Chapter 7
Gauss Sums, Quadratic Reciprocity, and the Jacobi Symbol

Our first goal in this chapter is to present Gauss' sixth proof of his Law of Quadratic Reciprocity. The presentation here follows [32, §3.3] fairly closely, except that our Gauss sums are over the complex numbers, as opposed to *ibid.* where Gauss sums are considered over a finite field. Later in the chapter we introduce the Jacobi symbol and study its basic properties. We will also prove the Law of Quadratic Reciprocity for the Jacobi symbol. At the end of the chapter we will show examples that demonstrate how the Jacobi symbol can be used to compute the Legendre symbol efficiently. The Jacobi symbol will make an appearance in Chapter 10 when we give a proof of the Three Squares Theorem. In the Notes, we give some references for the various proofs of the Law of Quadratic Reciprocity.

7.1 Gauss sums and Quadratic Reciprocity

For an odd prime p, let $\zeta = e^{\frac{2\pi i}{p}}$ and define the pth *Gauss sum* by

$$\tau_p = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k.$$

We start with the following lemma:

Lemma 7.1. *For all odd primes p,*

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

Proof. We have

$$\tau_p^2 = \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{k}{p}\right)\left(\frac{l}{p}\right) \zeta^{k+l} = \sum_{k=1}^{p-1} \sum_{l=1}^{p-1} \left(\frac{kl}{p}\right) \zeta^{k+l}.$$

R. Takloo-Bighash, *A Pythagorean Introduction to Number Theory*,
Undergraduate Texts in Mathematics, https://doi.org/10.1007/978-3-030-02604-2_7

We make a change of variables by introducing a new variable m by $l \equiv mk \bmod p$. When k, l range over $\{1, \ldots, p-1\}$, m varies over the same set. So we get

$$\tau_p^2 = \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{mk^2}{p}\right) \zeta^{k+mk} = \sum_{k=1}^{p-1} \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \zeta^{k+mk}$$

$$= \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \sum_{k=1}^{p-1} \zeta^{k(m+1)}.$$

The innermost sum is a geometric sum, and if $\zeta^{m+1} \neq 1$, we get

$$\sum_{k=1}^{p-1} \zeta^{k(m+1)} = \frac{(\zeta^p)^{m+1} - \zeta^{m+1}}{\zeta^{m+1} - 1} = \frac{1 - \zeta^{m+1}}{\zeta^{m+1} - 1} = -1.$$

If on the other hand $\zeta^{m+1} = 1$, we have

$$e^{\frac{2\pi i(m+1)}{p}} = 1.$$

Consequently, $p|m+1$, and, since $1 \leq m \leq p-1$, we conclude that $m = p-1$. In this case,

$$\sum_{k=1}^{p-1} \zeta^{k(m+1)} = p - 1.$$

Putting everything together,

$$\tau_p^2 = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right) \sum_{k=1}^{p-1} \zeta^{k(m+1)}$$

$$= \sum_{m=1}^{p-2} \left(\frac{m}{p}\right) \sum_{k=1}^{p-1} \zeta^{k(m+1)} + (p-1)\left(\frac{p-1}{p}\right)$$

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

$$= -\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) + \left(\frac{p-1}{p}\right) + (p-1)\left(\frac{p-1}{p}\right)$$

$$= -\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) + p\left(\frac{p-1}{p}\right) = -\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) + p\left(\frac{-1}{p}\right).$$

So in order to prove the lemma it suffices to prove

$$\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = 0.$$

To see this, let

$$X = \sum_{m=1}^{p-1} \left(\frac{m}{p}\right).$$

Pick an integer b, e.g, a primitive root modulo p, such that $(b/p) = -1$. Then

$$-X = \left(\frac{b}{p}\right) X = \sum_{m=1}^{p-1} \left(\frac{b}{p}\right)\left(\frac{m}{p}\right) = \sum_{m=1}^{p-1} \left(\frac{bm}{p}\right).$$

But when m ranges over the numbers $\{1, \ldots, p-1\}$, the product mb ranges over the same set modulo p. Consequently, the last expression is equal to X as well. Hence

$$-X = X.$$

This implies $X = 0$, and we are done.

Now we can proceed to prove the Quadratic Reciprocity, presenting a variation of Gauss's extremely clever argument. This proof uses Gauss sums. In the course of the proof we will use algebraic integers as introduced in Appendix B.

Proof of Theorem 6.8. For the first part we start with the observation that

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

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

after using Lemma 6.7. Next,

$$\tau_p^q = \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k\right)^q.$$

By Lemma 2.28 this last expression is equal to

$$\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^{kq} + qC \tag{7.1}$$

for some complex number C. It follows from Theorem B.4 and the fact that roots of unity are algebraic integers that the number C is an algebraic integer; see Exercise 7.3. Let q^{-1} be the multiplicative inverse of q modulo p. Then the sum is equal to

$$\sum_{k=1}^{p-1} \left(\frac{kq^{-1}}{p}\right) \zeta^k = \left(\frac{q^{-1}}{p}\right) \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \zeta^k = \left(\frac{q^{-1}}{p}\right) \tau_p,$$

Since $q \cdot q^{-1} \equiv 1 \bmod p$, we have

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

Putting everything together,

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

Dividing by τ_p gives,

$$\left(\frac{q}{p}\right) + q\frac{C}{\tau_p} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}}. \tag{7.2}$$

This expression in particular shows that $m := qC/\tau_p$ is an integer. We claim that m is divisible by q. We have

$$m^2 = \frac{q^2C^2}{\tau_p^2} = \pm\frac{q^2C^2}{p}. \tag{7.3}$$

Since C is an algebraic integer, by Theorem B.4, C^2 is an algebraic integer. Equation 7.3 shows that C^2 is a rational number. Corollary B.3 shows that $C^2 \in \mathbb{Z}$.

Since $p \mid q^2C^2$ and $(p, q^2) = 1$, Theorem 2.17 implies that $p \mid C^2$. Consequently, m^2 is divisible by q^2. This means m is divisible by q. Now that we know that qC/τ_p is an integer which is divisible by q, we reduce Equation (7.2) modulo q. We have by Lemma 6.5:

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

So we conclude that

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

Since the two sides of the equation are ± 1 and q is odd, an argument similar to the one in the proof of Lemma 6.6 gives

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

as claimed.

We now proceed to prove the second part of Theorem 6.8. Set

$$\zeta = e^{\frac{\pi i}{4}},$$

an eighth root of unity. We have

$$\zeta^2 = e^{\frac{\pi i}{2}} = \cos\frac{\pi i}{2} + i\sin\frac{\pi i}{2} = i,$$

and

$$\zeta^{-2} = i^{-1} = -i.$$

Now set

$$\rho = \zeta + \zeta^{-1}.$$

We have

$$\rho^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = i + i^{-1} + 2 = 2.$$

Next,

$$\rho^p = (\rho^2)^{\frac{p-1}{2}} \cdot \rho = 2^{\frac{p-1}{2}} \cdot \rho.$$

On the other hand,

$$\rho^p = (\zeta + \zeta^{-1})^p = \zeta^p + \zeta^{-p} + \sum_{k=1}^{p-1} \binom{p}{k} \zeta^k \zeta^{-(p-k)}$$

$$= \zeta^p + \zeta^{-p} + \sum_{k=1}^{(p-1)/2} \binom{p}{k} (\zeta^k \zeta^{-(p-k)} + \zeta^{-k} \zeta^{p-k})$$

$$= \zeta^p + \zeta^{-p} + \sum_{k=1}^{(p-1)/2} \binom{p}{k} (\zeta^{2k-p} + \zeta^{p-2k}).$$

If $8 \mid k$, then $\zeta^k = 1$. For this reason, for an odd number l, the value of $\zeta^l + \zeta^{-l}$ depends only on the residue of l modulo 8. We only need to consider the residue classes 1, 3, 5, 7:

- If $l \equiv 1 \bmod 8$, then $\zeta^l + \zeta^{-l} = \zeta + \zeta^{-1} = \rho$.
- If $l \equiv 3 \bmod 8$, then

  $$\zeta^l = \zeta^3 = e^{\frac{3\pi i}{4}} = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = -\cos\frac{\pi}{4} + \sin\frac{\pi}{4} = -\zeta^{-1},$$

  and similarly, $\zeta^{-l} = -\zeta$. Hence,

  $$\zeta^l + \zeta^{-l} = -\zeta^{-1} - \zeta = -\rho.$$

- If $l \equiv 5 \bmod 8$, then

  $$\zeta^l = \zeta^5 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = -\cos\frac{\pi}{4} - i\sin\frac{\pi}{4} = -\zeta,$$

  and also $\zeta^{-l} = -\zeta$. This means that in this case

  $$\zeta^l + \zeta^{-l} = -\zeta - \zeta^{-1} = -\rho.$$

- If $l \equiv 7 \bmod 8$, then $\zeta^l = \zeta^{-1}$, $\zeta^{-l} = \zeta$, and $\zeta^l + \zeta^{-l} = \zeta^{-1} + \zeta = \rho$.

These computations mean

$$\zeta^p + \zeta^{-p} = (-1)^{\frac{p^2-1}{8}}\rho,$$

and for all $1 \leq k \leq p-1$,

$$\zeta^{2k-p} + \zeta^{p-2k} = (-1)^{\frac{(p-2k)^2-1}{8}}\rho.$$

Consequently,

$$2^{\frac{p-1}{2}} \cdot \rho = (-1)^{\frac{p^2-1}{8}}\rho + \sum_{k=1}^{(p-1)/2} \binom{p}{k}(-1)^{\frac{(p-2k)^2-1}{8}}\rho.$$

Dividing by ρ gives

$$2^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}} + \sum_{k=1}^{(p-1)/2} \binom{p}{k}(-1)^{\frac{(p-2k)^2-1}{8}}. \tag{7.4}$$

By Lemma 2.27, the binomial coefficient $\binom{p}{k}$ for $1 \leq k \leq p-1$ is divisible by p. Reduce Equation (7.4) modulo p to get

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \mod p.$$

Lemma 6.5 now gives the result. □

7.2 The Jacobi Symbol

In this section we introduce the *Jacobi symbol* which is a generalization of the Legendre symbol.

Definition 7.2. Let b be an odd positive integer, and let a be an integer. We define the Jacobi symbol $\left(\frac{a}{b}\right)$ as follows. If $b = p_1 \dots p_k$, with p_i's not necessarily distinct, we set

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)$$

For example,

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right).$$

In the case where b is an odd prime number, the Jacobi symbol is identical with the Legendre symbol. There is an important difference between the Legendre symbol and the Jacobi symbol, however. The Legendre symbol (a/p) for a prime number

p determines the solvability of the congruence equation $X^2 \equiv a \bmod p$. In general, the Jacobi symbol (a/b) gives no information about the solvability of the equation $X^2 \equiv a \bmod b$. Suppose, for example, $b = p^2$, with p a prime number. If $X^2 \equiv a \bmod b$ is solvable, then, since $p \mid b$, so is $X^2 \equiv a \bmod p$. So if $(a/p) = -1$, the equation $X^2 \equiv a \bmod b$ will not be solvable. However, $(a/b) = (a/p^2) = (a/p)^2 = (\pm 1)^2 = +1$. The simplest example of this is when $a = -1$ and $b = 9 = 3^2$. In this case, $(-1/9) = (-1/3)^2 = (-1)^2 = +1$, but the equation $X^2 \equiv -1 \bmod 9$ is not solvable. Despite this issue the Jacobi symbol is a useful tool that allows to compute the Legendre symbol without having to factorize integers. We will see some examples at the end of this section.

We have the following theorem:

Theorem 7.3 (Quadratic Reciprocity for the Jacobi symbol).

1. *If m is an odd natural number,*
$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$
2. *If m is an odd natural number,*
$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$
3. *For odd natural numbers m and n,*
$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

Before we start the proof of the theorem, we note that the above theorem is a generalization of Theorem 6.8.

We start the proof of the theorem with a lemma:

Lemma 7.4. *For an odd natural number q and a natural number α the following identities hold:*

1. $\frac{q^\alpha - 1}{2} \equiv \frac{\alpha(q-1)}{2} \bmod 2$;
2. $\frac{q^{2\alpha} - 1}{8} \equiv \frac{\alpha(q^2-1)}{8} \bmod 2$.

Proof. Proof is by induction. Clearly both identities are true for $\alpha = 1$. So assume that the identities are true for α, and we wish to show their validity for $\alpha + 1$.

We have
$$\frac{q^{\alpha+1} - 1}{2} = \frac{q^{\alpha+1} - q^\alpha + q^\alpha - 1}{2} = q^\alpha\left(\frac{q-1}{2}\right) + \frac{q^\alpha - 1}{2}.$$

This last expression, by the induction assumption, is congruent to

$$\frac{q-1}{2}+\frac{\alpha(q-1)}{2}\equiv\frac{(\alpha+1)(q-1)}{2} \mod 2.$$

The second identity is proved in a completely similar way.

We can now prove the theorem.

Proof of Theorem 7.3. To prove the first part we do induction on the number of distinct prime divisors of m. Write $m = p_1^{\alpha_1}\dots p_r^{\alpha_r}$, and we do induction on r. We need to prove

$$\frac{p_1^{\alpha_1}\cdots p_r^{\alpha_r}-1}{2}\equiv\alpha_1\frac{p_1-1}{2}+\cdots+\alpha_r\frac{p_r-1}{2} \mod 2.$$

The $r = 1$ case is the first part of Lemma 7.4. Now suppose the identity is valid for r, and we wish to prove it for $r+1$. We have

$$\begin{aligned}\frac{p_1^{\alpha_1}\cdots p_r^{\alpha_r}p_{r+1}^{\alpha_{r+1}}-1}{2}&=\frac{p_1^{\alpha_1}\cdots p_r^{\alpha_r}p_{r+1}^{\alpha_{r+1}}-p_1^{\alpha_1}\cdots p_r^{\alpha_r}+p_1^{\alpha_1}\cdots p_r^{\alpha_r}-1}{2}\\&=p_1^{\alpha_1}\cdots p_r^{\alpha_r}\frac{p_{r+1}^{\alpha_{r+1}}-1}{2}+\frac{p_1^{\alpha_1}\cdots p_r^{\alpha_r}-1}{2}\\&\equiv\frac{p_{r+1}^{\alpha_{r+1}}-1}{2}+\frac{p_1^{\alpha_1}\cdots p_r^{\alpha_r}-1}{2} \mod 2 \quad (\text{as } p_1^{\alpha_1}\cdots p_r^{\alpha_r} \text{ is odd.})\\&\equiv\alpha_1\frac{p_1-1}{2}+\cdots+\alpha_r\frac{p_r-1}{2}+\alpha_{r+1}\frac{p_{r+1}-1}{2} \mod 2\end{aligned}$$

after using the first part of Lemma 7.4 and the induction hypothesis.

The proof of the second part of the theorem is completely similar to our proof of the first part, except that here we need to use the second part of Lemma 7.4 and the computation of $(2/p)$ for an odd prime p from Theorem 6.8.

We now prove the last part of the theorem. Let $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ and $n = q_1^{\beta_1}\cdots q_s^{\beta_s}$ be the prime factorizations of m and n. If m and n are not coprime, both sides of the identity are equal to zero, and there is nothing to prove. So we assume that the p_i's and q_j's are distinct primes. By definition,

$$\begin{aligned}\left(\frac{m}{n}\right)&=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{p_i}{q_j}\right)^{\alpha_i\beta_j}\\&=\prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_j}{p_i}\right)^{\alpha_i\beta_j}(-1)^{\alpha_i\beta_j\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}} \quad (\text{by Theorem 6.8})\\&=\left(\frac{n}{m}\right)\prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\alpha_i\beta_j\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.\end{aligned}$$

So to prove the third part we just need to show that

$$\frac{m-1}{2}\cdot\frac{n-1}{2}\equiv\sum_{i=1}^{r}\sum_{j=1}^{s}\alpha_i\beta_j\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}\mod 2.$$

To see this, we note that by the proof of the first part of the Theorem,

$$\frac{m-1}{2}\equiv\sum_{i=1}^{r}\alpha_i\frac{p_i-1}{2}\mod 2,$$

and

$$\frac{n-1}{2}\equiv\sum_{j=1}^{s}\beta_j\frac{q_j-1}{2}\mod 2.$$

Multiplying these identities gives the result. □

Now, we will use the Jacobi symbol to compute some Legendre symbols. Let's start with a small example. Suppose we want to compute

$$\left(\frac{37}{89}\right).$$

Since both 37 and 89 are odd primes we can use the Law of Quadratic Reciprocity, Theorem 6.8, to obtain

$$\left(\frac{37}{89}\right)=(-1)^{(37-1)(89-1)/4}\left(\frac{89}{37}\right)=\left(\frac{89}{37}\right).$$

Since $89\equiv 15 \mod 37$, the latter quadratic residue symbol is equal to

$$\left(\frac{15}{37}\right).$$

If we were to use the methods of Chapter 6 at this point we would use the fact that $15=3\times 5$ to write $(15/37)=(3/37)\cdot(5/37)$, and then we would apply the Law of Quadratic Reciprocity twice to compute these latter quadratic residue symbols. The problem with this approach is that it requires factorizing 15, and this is something we can do because 15 is a small number. As mentioned in Notes to Chapters 2 and 6, at present we do not know how to factorize a very large natural number in reasonable time. Using the Jacobi symbol allows us to bypass this obstacle. In fact, by Theorem 7.3 we have

$$\left(\frac{15}{37}\right)=(-1)^{(15-1)(37-1)/4}\left(\frac{37}{15}\right)=\left(\frac{37}{15}\right)=\left(\frac{7}{15}\right),$$

as $37\equiv 7 \mod 15$. Applying Theorem 7.3 to $(7/15)$ gives

$$\left(\frac{7}{15}\right) = (-1)^{(7-1)(15-1)/2}\left(\frac{15}{7}\right) = -\left(\frac{15}{7}\right) = -\left(\frac{1}{7}\right) = -1,$$

after using $15 \equiv 1 \bmod 7$. Putting everything together, we obtain

$$\left(\frac{37}{89}\right) = -1.$$

Let us now examine an example involving larger numbers. We wish to compute the Legendre symbol

$$\left(\frac{2455927}{36838897}\right).$$

By Theorem 7.3 we have

$$\left(\frac{2455927}{36838897}\right) = (-1)^{(2455927-1)(36838897-1)/4}\left(\frac{36838897}{2455927}\right)$$

$$= \left(\frac{36838897}{2455927}\right) = \left(\frac{2455919}{2455927}\right),$$

as $36838897 \equiv 2455919 \bmod 2455927$. Again using Theorem 7.3 gives

$$\left(\frac{2455919}{2455927}\right) = (-1)^{(2455919-1)(2455927-1)/4}\left(\frac{2455927}{2455919}\right)$$

$$= \left(\frac{2455927}{2455919}\right) = \left(\frac{8}{2455919}\right) = \left(\frac{2}{2455919}\right)^3.$$

Here we have used the fact that $2455927 \equiv 8 \equiv 2^3 \bmod 2455919$, and also the multiplicativity of the Jacobi symbol. Since $(\pm 1)^3 = \pm 1$, the latter Jacobi symbol is equal to $(2/2455919)$. So we have established that

$$\left(\frac{2455927}{36838897}\right) = \left(\frac{2}{2455919}\right).$$

To finish the computation we use the second part of Theorem 7.3 to get

$$\left(\frac{2}{2455919}\right) = (-1)^{(2455919^2-1)/8} = +1.$$

We have proved

$$\left(\frac{2455927}{36838897}\right) = +1.$$

The important point to note here is that we did not have to worry the primality of the numbers that showed up in the computation. In fact, $2455919 = 6841 \times 359$ is not prime.

Exercises

7.1 Compute τ_p for $p = 3, 5$, and verify Lemma 7.1 directly.

7.2 (✠) Compute τ_p for $p = 17$.

7.3 Show that the complex number C defined in Equation (7.1) is an algebraic integer.

7.4 Prove the second part of Lemma 7.4.

7.5 Prove the second part of Theorem 7.3.

7.6 Determine all natural numbers n such that $(n/15) = +1$.

7.7 Determine $(215/997)$ and $(113/1093)$ using the Jacobi symbol.

7.8 Find five pairs of integers (a, b) such that the Jacobi symbol $(a/b) = +1$ but $x^2 \equiv a \bmod b$ is not solvable.

7.9 Show that for all $n > 1$ we have the following identities for Jacobi symbols

$$\left(\frac{n}{4n-1}\right) = -\left(\frac{-n}{4n-1}\right) = 1.$$

7.10 Show that for an integer d with $|d| > 1$ we have

$$\left(\frac{d}{|d|-1}\right) = \begin{cases} 1 & d > 0; \\ -1 & d < 0. \end{cases}$$

7.11 Let $k \in \mathbb{N}$, and let $\gcd(d, k) = 1$. Prove that the number of solutions of $x^2 \equiv d \bmod 4k$ is

$$2 \sum_{\substack{f \mid k \\ f \text{ squarefree}}} \left(\frac{d}{f}\right).$$

7.12 Show that for an odd prime p, and $a \in \mathbb{N}$ with $p \nmid a$, we have

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p - 4a}\right).$$

7.13 This exercise gives another proof of the Law of Quadratic Reciprocity due to Rousseau [94]. The proof uses a bit of group theory. Let p, q be odd primes, and define $G = (\mathbb{Z}/pq\mathbb{Z})^\times/\{\pm 1\}$.

a. Show that the set

$$S = \left\{(x, y) \mid 1 \le x \le p-1, 1 \le y \le \frac{q-1}{2}\right\}$$

is a set of representatives for G. What is the product of elements of S modulo $\{\pm 1\}$?

b. Show that the set

$$S' = \left\{(z \bmod p, z \bmod q) \mid 1 \le z \le \frac{pq-1}{2}\right\}$$

is another set of representatives of G. Determine the product of elements of S' modulo $\{\pm 1\}$.

c. Derive the Law of Quadratic Reciprocity from the first two parts.

Notes

Proofs of quadratic reciprocity

As mentioned in Chapter 6, the Law of Quadratic Reciprocity was conjectured by Euler around 1745, in a paper titled "Theoremata circa divisores numerorum in hac forma $pa^2 \pm qb^2$ contentorum" available from the *Euler Archive* at

http://eulerarchive.maa.org/index.html

though here the conjecture is not explicitly stated as such. The explicit formulation of the conjecture appears in a later paper of Euler's, titled "Observationes circa divisionem quadratorum per numeros primos" available at

http://eulerarchive.maa.org/pages/E552.html

Gauss noted in his notebook that he had found a proof on April 8, 1796. So far over 200 proofs of the Law of Quadratic Reciprocity have been obtained by various mathematicians. Franz Lemmermeyer, the author of [32], maintains a website that keeps track of the various proofs of theorem. The website is available at

http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html

Generalizations

One can generalize the Law of Quadratic Reciprocity in two different directions, one is by considering higher powers, and the other by considering other number fields, introduced in the Notes to Chapter 5. For introductions to reciprocity laws for higher powers we refer the reader to Lemmermeyer [32] or Cox [14], especially §4. For the generalization of Quadratic Reciprocity to other number fields, known as *Hilbert's Law of Reciprocity*, see the Notes to Chapter 8.