, we obtain an injective function

$$x \mapsto \lfloor ax \rceil_p : \{1, \dots, \tfrac{p-1}{2}\} \to \{-\tfrac{p-1}{2}, \dots, \tfrac{p-1}{2}\}.$$

The following lemma implies that every $1 \le x \le \frac{p-1}{2}$ occurs exactly once as the absolute value of any number of the form $\lfloor ax \rceil_p$. This holds whenever a is relatively prime to the modulus $m \ge 3$, as illustrated in Figure 28.3.

Lemma 28.3.2. *Consider a modulus $m \ge 3$ with $m' := \lfloor \frac{m-1}{2} \rfloor$, and let a be an integer. Then the map r_a given by $x \mapsto \llbracket ax \rrbracket_m$ defines a function*

$$r_a : \{1, \dots, m'\} \to \{1, \dots, m'\}.$$

Furthermore, this function r_a is a bijection if and only if a is relatively prime to m.

Proof. Suppose first that $\gcd(a, m) = 1$. For any $1 \le x \le m'$, we have $0 < 2x < m$, so that $m \nmid 2ax$. Consequently,

$$0 < \llbracket ax \rrbracket_m < \frac{m}{2},$$

showing that r_a takes values in the indicated set.

To prove injectivity, suppose that $r_a(x) = r_a(y)$. Then

$$ax \equiv \pm ay \pmod{m},$$

and hence $x \equiv \pm y \pmod{m}$. The negative sign is impossible because $0 < x + y < m$. Thus $x \equiv y \pmod{m}$, which implies $x = y$. Since the domain and codomain have the same finite size, r_a is a bijection.

Conversely, suppose that the formula defines a bijection. Since $m \ge 3$, its codomain contains 1, so there is an x such that $\llbracket ax \rrbracket_m = 1$. Therefore $ax \equiv \pm 1 \pmod{m}$, which implies $\gcd(a, m) = 1$. □

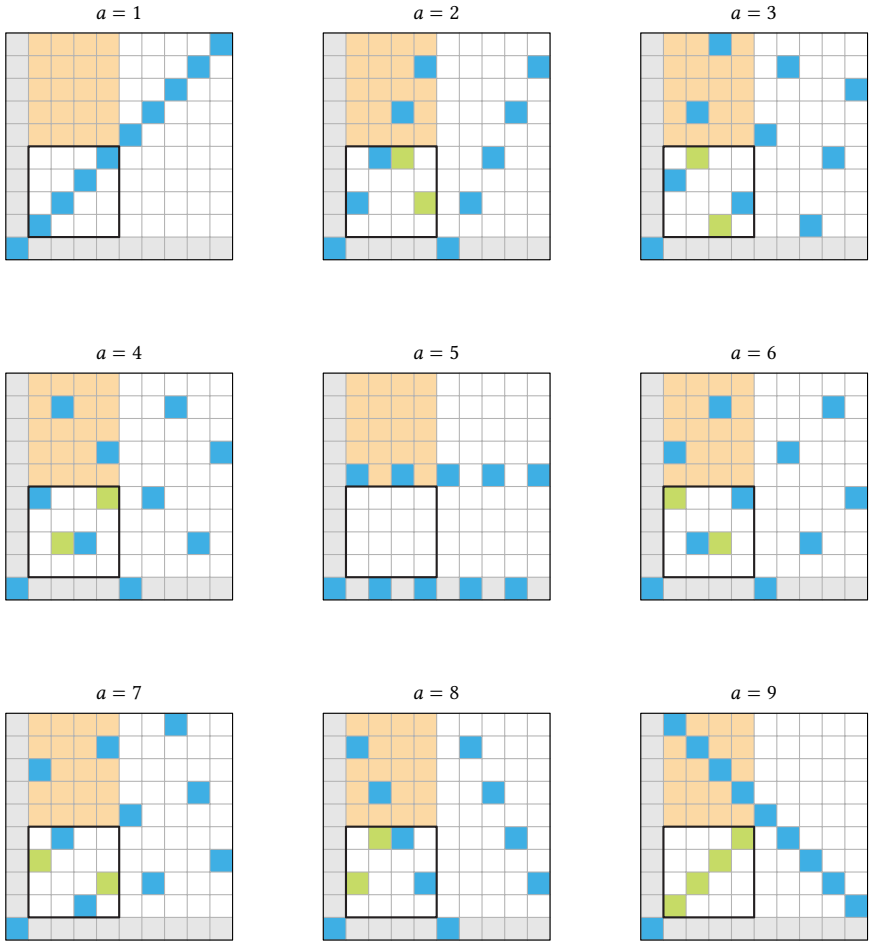


Figure 28.2: The least absolute residue function is a bijection on $\{1, \ldots, \lfloor (m-1)/2 \rfloor\}$ if and only if the multiplier a is relatively prime to m.

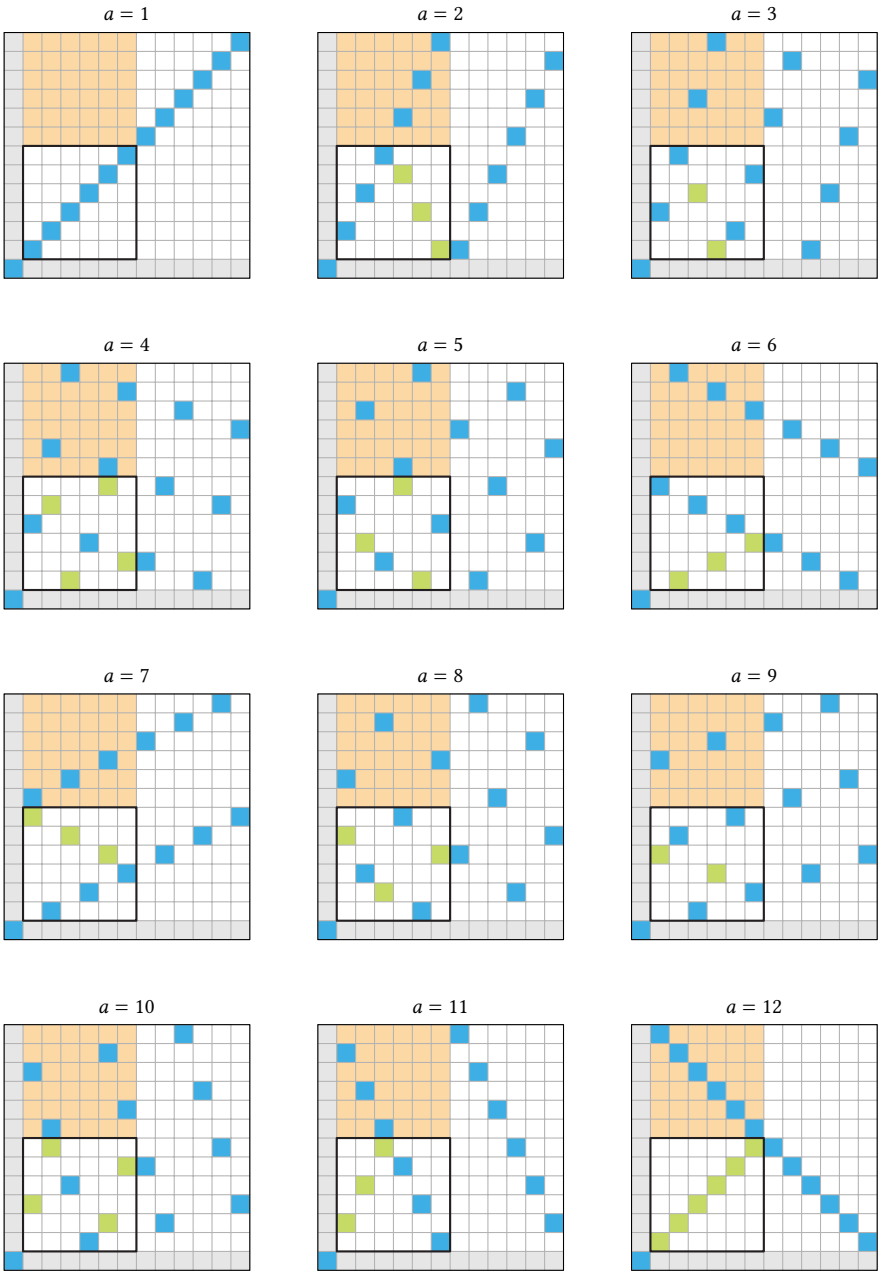


Figure 28.3: If p is an oodd prime, then the number of reflected residues of ax modulo p for $1 \leq x \leq \frac{p-1}{2}$ is even if and only if a is a quadratic residue.

LEMMA 28.3.3 (Gauss's Lemma). *Consider an odd prime p and an integer such that $p \nmid a$. Define μ to be the number of elements x among the residue classes*

$$a,\ 2a,\ 3a,\ \ldots,\ \tfrac{p-1}{2}a \pmod{p},$$

such that $\lfloor ax \rceil_p$ is negative. Then we have

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

PROOF. Write $P := (p-1)/2$. Then we have that $p \nmid P!$, so suffices to show that

$$\left(\frac{a}{p}\right) P! \equiv (-1)^{\mu} P! \pmod{p}.$$

By Theorem 27.4.1 (Euler's Criterion) we have $\left(\frac{a}{p}\right) \equiv a^P \pmod{p}$, so we obtain that

$$\left(\frac{a}{p}\right) P! \equiv a^P P! \pmod{p}.$$

Redistributing the P factors of a of the exponent a^P over $P!$, and using Lemma 28.3.3, we obtain:

$$a^P P! = (1a)(2a)\cdots(Pa) \equiv (-1)^{\mu} P! \pmod{p}. \qquad \square$$

28.4 Eisenstein's Proof of the Law of Quadratic Reciprocity

Gauss was the first to prove the law of quadratic reciprocity in 1796, when he was only 19 years old. This proof was included in his seminal work, *Disquisitiones Arithmeticae*, published in 1801. Gauss was very fond of this result, and throughout his life-time he would publish seven different proofs.

The proof we will present here is due to Gotthold Eisenstein, which he published in 1844. It is celebrated for its simplicity and for the insightful perspective it provides on geometric aspects of the quadratic reciprocity law.

In Eisenstein's proof of the law of quadratic reciprocity, we will make use of the *floor function* $x \mapsto \lfloor x \rfloor$, which is a function from the rational numbers or the real numbers, to the integers. The integer

$$\lfloor x \rfloor$$

is the largest integer below x. In other words, its defining property is that the floor function satisfies the logical equivalence

$$k \leq \lfloor x \rfloor \quad \Leftrightarrow \quad k \leq x$$

for every integer k and every rational or real number x. Concretely, we have the following examples:

$$\left\lfloor \frac{3}{2} \right\rfloor = 1, \qquad \left\lfloor \frac{29}{31} \right\rfloor = 0, \qquad \text{and} \qquad \left\lfloor -\frac{1}{4} \right\rfloor = -1.$$

Eisenstein's proof of Theorem 28.2.1 (The Law of Quadratic Reciprocity). By Lemma 28.3.3 (Gauss's Lemma) it suffices to show that

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

In other words, we have to show that

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

This suggests that there should be a way of splitting a set of $\frac{p-1}{2}\frac{q-1}{2}$ points into two subsets S and T, so that their respective number of elements have the same parities as the quantities $\mu(q,p)$ and $\mu(p,q)$. There is indeed such a way. Figure 28.4 shows Eisenstein's setup in case of the primes $p = 17$ and $q = 13$.

Consider the set of $\frac{p-1}{2}$ by $\frac{q-1}{2}$ lattice points in the positive quadrant of the plane; that is, the points with positive integer coordinates within the rectangle spanned by the four points

$$\left(0,0\right),\ \left(\tfrac{p}{2},0\right),\ \left(\tfrac{p}{2},\tfrac{q}{2}\right),\ \text{and}\ \left(0,\tfrac{q}{2}\right).$$

We partition these lattice points by the diagonal of the rectangle: The set of lattice points below the diagonal is S, and the set of lattice points above the diagonal is T. Since the diagonal of this rectangle is given by the line $y = \frac{q}{p}x$, there is no point with positive integer coordinates on the diagonal, so there is no ambiguity as to which part a lattice point belongs to.

Now observe that the number $|S|$ of lattice points in the set S is given by

$$|S| = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor.$$

This formula is obtained by first recognizing that for each $1 \le k \le \frac{p-1}{2}$, a lattice point of the form (k,i) is in the set S if and only if

$$1 \le i \le \frac{q}{p}k.$$

The number of such lattice points is $\lfloor \frac{kq}{p} \rfloor$, so the total number of elements in S is obtained by summing up all of these totals. Similarly, the number $|T|$ of lattice points in the set T is given by

$$|T| = \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$



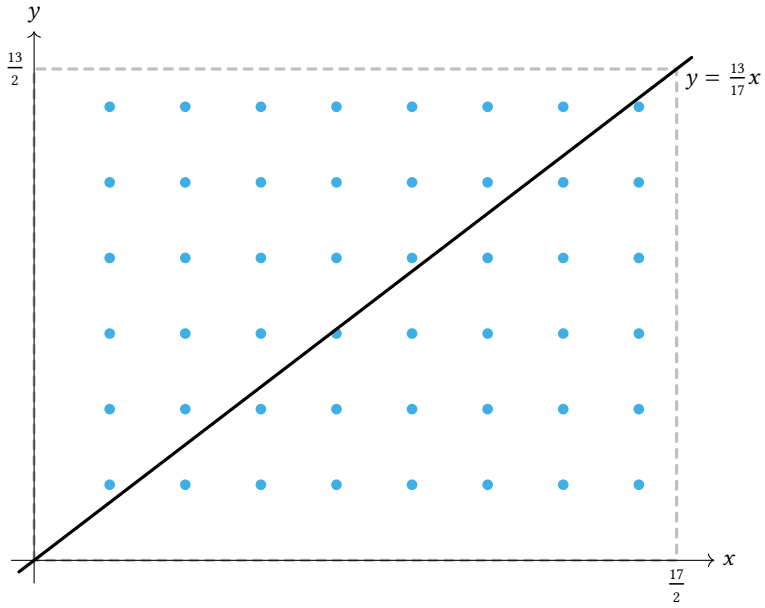


Figure 28.4: In Eisenstein's proof of quadratic reciprocity, we count the $\frac{p-1}{2}$ by $\frac{q-1}{2}$ lattice points in the marked rectangle as the sum of the number lattice points below the diagonal and the number of lattice points above the diagonal.

Thus, it remains to prove that

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \equiv \mu(q,p) \pmod 2 \quad \text{and} \quad \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor \equiv \mu(p,q) \pmod 2.$$

We will verify these congruences separately in the following lemma. □

LEMMA 28.4.1. *Consider an odd prime p and an odd integer a not divisible by p, and let $\mu(a,p)$ be the quantity defined in Lemma 28.3.3 (Gauss's Lemma). Then*

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor \equiv \mu(a,p) \pmod 2.$$

PROOF. For each k there are unique integers q_k and r_k such that $ka = q_k p + r_k$, where

$$-\frac{p-1}{2} \le r_k \le \frac{p-1}{2}.$$

It follows that

$$\left\lfloor \frac{ka}{p} \right\rfloor = \begin{cases} q_k & \text{if } r_k > 0 \\ q_k - 1 & \text{if } r_k < 0. \end{cases}$$

Adding up the integers $\lfloor \frac{ka}{p} \rfloor$ therefore amounts to adding up the integers q_k and subtracting the number of integers k such that r_k is negative:

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor = \sum_{k=1}^{\frac{p-1}{2}} q_k - \mu(a,p).$$

To complete the proof, it therefore suffices to show that

$$\sum_{k=1}^{\frac{p-1}{2}} q_k \equiv 0 \pmod 2.$$

To prove this, recall from Lemma 28.3.2 that the map $k \mapsto |r_k|$ is a permutation of the set $\{1, \dots, \frac{p-1}{2}\}$. In other words, every integer from 1 to $\frac{p-1}{2}$ occurs exactly once as an integer of the form $|r_k|$. Since the parity of an integer is unchanged by taking its absolute value, we have

$$\sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} |r_k| \equiv \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2.$$

On the other hand, observe that since a and p are assumed to be odd, we have the congruences

$$k \equiv ka = q_k p + r_k \equiv q_k + r_k \pmod 2.$$

Thus we obtain the congruences

$$\sum_{k=1}^{\frac{p-1}{2}} k \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} r_k \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k + \sum_{k=1}^{\frac{p-1}{2}} k \pmod 2.$$

Subtracting $\sum_k k$ from both sides, we find that $\sum_k q_k \equiv 0 \pmod 2$. □

Exercises

Starter Exercises

28.1 Compute the values of the following Legendre symbols:

$$\left(\frac{101}{163}\right), \quad \left(\frac{137}{359}\right), \quad \left(\frac{113}{479}\right), \quad \text{and} \quad \left(\frac{139}{953}\right).$$

28.2 Compute the values of the following Legendre symbols:

$$\left(\frac{113}{131}\right), \quad \left(\frac{131}{311}\right), \quad \text{and} \quad \left(\frac{311}{113}\right).$$

28.3 Compute the values of the following Legendre symbols:

$$\left(\frac{199}{919}\right), \quad \left(\frac{919}{991}\right), \quad \text{and} \quad \left(\frac{991}{199}\right).$$

28.4 Compute the values of the following Legendre symbols:

$$\left(\frac{337}{373}\right), \quad \left(\frac{373}{733}\right), \quad \text{and} \quad \left(\frac{733}{337}\right).$$

28.5 Show that the system of congruences

$$\begin{aligned} x - y &\equiv 1 \pmod{p}, \\ xy &\equiv 1 \pmod{p} \end{aligned}$$

has a solution if and only if $p \equiv \pm 1 \pmod{10}$.

Routine-Building Exercises

28.6 Consider a prime $p > 3$. Show that

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 5 \pmod{24}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11 \pmod{24}. \end{cases}$$

28.7 Consider an odd prime $p \neq 5$. Show that

$$\left(\frac{10}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}, \\ -1 & \text{if } p \equiv \pm 7, \pm 11, \pm 17, \pm 19 \pmod{40}. \end{cases}$$

28.8 Determine whether the following quadratic congruences have solutions:

(a) $x^2 + x + 1 \equiv 0 \pmod{13}$.
(b) $x^2 + x + 3 \equiv 0 \pmod{7}$.
(c) $2x^2 + 3x + 5 \equiv 0 \pmod{17}$.
(d) $x^2 + 4x + 8 \equiv 0 \pmod{23}$.

(e) $2x^2 + 3x + 4 \equiv 0 \pmod{11}$.
(f) $4x^2 + 7x + 14 \equiv 0 \pmod{31}$.

28.9 Show that 2 is a quadratic residue modulo any prime divisor of the nth Fermat number $F_n = 2^{2^n} + 1$, for $n \geq 2$.

28.10 Consider a prime p such that $q := 2p + 1$ and $r := 2(2p + 1) + 1 = 4p + 3$ are both prime. Prove that

$$\operatorname{ord}_r(2) = q.$$

Challenge Exercises

28.11 Show that if the nth Fermat number $F_n = 2^{2^n} + 1$ is prime, then 3 is a primitive root modulo F_n.

28.12 Consider an odd prime p. Show that the following are equivalent:

(i) The Mersenne number $M_p = 2^p - 1$ has a common prime divisor with $2p + 1$.

(ii) The prime p is a *Sophie Germain prime*, meaning that the number $2p + 1$ is prime, and furthermore $p \equiv 3 \pmod{4}$.

Conclude that

$$M_{11}, M_{23}, M_{83}, M_{131}, M_{179}, \text{ and } M_{191}$$

are all composite.

28.13 (a) Show that for any prime $p \equiv 3 \pmod{4}$ greater than 3, there exists a prime $q < p$ such that p is a quadratic nonresidue modulo q.
(b) Show that for any prime $p \equiv 1 \pmod{4}$, there exists a prime $q < p$ such that p is a quadratic nonresidue modulo q. Hint: First show that there exists a quadratic nonresidue $0 < a < p$ such that $a \equiv 1 \pmod{4}$.

28.14 (a) For any integer $a > 2$, let p be a prime factor of $a^4 - a^2 + 1$. Show that

$$\operatorname{ord}_p(a) = 12.$$

(b) Use a suitable choice of a in

$$N_a := a^6 + 1$$

to show that there are infinitely many primes congruent to 1 modulo 12.
(c) For each r in the set $\{5, 7, 11\}$, show that there are infinitely many primes congruent to r modulo 12.



Chapter 29

Primality Testing

29.1 Pépin's Primality Test for the Fermat Numbers

Édouard Lucas observed that the quadratic character of -1 can be used to reach a sharper conclusion on the congruence class of a prime dividing a Fermat number.

Theorem 29.1.1 (Lucas's refinement of Theorem 16.1.4). *Consider a prime divisor $p = k2^{n+1} + 1$ of the nth Fermat number F_n, where $n \geq 2$. Then k is even and*

$$\operatorname{ord}_p(k) = \operatorname{ord}_p(2^{n+1}) = 2^{n+1-\nu_2(n+1)}.$$

Consequently, we have $p \equiv 1 \pmod{2^{n+2}}$.

Théophile Pépin used the theory of quadratic residues to develop a deterministic primality test for Fermat primes.

Theorem 29.1.2 (Pépin's Primality Test). *For $n \geq 1$, the nth Fermat number F_n is prime if and only if*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}.$$

29.2 The Carmichael Numbers

Theorem 16.1.1 (Fermat's Little Theorem) asserts that if p is a prime number, then the congruence

$$x^p \equiv x \pmod{p}$$

holds for every integer x. Thus it is natural to wonder whether Fermat's Little Theorem can be used to test whether a number is prime. If we can find an integer x such that

$$x^n \not\equiv x \pmod{n}$$

then it is certain that n must be composite. This is a very useful test, since it provides a way to establish that the number n is composite without factoring it, and for many composite numbers it is indeed possible to find an integer x such that $x^n \not\equiv x \pmod{n}$.

However, if no such integer x exists, this simple test does not provide a guarantee for the primality of n. Robert Carmichael discovered that there are composite numbers that satisfy Fermat's congruence for every integer [CAR1912].

DEFINITION 29.2.1. A *Carmichael number* is a composite integer $n > 1$ such that the congruence

$$x^n \equiv x \pmod{n}$$

holds for every integer x.

Alternatively, we can define a Carmichael number to be a composite number n such that

$$n \mid x^n - x.$$

Thus, a Carmichael number is a composite number n dividing the fixed divisor of the polynomial x^n. In order to find examples of Carmichael numbers, it is therefore useful to first compute the fixed divisor of this polynomial.

Recall from Definition 20.5.1 that the fixed divisor of a polynomial $f(x)$ is the greatest common divisor of all the values of $f(x)$. In §20.5 we showed that the fixed divisor of $f(x) = x^n - x$ can be determined by computing the greatest common divisor of the values

$$f(2), \ldots, f(\lfloor \tfrac{n+1}{2} \rfloor).$$

While this theorem is useful to compute the fixed divisor of any specific polynomial, such as $x^7 - x$, we shall compute the fixed divisor of $x^n - x$ using Theorem 16.1.1 (Fermat's Little Theorem) and Theorem 20.3.2 (Lagrange's Theorem).

THEOREM 29.2.2. *Consider the polynomial $x^n - x$, for some natural number $n > 1$. Its fixed divisor is the square-free number*

$$\prod_{\substack{p \text{ prime} \\ p-1 \mid n-1}} p.$$

PROOF. First, we claim that a prime number p appears as a factor of the fixed divisor of $x^n - x$ if and only if

$$p - 1 \mid n - 1.$$

For the forward direction of this claim, suppose that p divides every integer of the form $x^n - x$ and write $n - 1 = k(p-1) + r$ where $0 \leq r < p - 1$. Since $x^n - x = x(x^{n-1} - 1)$ and p is prime, it follows from Theorem 16.1.1 (Fermat's Little Theorem) that

$$x^r - 1 \equiv x^{k(p-1)+r} - 1 \equiv x^{n-1} - 1 \equiv 0 \pmod{p},$$

when x is not divisible by p. However, Theorem 20.3.2 (Lagrange's Theorem) tells us that the polynomial $x^r - 1$ has at most $r < p-1$ roots modulo p when $r \neq 0$. Therefore we conclude that $r = 0$; that is, $p - 1 \mid n - 1$.

Conversely, if $p - 1 \mid n - 1$, then it follows by Fermat's Little Theorem that

$$x^{n-1} \equiv 1 \pmod{p}$$

for every x not divisible by p. This implies that $x(x^{n-1} - 1)$ is divisible by p for every x, completing the proof of the first claim.

To finish the proof, it remains to show that the fixed divisor of $x^n - x$ is square-free, i.e., that for each prime number p there is an integer x such that $p^2 \nmid x^n - x$. We choose $x = p$, because the integer $p^n - p = p(p^{n-1} - 1)$ is indeed not divisible by p^2. □

Theorem 29.2.2 can be used to obtain a characterization of the Carmichael numbers due to Alwin Korselt [Kor1899]. Since n is a Carmichael number if and only if n divides the fixed divisor of $x^n - x$, we see that such n must be square-free and for each of its prime divisors p we must have $p - 1 \mid n - 1$. Thus, we obtain:

Theorem 29.2.3 (Korselt's criterion). *A composite number $n > 1$ is a Carmichael number if and only if the following two conditions hold:*

(i) *The number n is squarefree.*

(ii) *For any prime divisor p of n, we have $p - 1 \mid n - 1$.*

In order to narrow our search for examples of Carmichael numbers further, we show that there are no Carmichael numbers of the form pq, and that they are always odd.

Theorem 29.2.4. *Any Carmichael number is an odd number with at least three prime factors.*

Proof. First, suppose n is an even Carmichael number. Since n is composite and square-free, there must exists an odd prime p dividing n. For such a prime p we have

$$p - 1 \mid n - 1.$$

However, $p - 1$ is even while $n - 1$ is odd, which is a contradiction. Any Carmichael number must therefore be odd.

Now consider a number $n = pq$ where p and q are distinct primes. In order for n to be a Carmichael number, we must have

$$p - 1 \mid pq - 1 \qquad \text{and} \qquad q - 1 \mid pq - 1.$$

By writing $pq - 1 = (p - 1)q + (q - 1)$ we see that

$$p - 1 \mid pq - 1 \quad \Leftrightarrow \quad p - 1 \mid q - 1$$

and we get a similar logical equivalence when we reverse the roles of p and q. This shows that $p = q$, contradicting the assumption that p and q are distinct. □



A trick similar to the factorization trick we used to rule out two-prime Carmichael numbers can be used to obtain some useful congruences involving the prime factors of a three-prime Carmichael number.

PROPOSITION 29.2.5. *Any three-prime Carmichael number $n = pqr$ satisfies the congruences*

$$\begin{aligned} qr &\equiv 1 \pmod{p-1} \\ pr &\equiv 1 \pmod{q-1} \\ pq &\equiv 1 \pmod{r-1}. \end{aligned}$$

PROOF. Since the three congruences are symmetric in p, q, and r, it suffices to show prove the first congruence. By writing $pqr - 1 = (p-1)qr + qr - 1$ we see that

$$p - 1 \mid pqr - 1 \quad \Leftrightarrow \quad p - 1 \mid qr - 1,$$

from which it follows that if $n = pqr$ is a Carmichael number then $qr \equiv 1 \pmod{p-1}$. □

We have now gathered enough information about three-prime Carmichael numbers to start hunting for small examples. In the following theorem we will show that there is exactly one three-prime Carmichael number divisible by 3. Similar techniques can be used to find the finitely many three-prime Carmichael numbers whose smallest prime divisor is a fixed small prime p such as $p = 5$ or $p = 7$.

THEOREM 29.2.6. *There is exactly one Carmichael number of the form $3qr$ with $3 < q < r$ prime, namely*

$$561 = 3 \cdot 11 \cdot 17.$$

PROOF. Suppose that the number $3qr$ is a Carmichael number. Then the congruences

$$\begin{aligned} qr &\equiv 1 \pmod{2} \\ 3r &\equiv 1 \pmod{q-1} \\ 3q &\equiv 1 \pmod{r-1} \end{aligned}$$

hold. The first one simply says that q and r are both odd, which we already knew. The second congruence says that 3 is invertible modulo $q - 1$. This implies that $q \equiv 0$ or $2 \pmod{3}$. However, since q is assumed to be a prime larger than 3 it follows that $q \equiv 2 \pmod{3}$.

Using that $q = 3u + 2$ with $0 < u$ we see that the congruences $3r \equiv 1 \pmod{q-1}$ and $3q \equiv 1 \pmod{r-1}$ can be stated equivalently as the congruences

$$\begin{aligned} r &\equiv 2u + 1 \pmod{3u+1} \\ 9u + 5 &\equiv 0 \pmod{r-1}. \end{aligned}$$

From the first of these congruences we see that $r = k(3u+1) + (2u+1)$, where we may note that $k \neq 0$ since $q < r$. However, the second congruence now gives us that $r \leq 9u + 6$. This inequality can be used to further restrict the possible values of the integer k:

$$k(3u+1) + (2u+1) \leq 9u + 6 \quad \Rightarrow \quad k \leq \frac{7u+5}{3u+1} \leq 3.$$

There are thus three options for k:

(i) If $k = 3$ then we must have $q = 5$ and $r = 15$. However, 15 is composite, so we conclude that $k \neq 3$.

(ii) If $k = 2$ then $r - 1 = 8u + 2$. However, no number of the form $8u + 2$ divides a number of the form $9u + 5$, so we conclude that $k \neq 2$.

(iii) The only remaining case is where $k = 1$ and $r - 1 = 5u + 1$. The divisibility relation

$$5u + 1 \mid 9u + 5$$

implies that $0 < u \leq 3$. Since

$$5 \cdot 1 + 1 \nmid 9 \cdot 1 + 5, \qquad 5 \cdot 2 + 1 \nmid 9 \cdot 2 + 5, \qquad \text{and} \qquad 5 \cdot 3 + 1 \mid 9 \cdot 3 + 5$$

we find that $u = 3$, and therefore $q = 11$ and $r = 17$. □

In 1994, William Robert Alford, Andrew Granville, and Carl Pomerance made extensive use of Korselt's criterion to show that there are infinitely many Carmichael numbers [AGP1994]. Thomas Wright showed in 2013 that there are infinitely many Carmichael numbers in any arithmetic progression $ax+b$ with a and b relatively prime [Wri2013].

29.3 The Lucas–Lehmer Primality Test

This test is named after Édouard Lucas and Derrick Henry Lehmer, who refined Lucas's ideas in the 1930s.

29.4 Pocklington's Criteria

Theorem 29.4.1 (Pocklington's Theorem). *Consider a number $n > 1$, and suppose there exist a positive integer a and a prime number p such that*

(i) $a^{n-1} \equiv 1 \pmod{n}$,

(ii) $p \mid n - 1$ *and* $p > \sqrt{n} - 1$,

(iii) $\gcd\left(a^{(n-1)/p} - 1, n\right) = 1$.

Then the number n is prime.



PROOF. Assume to the contrary that n is composite, and let q be a prime factor of n such that $q \leq \sqrt{n}$. Then we have

$$q - 1 \leq \sqrt{n} - 1 < p,$$

showing that $q - 1$ and p are relatively prime. Thus, it follows that there is an integer u such that $pu \equiv 1 \pmod{q-1}$. Now we get the following congruences modulo q:

$$\begin{aligned} a^{(n-1)/p} &\equiv a^{pu(n-1)/p} \\ &\equiv a^{u(n-1)} \\ &\equiv (a^{n-1})^u \\ &\equiv 1. \end{aligned}$$

The last congruence holds since $q \mid n$ and the assumption that $a^{n-1} \equiv 1 \pmod{n}$. Thus, it follows that q is a divisor of both $a^{(n-1)/p} - 1$ and n, which contradicts the assumption that they are relatively prime. □

EXAMPLE 29.4.2. In order to illustrate the Pocklington-Lehmer test, we will show that the number

$$11! + 1 = 39,916,801$$

is prime. Primes of the form $n! \pm 1$ are called *factorial primes*. The largest known example is $632,760! - 1$.

Given that $n := 11! + 1$, we have that

$$n - 1 = 11! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11.$$

29.5 Mersenne Primes

DEFINITION 29.5.1. The *Mersenne numbers* are the numbers of the form $M_n := 2^n - 1$. *Mersenne primes* are Mersenne numbers that are prime.

PROPOSITION 29.5.2. *If M_n is a Mersenne prime, then n is prime.*

LEMMA 29.5.3. *The congruence*

$$2^{M_p} \equiv 2 \pmod{M_p}.$$

holds for any prime number p.

PROOF. First observe that by the definition $M_n = 2^n - 1$, it follows that $\operatorname{ord}_{M_n}(2) = n$. This implies that

$$2^k \equiv 2^l \pmod{M_n}$$

if and only if $k \equiv l \pmod{n}$.

By Fermat's Little Theorem we have that $2^p \equiv 2 \pmod{p}$, so that $M_p \equiv 1 \pmod{p}$. Thus we obtain that

$$2^{M_p} \equiv 2^1 \pmod{M_p}.$$ □

Proposition 29.5.4. *The Mersenne number $M_{31} = 2,147,483,647$ is prime.*

Proof. We set $a := 2$ and $n := M_{31}$ so that $n - 1 = 2(2^{30} - 1)$. First, note that since 31 is prime, it follows from Lemma 29.5.3 that

$$2^{n-1} \equiv 1 \pmod{n}.$$

Thus, the first condition in the Pocklington–Lehmer primality test is satisfied.

First, we factor the number $M_{31} - 1 = 2^{31} - 2$, which is $2(2^{30} - 1)$. We do so by the following calculation:

$$\begin{aligned} 2^{30} - 1 &= (2^{15} - 1)(2^{15} + 1) \\ &= (2^5 - 1)(2^{10} + 2^5 + 1)(2^5 + 1)(2^{10} - 2^5 + 1) \\ &= 31 \cdot 1057 \cdot 33 \cdot 993 \\ &= 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331. \end{aligned}$$

The number $151 \cdot 331$ is strictly larger than $\sqrt{M_{31}}$, so it will be suitable for the Pocklington Lehmer test. □



Exercises

Routine-Building Exercises

29.1 Use Pocklington's criterion to show that the following numbers are prime:

(a) $13,421 = 11^4 - 11^3 + 11^2 - 11 + 1$,
(b) $28,393 = 13^4 - 13^2 + 1$,
(c) $2,311,921 = 39^4 - 39^2 + 1$.

Hints: $13,421$ divides $11^{10} - 1$, $28,393$ divides $13^{12} - 1$, and $2,311,921$ divides $39^{12} - 1$.

29.2 Prove that the following are equivalent:

(i) $2^{M_n} \equiv 2 \pmod{M_n}$.
(ii) $2^{n-1} \equiv 1 \pmod{n}$.

29.3 Show that for every integer n there is an integer x such that $\lambda(n)/2$ is the least positive integer k for which the congruence

$$x^k \equiv -1 \pmod{n}$$

is solvable.

29.4 Show that the only Carmichael numbers of the form $5qr$ are

$$1105 = 5 \cdot 13 \cdot 17, \qquad 2464 = 5 \cdot 17 \cdot 29, \qquad \text{and} \qquad 10585 = 5 \cdot 29 \cdot 73.$$

29.5 Show that any Carmichael number n is relatively prime to the value $\phi(n)$ of Euler's totient function. Numbers with this property are called *cyclic*.

References

[AGP1994] William Robert Alford, Andrew Granville, and Carl Pomerance. *There are infinitely many Carmichael numbers*. In: Annals of Mathematics. 2nd Ser. 139.3 (1994), pp. 703–722. doi: 10.2307/2118576.

[Car1912] Robert D. Carmichael. *On Composite Numbers P Which Satisfy the Fermat Congruence* $a^{P-1} \equiv 1 \pmod{P}$. In: The American Mathematical Monthly 19.2 (1912), pp. 22–27. doi: 10.2307/2972687.

[Kor1899] Alwin Korselt. *Problème Chinois*. French. In: L'Intermédiaire des Mathématiciens 6 (1899), pp. 142–143.

[Leg1798] Adrien-Marie Legendre. *Essai sur la théorie des nombres*. Paris: Duprat, 1798. url: https://openlibrary.org/books/OL24146260M/Essai_sur_la_th%C3%A9orie_des_nombres.

[Sie1988] Wacław Sierpiński. *Elementary Theory of Numbers*. Ed. by A. Schinzel. 2nd English Edition. Amsterdam: North-Holland, 1988. isbn: 9780444866622.

[Sti1884] Thomas Joannes Stieltjes. *Sur le caractère du nombre 2 comme résidu ou non-résidu quadratique*. In: Bulletin des Sciences Mathématiques et Astronomiques. 2nd ser. 8.1 (1884), pp. 175–176. url: https://www.numdam.org/item/BSMA_1884_2_8_1_175_1/.

[Wri2013] Thomas Wright. *Infinitely many Carmichael numbers in arithmetic progressions*. In: Bulletin of the London Mathematical Society 45.5 (2013), pp. 943–952. doi: 10.1112/blms/bdt013.