Chapter 8

Quadratic residues

8.1. Squares modulo prime p

Exercise 8.1.1. (a) Prove that 337 is not a square (that is, the square of an integer) by reducing it mod 5.
(b) Prove that 391 is not a square by reducing it mod 7.
(c) Prove that there do not exist integers x and y for which $x^2 - 3y^2 = -1$, by reducing any solution mod 3.

Exercise 8.1.2. (a) Prove that if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
(b) Prove that $\sum_{a=0}^{p-1} \left(\frac{a}{p}\right) = 0$.

Exercise 8.1.3. Suppose that prime p does not divide ab.
(a) Prove that $\left(\frac{a/b}{p}\right) = \left(\frac{ab}{p}\right)$.
(b) Prove that there are non-zero residues x and $y \pmod{p}$ for which $ax^2 + by^2 \equiv 0 \pmod{p}$ if and only if $\left(\frac{-ab}{p}\right) = 1$.

Exercise 8.1.4. Prove that if odd prime p divides $b^2 - 4ac$ but neither a nor c, then $\left(\frac{a}{p}\right) = \left(\frac{c}{p}\right)$.

Exercise 8.1.5. Let p be a prime > 3. Prove that if there is no residue $x \pmod{p}$ for which $x^2 \equiv 2 \pmod{p}$, and no residue $y \pmod{p}$ for which $y^2 \equiv 3 \pmod{p}$, then *there is* a residue $z \pmod{p}$ for which $z^2 \equiv 6 \pmod{p}$.

Exercise 8.1.6. One can write each non-zero residue mod p as a power of a primitive root g.
(a) Prove that the quadratic residues are precisely those residues that are an even power of g, and the quadratic non-residues are those that are an odd power.
(b) Deduce that $\left(\frac{g}{p}\right) = -1$.

Exercise 8.1.7. (a) Show that if n is odd and p divides $a^n - 1$, then $\left(\frac{a}{p}\right) = 1$.
(b) Show that if n is prime and p divides $a^n - 1$, but $a \not\equiv 1 \pmod{p}$, then $p \equiv 1 \pmod{n}$.
(c) Give an example to show that (b) can be false if we only assume that n is odd.

Exercise 8.1.8. (a) Prove that, for every prime $p \neq 2, 5$, at least one of 2, 5, and 10 is a quadratic residue mod p.
(b)† Prove that, for every prime $p > 5$, there are two consecutive positive integers that are both quadratic residues mod p and are both ≤ 10.

8.2. The quadratic character of a residue

Exercise 8.2.1.† Prove Euler's criterion for $(a/p) = 1$, by evaluating $(p-1)!$ (mod p) as in the second part of proof #1, but now taking account of the solutions r (mod p) to $r^2 \equiv a$ (mod p).

Exercise 8.2.2. Let p be an odd prime. Explain how one can determine the integer $\left(\frac{a}{p}\right)$ by knowing $a^{\frac{p-1}{2}}$ (mod p). (Euler's criterion gives a congruence, but here we are asking for the value of the integer $\left(\frac{a}{p}\right)$.)

Exercise 8.2.3. Use Euler's criterion to reprove Theorem 8.1.

Exercise 8.2.4. Let p be a prime $\equiv 3$ (mod 4). Show that if $\left(\frac{a}{p}\right) = 1$ and $b \equiv a^{\frac{p+1}{4}}$ (mod p), then $b^2 \equiv a$ (mod p). (This idea is explored further in section 7.21 of appendix 7C.)

8.3. The residue -1

Exercise 8.3.1. Let p be a prime $\equiv 3$ (mod 4), which does not divide integer a. Prove that either there exists x (mod p) for which $x^2 \equiv a$ (mod p) or there exists y (mod p) for which $y^2 \equiv -a$ (mod p), but not both.

Exercise 8.3.2. (a) Prove that every prime factor p of $4n^2+1$ satisfies $p \equiv 1$ (mod 4).
(b) Deduce that there are infinitely many primes $\equiv 1$ (mod 4).

8.4. The residue 2

Exercise 8.4.1. For any odd integer q, let r denote the number of positive odd integers $\leq \frac{q-1}{2}$. Prove that r is even if $q \equiv \pm 1$ (mod 8), while r is odd if $q \equiv \pm 3$ (mod 8).

Exercise 8.4.2. Prove that if p is an odd prime, then

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

Exercise 8.4.3. Prove that if 2 is a primitive root mod p, then $p \equiv 3$ or 5 (mod 8).

Exercise 8.4.4.† (a) Prove that if prime $p|M_n := 2^n - 1$ where $n > 2$ is prime, then $p \equiv 1$ (mod n) and $p \equiv \pm 1$ (mod 8).
(b) Prove that if $p = 2n+1$ is prime, then $p|2^n - 1$ if and only if $p \equiv \pm 1$ (mod 8).
(c) Prove that if $p = 2n+1$ is prime, then $p|2^n + 1$ if and only if $p \equiv \pm 3$ (mod 8).
(d) Prove that if q and $p = 2q+1$ are both prime, then p divides $2^q - 1$ if and only if $q \equiv 3$ (mod 4).
(e) Factor $2^{11} - 1 = 2047$.

Exercise 8.4.5.† In exercise 7.3.2 we proved that if prime p divides $2^{2^k} + 1$, then $p \equiv 1$ (mod 2^{k+1}). Now show that $p \equiv 1$ (mod 2^{k+2}) if $k \geq 2$.

8.5. The law of quadratic reciprocity

Exercise 8.5.1. Determine (a) $\left(\frac{13}{31}\right)$; (b) $\left(\frac{323}{31}\right)$; (c) $\left(\frac{377}{233}\right)$; (d) $\left(\frac{13}{71}\right)$; (e) $\left(\frac{-104}{131}\right)$.

Exercise 8.5.2. (a) Show that if prime $p \equiv 1$ (mod 5), then 5 is a quadratic residue mod p.
(b) Show that if prime $p \equiv 3$ (mod 5), then 5 is a quadratic non-residue mod p.
(c) Determine all odd primes p for which $(5/p) = -1$.

Exercise 8.5.3. Prove that if $p := 2^n - 1$ is prime with $n > 2$, then $(3/p) = -1$.

Exercise 8.5.4.† Suppose that $F_m = 2^{2^m} + 1$ with $m \geq 2$ is prime. Prove that $3^{\frac{F_m-1}{2}} \equiv 5^{\frac{F_m-1}{2}} \equiv -1$ (mod F_m).

Exercise 8.5.5.† (a) Determine all odd primes p for which $(7/p) = 1$.
(b) Find all primes p such that there exists $x \pmod p$ for which $2x^2 - 2x - 3 \equiv 0 \pmod p$.

Exercise 8.5.6. Show that if p and $q = p + 2$ are "twin primes", then p is a quadratic residue mod q if and only if q is a quadratic residue mod p.

Exercise 8.5.7. Prove that $(-3/p) = (p/3)$ for all primes p.

8.6. Proof of the law of quadratic reciprocity

8.7. *The Jacobi symbol*

Exercise 8.7.1. Suppose that m is an odd positive integer.
(a) Prove that $\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$ whenever $a \equiv b \pmod m$.
(b) Prove that $\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right)$.
(c) Prove that if $\left(\frac{a}{m}\right) = -1$, then a is not a square mod m.
(d) Prove that $\left(\frac{a}{m}\right) = 0$ if and only if $(a, m) > 1$.

Exercise 8.7.2. (a) Prove that $\sum_{a=0}^{m-1}\left(\frac{a}{m}\right) = 0$ for every non-square odd integer $m \geq 2$.
(b) For how many residues a mod m do we have $(a/m) = 1$?
(c) For how many residues a mod m do we have $(a/m) = -1$?

Exercise 8.7.3. Show that if $n \geq 1$, then $\left(\frac{n}{4n-1}\right) = 1$.

Exercise 8.7.4. Determine (a) $\left(\frac{13}{27}\right)$; (b) $\left(\frac{323}{225}\right)$; (c) $\left(\frac{233}{377}\right)$; (d) $\left(\frac{-104}{135}\right)$.

Exercise 8.7.5. Prove that $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod 2$ for any odd integers a, b.

Exercise 8.7.6. Prove an analogous induction step for integers $n \equiv 5$ or $7 \pmod 8$ when establishing the value of $\left(\frac{-2}{n}\right)$.

Exercise 8.7.7 (A useful reformulation of the law of quadratic reciprocity)**.** For a given odd, squarefree integer $n > 1$ let $n^* = \left(\frac{-1}{n}\right) n$. Prove that $n^* \equiv 1 \pmod 4$ and that we have $\left(\frac{m}{n}\right) = \left(\frac{n^*}{m}\right)$ for all odd integers $m > 1$.

8.8. *The squares modulo* m

Exercise 8.8.1. Deduce that an integer r is a quadratic residue mod p^k if and only if r is a quadratic residue mod p, when p is odd, and if and only if $r \equiv 1 \pmod{\gcd(2^k, 8)}$ when $p = 2$.

Exercise 8.8.2. Suppose that $(a, n) = 1$ and that $b^2 \equiv a \pmod n$. Prove that the set of solutions $x \pmod n$ to $x^2 \equiv a \pmod n$ is given by the values $br \pmod n$ as r runs through the solutions to $r^2 \equiv 1 \pmod n$. (Determining the square roots of $1 \pmod n$ is discussed in section 3.8.)

Additional exercises

Exercise 8.9.1. Let p be an odd prime where $p \nmid a$. Show that the congruence $ax^2 + bx + c \equiv 0 \pmod p$ has a solution $x \pmod p$ if and only if $b^2 - 4ac$ is a square mod p.

Exercise 8.9.2.† Prove that m^2 and $m^2 + 1$ are both squares mod p, for m equal to at least one of a, $a + 1$, or $a^2 + a + 1$, for any integer a. (This generalizes exercise 8.1.8(a).)

Exercise 8.9.3. The polynomial $x^4 - 4x^2 + 1$ is irreducible over $\mathbb{Q}[x]$ by Theorem 3.4.
(a) Prove that x^4-4x^2+1 can be factored mod p as $(x^2-\alpha)(x^2-\beta)$ or $(x^2-ax+1)(x^2+ax+1)$ or $(x^2-ax-1)(x^2+ax-1)$ if 3 or 6 or 2 is a square mod p, respectively.
(b) Deduce that $x^4 - 4x^2 + 1 \pmod p$ is reducible for every prime p.
(c)† Prove that every quadratic polynomial of the form $x^4+ax^2+b^2$ factors into two quadratics mod p, for every prime p.

Exercise 8.9.4. Prove that if $p \equiv 1 \pmod 4$, then $x^4 + 4$ factors into four linear factors mod p.

Exercise 8.9.5. Let $f(.)$ be the totally multiplicative function for which $f(3) = 1$ and $f(p) = \left(\frac{p}{3}\right)$ if $p \neq 3$.
(a) Give a formula for $f(n)$ for an arbitrary integer n.
(b)† For any given large constant B, suppose that p is a prime for which $(q/p) = f(q)$ for every prime $q \leq B$. Show that there are no three consecutive squares mod p that are all $\leq B$.

This shows that the result in exercise 8.1.8(b) cannot be extended to three consecutive integers provided the hypothesis in (b) holds. This hypothesis will be justified in exercise 8.17.2 of appendix 8D.

Exercise 8.9.6. Show that if $\left(\frac{n}{p}\right) = -1$, then $\sum_{d|n} \left(\frac{d}{p}\right) = 0$.

Exercise 8.9.7. Suppose that a and b are integers and $\{x_n : n \geq 0\}$ is the second-order linear recurrence sequence given by (0.1.2) with $x_0 = 0$ and $x_1 = 1$. Using exercise 0.4.10(b) prove that if odd prime p divides some x_n with n odd, then $(-b/p) = 1$. Deduce that if $(-b/p) = -1$ and p divides x_n, then n is even.

Exercise 8.9.8. (a) Suppose that p^k is an odd prime power. Prove that there are $1 + \left(\frac{a}{p}\right)$ residue classes $b \pmod{p^k}$ for which $b^2 \equiv a \pmod{p^k}$.
(b) Suppose that n is an odd positive integer. Prove that there are $\prod_{p \text{ prime: } p|n} \left(1 + \left(\frac{a}{p}\right)\right)$ residue classes $b \pmod n$ for which $b^2 \equiv a \pmod n$.
(c) Show that this equals $\sum_{d|n} \left(\frac{a}{d}\right)$ where the sum is restricted to squarefree integers d.

Exercise 8.9.9.† Let p be a given odd prime.
(a) Prove that for every $m \pmod p$ there exist a and b mod p such that $a^2 + b^2 \equiv m \pmod p$.
(b) Deduce that there are three squares, not all divisible by p, whose sum is divisible by p.
(c) Generalize this argument to show that if a, b, and c are not divisible by p, then there are at least p solutions $x, y, z \pmod p$ to $ax^2 + by^2 + cz^2 \equiv 0 \pmod p$.

Exercise 8.9.10.† Let m be a squarefree integer $\neq 1$, and let a be an odd positive integer.
(a) Prove that the Jacobi symbol $\left(\frac{4m}{a}\right)$ is a periodic function of a of period dividing $4m$.
(b) Show that the Jacobi symbol $\left(\frac{12}{a}\right)$ has minimal period 12.
(c) Prove that if m is odd and $(a, 2m) = 1$, then $\left(\frac{4m}{a+2m}\right) = \left(\frac{-1}{m}\right)\left(\frac{4m}{a}\right)$.
Now suppose that $m \equiv 3 \pmod 4$.
(d) Prove that there exists an integer r for which $\left(\frac{4m}{r}\right) = -1$.
(e) Prove that $\sum_{a=1}^{4m} \left(\frac{4m}{a}\right) = 0$.

Exercise 8.9.11. (This extends exercise 8.2.4.)
(a) Let $n = pq$ where p and q are distinct primes $\equiv 3 \pmod 4$, and $m = \frac{1}{2}\left(\frac{p-1}{2} \cdot \frac{q-1}{2} + 1\right)$. Show that if $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ and $b \equiv a^m \pmod n$, then $b^2 \equiv a \pmod n$.
(b) Any odd prime p can be written uniquely in the form $p = 1 + 2^k m$ where m is odd and $k \geq 1$. Prove that if a is a 2^kth power mod p and $b \equiv a^{\frac{m+1}{2}} \pmod p$, then $b^2 \equiv a \pmod p$.

If prime $p \equiv 1 \pmod 4$ and $(a/p) = 1$ but a is not a fourth power mod p, then we do not know how to use this idea to find a square root of $a \pmod p$. Known methods in this case are considerably more complicated (see, e.g., ?CranPom05).

Exercise 8.9.12. Suppose that p is a prime $\equiv 3 \pmod 4$ and $\left(\frac{b}{p}\right) = 1$. Prove that there are exactly two solutions $x \pmod p$ to $x^4 \equiv b \pmod p$.

Exercise 8.9.13.† Show that if p is a prime which divides $m^2 - 15$ for some integer m, then either $p = 2$, 3, or 5, or $p \equiv \pm 1, \pm 7, \pm 11$, or $\pm 17 \pmod{60}$.

Exercise 8.9.14.† Show that if p is a prime $\equiv 1 \pmod 4$, then -1 is a fourth power (mod p) if and only if 2 is a square mod p.

Exercise 8.9.15.† If $(a, n) = 1$, then multiplication by $a \pmod n$ generates a permutation of the reduced residues mod n. For example for 3 (mod 7) we get the permutation $\sigma_{3,7} := (1, 3, 2, -1, -3, -2)$, whereas for 2 (mod 7) we get the permutation $\sigma_{2,7} := (1, 2, 4)(3, 6, 5)$. Prove that if p is prime and $(a, p) = 1$, then the signature of the permutation

$$\epsilon(\sigma_{a,p}) = \left(\frac{a}{p}\right).$$

Exercise 8.9.16. (a) Prove that $\left(\frac{2^n-1}{2^m-1}\right) = 0$ if $(m, n) > 1$.

(b) Suppose that $n = mq + r$ where $n \geq m \geq r \geq 2$. Prove that $\left(\frac{2^n-1}{2^m-1}\right) = -\left(\frac{2^m-1}{2^r-1}\right)$.

(c)‡ Prove that if $n/m = [a_0, a_1, \ldots, a_k]$ with $(n, m) = 1$ and $a_k \geq 2$, then $\left(\frac{2^n-1}{2^m-1}\right) = (-1)^{k+1}$.

Infinitely many primes.

Exercise 8.9.17.† Fix odd, squarefree integer $n > 1$. Prove that there are infinitely many primes p for which $(p/n) = -1$.

Exercise 8.9.18.† Let n be a squarefree integer.

(a) By considering the prime divisors of $m^2 - n$, for well-chosen values of m, prove that there are infinitely many primes p for which $(n/p) = 1$.
(b) Deduce that there are infinitely many primes $\equiv 1 \pmod 3$.
(c) Refine this to deduce that there are infinitely many primes $\equiv 7 \pmod{12}$.
(d) Prove that there are infinitely many primes $\equiv 11 \pmod{12}$.
(e) Prove that there are infinitely many primes $\equiv 5 \pmod 8$.
(f) Prove that there are infinitely many primes $\equiv 7 \pmod 8$.
(g) Prove that there are infinitely many primes $\equiv 3 \pmod 8$.
(h) Prove that there are infinitely many primes $\equiv 5 \pmod{12}$.

Exercise 8.9.19.† Fix odd, squarefree integer $n > 1$. Using exercises 8.9.18(a) and 8.7.7 prove that there are infinitely many primes p for which $(p/n) = 1$.

Primitive roots for specially chosen primes.

Exercise 8.9.20.† Suppose that q and $p = 2q + 1$ are odd (Sophie Germain twin) primes.

(a) Show that if $p \equiv 3 \pmod 8$, then 2 is a primitive root mod p (e.g., 11, 59, 83, 107, ...).
(b) Show that if $p \equiv 7 \pmod 8$, then -2 is a primitive root mod p.
(c) Prove that -3 is a primitive root mod p, but 3 is not.

Exercise 8.9.21.† Suppose that q and $p = 4q + 1$ are odd primes. Prove that 2, -2, 3, and -3 are all primitive roots mod p.

Exercise 8.9.22.† Suppose that the Fermat number $F_m = 2^{2^m} + 1$ is prime with $m \geq 1$. Prove that if $(q/F_m) = -1$, then q is a primitive root mod F_m. (We deduce that 3 and 5 (for $m > 1$) are primitive roots mod F_m by exercise 8.5.4.)

Alternate proofs of the value of $(2/n)$.

Exercise 8.9.23. Let p be a prime $\equiv 1 \pmod 4$ so that there exists a reduced residue $r \pmod p$ such that $r^2 \equiv -1 \pmod p$.

(a) By expanding $(r + 1)^2 \pmod p$ prove that 2 is a square mod p if and only if r is a square mod p.
(b) Prove that r is a square mod p if and only if there is an element of order 8 mod p.
(c) Use Theorem 7.6 to deduce that 2 is a square mod p if and only if $p \equiv 1 \pmod 8$.

Exercise 8.9.24 (Proof of (8.7.2))**.** By induction on odd $n \geq 1$. By the law of quadratic reciprocity, as stated in (8.7.3), we have

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

as one of n and $n-2$ is $\equiv 1 \pmod 4$. Complete the proof.

Exercise 8.9.25. Every odd prime p may be written in the form $p = 4k + \sigma$ with $\sigma = \left(\frac{-1}{p}\right)$. We will show that $\left(\frac{2}{p}\right) = (-1)^k$ which implies Theorem 8.4. Let $m = 2k + \sigma$ so that $2m = p + \sigma$. Verify that

$$\left(\frac{2\sigma}{p}\right) = \left(\frac{2p+2\sigma}{p}\right) = \left(\frac{4m}{p}\right) = \left(\frac{m}{p}\right) = \left(\frac{\sigma p}{m}\right) = \left(\frac{2\sigma m - 1}{m}\right) = \left(\frac{-1}{m}\right)$$

and deduce the result from here.

Further proofs of the law of quadratic reciprocity.

Exercise 8.9.26.† (a) In the mid-18th century, Euler conjectured that if $m > n$ are coprime, odd, positive integers, then $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$ where $m - n = 4a$ if $m \equiv n \pmod 4$, and $m + n = 4a$ otherwise. Use the law of quadratic reciprocity to prove Euler's conjecture.

(b) Use Euler's conjecture to prove (8.7.3), the law of quadratic reciprocity.

Scholze (1938) proved Euler's conjecture using Gauss's Lemma (Theorem 8.6) and so gave a different proof of the law of quadratic reciprocity.

Exercise 8.9.27.‡ Finally we present my own variation of Rousseau's proof of quadratic recipocity, as a series of (challenging) exercises. Let $p < q$ be odd primes, and let $n = pq$. Let $A = \prod_{1 \leq m < n/2,\ (m,n)=1} m$. In the proof given of Theorem 8.5 in section 8.6, we showed that $A \equiv \left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) \pmod p$ and, analogously, $A \equiv \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right) \pmod q$. We now evaluate $A \pmod n$ much as in Gauss's proof of Wilson's Theorem, where we paired up each residue with its inverse: Let S be the set of (unordered) pairs $\{a, b\} \in [1, \frac{n}{2})$ for which $ab \equiv 1$ or $-1 \pmod n$.

(a) Prove that the residues a and b are distinct unless $a^2 \equiv 1$ or $-1 \pmod n$.

(b) Prove that if $a^2 \equiv 1 \pmod n$, then $a \equiv 1$, -1, r, and $-r \pmod n$ for some $r \not\equiv \pm 1 \pmod n$.

(c) Prove that the product of the integers $a \in [1, \frac{n}{2})$ with $a^2 \equiv 1 \pmod n$ is $\equiv \pm r \pmod n$.

(d) Prove that if $b^2 \equiv -1 \pmod n$, then $p \equiv q \equiv 1 \pmod 4$. In this case:
- Deduce that the product of the integers $b \in [1, \frac{n}{2})$ for which $b^2 \equiv -1 \pmod n$ is $\equiv \pm r \pmod n$.
- Deduce that $A \equiv \pm 1 \pmod n$.
- Combine the above to show that $\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{q}\right)$.

(e) If at least one of p and q is $\equiv 3 \pmod 4$:
- Deduce that $A \equiv \pm r \pmod n$.
- Combine the above to show that $\left(\frac{-1}{q}\right)\left(\frac{q}{p}\right) = -\left(\frac{-1}{p}\right)\left(\frac{p}{q}\right)$.

(f) Deduce Theorem 8.5.

Appendix 8A. Eisenstein's proof of quadratic reciprocity

8.10. Eisenstein's elegant proof, 1844

Exercise 8.10.1.† Use Gauss's Lemma to determine the values of (a) $(-1/p)$ and of (b) $(3/p)$, for all primes $p > 3$.

Exercise 8.10.2.† Let r be the absolutely least residue of $N \pmod p$. Prove that the least non-negative residue of $N \pmod p$ is given by

$$N - p\left[\frac{N}{p}\right] = \begin{cases} r & \text{if } r \geq 0, \\ p + r & \text{if } r < 0. \end{cases}$$

Appendix 8B. Small quadratic non-residues

Exercise 8.11.1. Prove that the smallest quadratic non-residue mod p must be a prime.

8.11. The least quadratic non-residue modulo p

8.12. The smallest prime q for which p is a quadratic non-residue modulo q

8.13. Character sums and the least quadratic non-residue

Exercise 8.13.1. (a) Prove that $S(x)$ is periodic with period p.
(b) Prove that $|S(x)| \leq \frac{p-1}{2}$ for all integers x.

Appendix 8C. The first proof of quadratic reciprocity

8.14. Gauss's original proof of the law of quadratic reciprocity

Appendix 8D. Dirichlet characters and primes in arithmetic progressions

8.15. The Legendre symbol and a certain quotient group

Exercise 8.15.1.† Suppose that A is a subset of G_p of size $\frac{p-1}{2}$ that is closed under multiplication. Prove that $A = H_p$.

8.16. Dirichlet characters

Exercise 8.16.1. Deduce that either $\chi(1) = 1$ or $\chi(a) = 0$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Exercise 8.16.2.† Given $\chi, \psi \in X(n)$, define $\chi\psi$ by $(\chi\psi)(a) = \chi(a)\psi(a)$ for all integers a, and then prove that $\chi\psi \in X(n)$. Prove that $\overline{\chi}$ defined by $\overline{\chi}(a) = \overline{\chi(a)}$ is a character. Prove that $X(n)$ forms a group under multiplication.

Exercise 8.16.3. (a) † Use the Chinese Remainder Theorem to show that if $n = \prod_p p^{e_p}$, then $X(n) = \left\{\prod_p \chi_p : \ \chi_p \in X(p^{e_p})\right\}$.
(b) Deduce that $X(n)$ has $\phi(n)$ elements.
(c) Show that if $\chi \in X(n)$, then $\chi^{\lambda(n)} = \chi_0$ where $\lambda(n)$ is Carmichael's function (as defined in section 7.17 of appendix 7B).
(d) Show that if $\chi \in X(n)$ is non-principal, then there exists $a \pmod n$ such that $\chi(a) \neq 0$ or 1.
(e) Prove that if p is an odd prime and $m \not\equiv 0$ or $1 \pmod p$, then there exists $\chi \in X(p)$ such that $\chi(m) \neq 1$.
(f) Prove that if $(m, n) = 1$ and $m \not\equiv 1 \pmod n$, then there exists $\chi \in X(n)$ such that $\chi(m) \neq 1$.

Exercise 8.16.4.‡ (a) Prove that if n is a squarefree odd integer, then the Jacobi symbol $\left(\frac{\cdot}{n}\right)$ is primitive.

(b) Prove that the real, primitive characters are given by 1, and for each squarefree, odd n:
- The Jacobi symbol $\left(\frac{\cdot}{n}\right)$ of modulus n, if $n > 1$.
- The symbol $\left(\frac{2n}{\cdot}\right)$ of modulus $8|n|$.
- The symbol $\left(\frac{4n}{\cdot}\right)$ of modulus $4|n|$, if $n \equiv 3 \pmod 4$.

Exercise 8.16.5. Reprove (8.16.2) using the representation of the reduced residues given in (8.16.1).

8.17. Dirichlet series and primes in arithmetic progressions

Exercise 8.17.1. (a) Prove that there are infinitely many integers n for which $\mu(n)+\mu(n+1) = -1$.

(b) Prove that there are infinitely many integers n for which $\mu(n) + \mu(n+1) = 1$.

Exercise 8.17.2.‡ (a) Given $\sigma \in \{-1, 1\}$ and prime q, show that there are infinitely many primes p for which $\left(\frac{q}{p}\right) = \sigma$.

(b) Given $\sigma_1, \dots, \sigma_k \in \{-1, 1\}$ and primes $q_1, \dots, q_k$, show that there are infinitely many primes p for which $\left(\frac{q_j}{p}\right) = \sigma_j$ for $j = 1, 2, \dots, k$.

(c) Prove that for any given integer B there are infinitely many primes p such that there are no integers $n, 1 \le n \le B$, for which $\left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) = \left(\frac{n+2}{p}\right)$.

We will return to the question of finding strings of consecutive quadratic residues with more sophisticated tools in section 14.6.

Appendix 8E. Quadratic reciprocity and recurrence sequences

8.18. The Fibonacci numbers modulo p

Exercise 8.18.1. Deduce that if $(5/p) = 1$, then $F_{n+p-1} \equiv F_n \pmod p$ for all $n \ge 0$.

Exercise 8.18.2. Deduce that if $(5/p) = -1$, then $F_{n+2p+2} \equiv F_n \pmod p$ for all $n \ge 0$.

Exercise 8.18.3.† Let $x_0 = 0$, $x_1 = 1$, and $x_{n+2} = ax_{n+1}+bx_n$ for all $n \ge 0$, and let $\Delta := a^2+4b$. Suppose that prime p does not divide $a\Delta$.

(a) Show that if $(\Delta/p) = 1$, then $x_{n+p-1} \equiv x_n \pmod p$ for all $n \ge 0$.

(b) Show that if $(\Delta/p) = -1$, then $x_{n+p+1} \equiv -bx_n \pmod p$ for all $n \ge 0$.

(c) Deduce that there exists a positive integer $d \le p^2 - 1$ such that $x_{n+d} \equiv x_n \pmod p$ for all $n \ge 0$.

Exercise 8.18.4.† Let $x_0 = 0$, $x_1 = 1$, and $x_{n+2} = ax_{n+1}+bx_n$ for all $n \ge 0$, and let $\Delta := a^2+4b$.

(a) Show that $x_n \equiv n(a/2)^{n-1} \pmod \Delta$ for all $n \ge 1$.

(b) Deduce that if p divides Δ, then $x_{n+p} \equiv \frac{a}{2}x_n \pmod p$ for all $n \ge 0$.

(c) Prove that if $p|a$, then $x_{n+p-1} \equiv \left(\frac{b}{p}\right) x_n \pmod p$ for all $n \ge 0$.

Exercise 8.18.5.† Let $(x_n)_{n\ge0}$ be as in exercise 8.18.3 with $(a, b) = 1$, and let p be a prime.

(a) Prove that $(x_n, b) = 1$ for all $n \ge 0$.

(b) Prove that $(x_n, x_{n+1}) = 1$ for all $n \ge 0$.

(c) By considering the possible pairs $\{x_n, x_{n+1}\} \pmod p$, prove that there exists a positive integer $d \le p^2 - 1$ such that $x_{n+d} \equiv x_n \pmod p$ for all $n \ge 0$.

Exercise 8.18.6.† Let r be the smallest integer ≥ 1 for which given prime p divides F_r.
(a) Using exercises 0.4.10 and 2.5.19(c) to show that $F_{kr} \equiv rF_k F_{k+1}^{r-1} \pmod{F_k^2}$ and $F_{kr+1} \equiv F_{k+1}^r \pmod{F_k^2}$.
(b) Suppose that $F_n \pmod{p}$ has period k. Deduce that $F_n \pmod{p^2}$ has period k or kp.
(c) Deduce that the period of $F_n \pmod{p^2}$ divides $p(p-1)$ if $(5/p) = 1$, and it divides $2p(p+1)$ if $(5/p) = -1$.

8.19. General second-order linear recurrence sequences modulo p

8.20. Prime values in recurrence sequences

Exercise 8.20.1. Assume that p and $q = 2p + 1$ are both prime. Deduce that q divides $2^p - 1$ whenever $p \equiv 3 \pmod{4}$, and so $2^p - 1$ is not a Mersenne prime.