

Supplement 4

Permutations, Legendre symbol and quadratic reciprocity

1. Permutations.

If S is a finite set containing n elements then a permutation of S is a one to one mapping of S onto S . Usually S is the set $\{1, 2, \dots, n\}$ and a permutation σ can be represented as follows:

$$\begin{array}{cccccc} 1 & 2 & \dots & j & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(j) & \dots & \sigma(n) \end{array}$$

Thus if $n = 5$ we could have

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{array}$$

If $\{a, b\} \in S$, $a \neq b$ then we can define a permutation of S as follows:

$$\sigma(c) = \begin{cases} c & \text{if } c \notin \{a, b\} \\ b & \text{if } c = a \\ a & \text{if } c = b \end{cases}$$

We will call such a permutation a *transposition* and denote it (ab) . If σ and τ are permutations of S then we write $\sigma\tau$ for $\sigma \circ \tau$ the usual composition of maps ($\sigma\tau(a) = \sigma(\tau(a))$). Since a permutation is one to one and onto if σ is a permutation then we can define σ^{-1} by $\sigma^{-1}(y) = x$ if $\sigma(x) = y$. If I is the identity map then $\sigma^{-1}\sigma = \sigma\sigma^{-1} = I$. We also note that $(\sigma\mu)\nu = \sigma(\mu\nu)$ for permutations σ, μ, ν .

Lemma 1 *Every permutation, σ , can be written as a product of transpositions. (Here a product of no transpositions is the identity map, I .)*

Proof. Let n be the number of elements in S . We prove the result by induction on j with $n-j$ the number of elements in S fixed by σ . If $j = 0$ then σ is the identity map and thus is written as a product of $n = 0$ transpositions. Assume that we have prove the theorem for all σ at least $n - j$ fixed points. We look at the case when σ has $n - j - 1$ fixed points. Let $a \in S$ be such

that $\sigma(a) = b$ and $b \neq a$. Then $(ab)\sigma(a) = a$. Suppose that $\sigma(c) = c$ then $c \neq a$ and $c \neq b$ since if $\sigma(c) = b$ then $\sigma(a) = \sigma(c)$ which is contrary to our assumption. Thus if $\sigma(c) = c$ then $(ab)\sigma(c) = c$. This implies that the number of elements fixed by $(ab)\sigma$ is at least $n - j - 1 + 1 = n - j$. Thus $(ab)\sigma(c)$ can be written as $(a_1b_1) \cdots (a_rb_r)$. Now $(ab)(ab) = I$ the identity. Thus

$$\sigma = (ab)(ab)\sigma = (ab)(a_1b_1) \cdots (a_rb_r).$$

This completes the inductive step. ■

Note that the above lemma gives a method for calculation. Consider σ given by

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{array}$$

Then $(13)\sigma$ is given by

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{array}$$

$(23)(13)\sigma$ is given by

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{array}$$

$(35)(23)(13)\sigma$ is given by

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{array}$$

and finally $(45)(35)(23)(13)\sigma$ is the identity. Since a transposition is its own inverse we see that

$$\sigma = (13)(23)(35)(45).$$

Let x_1, \dots, x_n be n indeterminates. Set $\Delta(x_1, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$.

Theorem 2 *Let σ be a permutation of a set S with n elements. Let $\{a_1, a_2, \dots, a_n\}$ be a listing of the elements of S . If define $\tau : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ by $\sigma(a_i) = a_{\tau(i)}$ then*

(1) $\prod_{1 \leq i < j \leq n} (x_{\tau(i)} - x_{\tau(j)}) = \varepsilon(\tau)\Delta(x_1, \dots, x_n)$ with $\varepsilon(\tau) \in \{1, -1\}$.

(2) *If σ, μ are permutations and $\mu(a_i) = a_{\zeta(i)}$ then $\sigma\mu(a_i) = a_{\tau\zeta(i)}$ and $\varepsilon(\tau\zeta) = \varepsilon(\tau)\varepsilon(\zeta)$.*

(3) *Suppose that $\{b_1, \dots, b_n\}$ is another listing of the elements of S and we define $\nu : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ by $\sigma(b_i) = b_{\nu(i)}$. Then $\varepsilon(\nu) = \varepsilon(\tau)$. This says that we can define $\text{sgn}(\sigma) = \varepsilon(\tau)$ since the expression is independent of how we enumerate the elements of S .*

(4) Assume that $S = S_1 \cup S_2$ with $S_1 \cap S_2 = \emptyset$. Let σ_i be a permutation of S_i for $i = 1, 2$. Define a permutation of S by

$$\sigma(x) = \begin{cases} \sigma_1(x) & \text{if } x \in S_1 \\ \sigma_2(x) & \text{if } x \in S_2 \end{cases}.$$

Then $\text{sgn}(\sigma) = \text{sgn}(\sigma_1)\text{sgn}(\sigma_2)$.

(5) If $\sigma = (b_1 c_1) \cdots (b_r c_r)$ then $\varepsilon(\sigma) = (-1)^r$.

Proof. Let $A_\tau = \{(i, j) | 1 \leq i < j \leq n \text{ and } \tau(i) < \tau(j)\}$, and $B_\tau = \{(i, j) | 1 \leq i < j \leq n \text{ and } \tau(i) > \tau(j)\}$. Since τ is one to one we see that $A_\tau \cup B_\tau = \{(i, j) | 1 \leq i < j \leq n\}$. Thus

$$\prod_{1 \leq i < j \leq n} (x_{\tau(i)} - x_{\tau(j)}) = \prod_{(i, j) \in A_\tau} (x_{\tau(i)} - x_{\tau(j)}) \prod_{(i, j) \in B_\tau} (x_{\tau(i)} - x_{\tau(j)}).$$

Thus

$$\prod_{1 \leq i < j \leq n} (x_{\tau(i)} - x_{\tau(j)}) = (-1)^{|B_\tau|} \prod_{(i, j) \in A_\tau} (x_{\tau(i)} - x_{\tau(j)}) \prod_{(i, j) \in B_\tau} (x_{\tau(j)} - x_{\tau(i)}).$$

We now note that

$$\prod_{(i, j) \in A_\tau} (x_{\tau(i)} - x_{\tau(j)}) \prod_{(i, j) \in B_\tau} (x_{\tau(j)} - x_{\tau(i)}) = \Delta(x_1, \dots, x_n).$$

This proves 1 with $\varepsilon(\tau) = (-1)^{|B_\tau|}$.

We will now prove 2. We have $a_{\tau(i)} = \sigma(a_i)$. Now $a_{\tau\zeta(i)} = \sigma(a_{\zeta(i)}) = \sigma(\mu(a_i))$. We have

$$\begin{aligned} \prod_{1 \leq i < j \leq n} (x_{\tau\zeta(i)} - x_{\tau\zeta(j)}) &= \prod_{(i, j) \in A_\zeta} (x_{\tau\zeta(i)} - x_{\tau\zeta(j)}) \prod_{(i, j) \in B_\zeta} (x_{\tau\zeta(i)} - x_{\tau\zeta(j)}) \\ &= (-1)^{|B_\zeta|} \prod_{(i, j) \in A_\zeta} (x_{\tau\zeta(i)} - x_{\tau\zeta(j)}) \prod_{(i, j) \in B_\zeta} (x_{\tau\zeta(j)} - x_{\tau\zeta(i)}) \\ &= \varepsilon(\zeta) \prod_{1 \leq i < j \leq n} (x_{\tau(i)} - x_{\tau(j)}) = \varepsilon(\zeta)\varepsilon(\tau)\Delta(x_1, \dots, x_n). \end{aligned}$$

This implies that $\varepsilon(\tau\zeta) = \varepsilon(\tau)\varepsilon(\zeta)$ proving 2.

We will now prove 3. For this we note that $b_i = a_{\zeta(i)}$ with ζ a permutation of $\{1, \dots, n\}$. Thus

$$\sigma(b_i) = \sigma(a_{\zeta(i)}) = a_{\tau(\zeta(i))} = b_{\zeta^{-1}(\tau(\zeta(i)))}.$$

Thus $\nu(i) = \zeta^{-1}\tau\zeta(i)$. Since $\varepsilon(\zeta^{-1}\zeta) = \varepsilon(I) = 1$, we have

$$\varepsilon(\nu) = \varepsilon(\zeta^{-1})\varepsilon(\tau)\varepsilon(\zeta) = \varepsilon(\zeta^{-1})\varepsilon(\zeta)\varepsilon(\tau) = \varepsilon(\tau).$$

To prove (4) we enumerate S by writing $S_1 = \{a_1, \dots, a_r\}$ and $S_2 = \{a_{r+1}, \dots, a_{r+s}\}$ with $r + s = n$. Then $\sigma_1(a_i) = a_{\tau(i)}$ for $i = 1, \dots, r$ with τ a permutation of $\{1, \dots, r\}$ and $\sigma_2(a_{r+j}) = a_{r+\nu(j)}$ with ν a permutation of $1, \dots, s$. Then if ζ is defined by

$$\zeta(j) = \begin{cases} \tau(x) & \text{if } 1 \leq x \leq r \\ \nu(x - r) & \text{if } r < x \leq n \end{cases}.$$

$$\begin{aligned} \text{sgn}(\sigma) \prod_{1 \leq i < j \leq n} (x_i - x_j) &= \prod_{1 \leq i < j \leq n} (x_{\zeta(i)} - x_{\zeta(j)}) = \\ \prod_{1 \leq i < j \leq r} (x_{\tau(i)} - x_{\tau(j)}) &\prod_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} (x_{\tau(i)} - x_{r+\nu(j)}) \prod_{1 \leq i < j \leq s} (x_{r+\nu(i)} - x_{r+\nu(j)}). \end{aligned}$$

The middle factor is just

$$\prod_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} (x_i - x_{r+j}).$$

The left most factor is

$$\varepsilon(\tau) \prod_{1 \leq i < j \leq r} (x_i - x_j)$$

and the right most is

$$\varepsilon(\nu) \prod_{1 \leq i < j \leq s} (x_{r+i} - x_{r+j}).$$

Thus $\text{sgn}(\sigma) = \varepsilon(\tau)\varepsilon(\nu) = \text{sgn}(\sigma_1)\text{sgn}(\sigma_2)$.

To prove (5) in light of 2. we need only show that if $a, b \in S$ and $a \neq b$ then $\text{sgn}((ab)) = -1$. Let $S_1 = \{a, b\}$ and $S_2 = S - \{a, b\}$ then (ab) is given as in (4) with $\sigma_1 = (ab)|_{S_1}$ and σ_2 the identity map on S_2 . The result now follows since $(x_2 - x_1) = -(x_1 - x_2)$. ■

Definition 3 We will call $sgn(\sigma)$ the sign of the permutation σ .

We will now look at the example above with σ given by

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & \\ 3 & 1 & 5 & 2 & 4 & \end{array}$$

we have seen that $\sigma = (13)(23)(35)(45)$ so $sgn(\sigma) = 1$ by (3) in the previous theorem. Note that the method of proof (1),(2) of the above theorem gives another method. It indicates that we should count the pairs $i < j$ such that the corresponding elements are in the reverse order. This means that we can read from left to right in the second row and in this example note that $3 > 1$, $3 > 2$, $5 > 2$ and $5 > 4$. all other pairs are left in increasing order. Thus the method of the proof gives an alternate determination that $sgn(\sigma) = 1$.

Definition 4 If

$$\begin{array}{cccccc} 1 & 2 & \dots & j & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(j) & \dots & \sigma(n) \end{array}$$

is a permutation and $\sigma(i) > \sigma(j)$ with $i < j$ then the pair $\sigma(i), \sigma(j)$ is called a descent. If N is the number of descents then $sgn(\sigma) = (-1)^N$. In the next section we will need a few calculations of signs of permutations.

Lemma 5 Let $\sigma(i) = i + 1$ for $1 \leq i \leq n - 1$ and $\sigma(n) = 1$. Then $sgn(\sigma) = (-1)^{n-1}$.

Proof. Here we are looking at

$$\begin{array}{cccccc} 1 & 2 & \dots & j & \dots & n-1 & n \\ 2 & 3 & \dots & j+1 & \dots & n & 1 \end{array}$$

we note that the descents are exactly $(2, 1), (3, 1), \dots, (n, 1)$ and thus there are exactly $n - 1$ descents. ■

Lemma 6 Assume that $n = 2k$ consider σ given by

$$\begin{array}{cccccccc} 1 & 2 & \dots & k & k+1 & k+2 & \dots & 2k-1 & 2k \\ 2 & 4 & \dots & 2k & 1 & 3 & \dots & 2k-3 & 2k-1 \end{array}$$

Then $\text{sgn}(\sigma) = (-1)^{\frac{k(k+1)}{2}}$.

Proof. The descents are

$$(2, 1), (4, 1), (4, 3), (6, 1), (6, 3), (6, 5), \dots, (2k, 1), (2k, 3), \dots, (2k, 2k - 1).$$

If we count them up we get $1 + 2 + \dots + k = \frac{k(k+1)}{2}$. Thus $\text{sgn}(\sigma) = (-1)^{\frac{k(k+1)}{2}}$ as asserted. ■

2. The Legendre symbol and permutations.

In this section p will denote an odd prime. Let F_p be the field $\mathbb{Z}/p\mathbb{Z} = \{1, 2, \dots, p - 1\}$, as usual. If $a \in F_p - \{0\}$ then we consider the elements $\{a \cdot 1, a \cdot 2, \dots, a \cdot (p - 1)\}$ then since $a \neq 0$ this defines a permutation σ_a of $F_p - \{0\}$. We note that $\sigma_{ab} = \sigma_a \sigma_b$ for $a, b \in F_p - \{0\}$. Our key observation is

Lemma 7 *If $a \in F_p - \{0\}$ then $\left(\frac{a}{p}\right) = \text{sgn}(\sigma_a)$.*

Proof. Let $\zeta \in F_p - \{0\}$ be a primitive element. Then $F_p - \{0\} = \{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$. We write $a_i = \zeta^{i-1}$ for $i = 1, \dots, p - 1$. Then with this enumeration σ_ζ corresponds to the permutation

$$\begin{array}{cccccccc} 1 & 2 & \dots & j & \dots & p-2 & p-1 \\ 2 & 3 & \dots & j+1 & \dots & p-1 & 1 \end{array}$$

which, by Lemma 5, has sign $(-1)^{(p-1)-1} = (-1)^{p-2} = -1$ since p is odd. We now note that if $a \in F_p - \{0\}$ then $a = \zeta^j$ with $0 \leq j \leq p - 2$. Thus $\text{sgn}(\sigma_a) = \text{sgn}(\sigma_{\zeta^j}) = \text{sgn}(\sigma_\zeta)^j = (-1)^j$. We have seen in supplement 3 that $(-1)^j = \left(\frac{a}{p}\right)$. ■

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

Proof. We note that $\sigma_2 i = 2i$ for $i \leq \frac{p-1}{2}$. Also

$$2\left(\frac{p-1}{2} + j\right) = p - 1 + 2j = p + (2j - 1).$$

Thus $2(\frac{p-1}{2} + j) \equiv 2j - 1 \pmod{p}$ for $j = 1, \dots, \frac{p-1}{2}$. This implies that if $k = \frac{p-1}{2}$ then σ_2 is given by

$$\begin{array}{cccccccc} 1 & 2 & \dots & k & k+1 & k+2 & \dots & 2k-1 & 2k \\ 2 & 4 & \dots & 2k & 1 & 3 & \dots & 2k-3 & 2k-1 \end{array}$$

and so Lemma 6 implies that $\text{sgn}(\sigma_2) = (-1)^{\frac{k(k+1)}{2}}$. Now $k = \frac{p-1}{2}$ and $k+1 = \frac{p+1}{2}$ hence $\frac{k(k+1)}{2} = \frac{(\frac{p-1}{2})(\frac{p+1}{2})}{2}$ which is $\frac{p^2-1}{8}$. The corollary now follows from Lemma 7. ■

Our next result is usually called Gauss' Lemma. He proved it as part of his third proof of the law of quadratic reciprocity.

Lemma 9 *Let $a \in \mathbb{Z}$ be such that $p \nmid a$. Let N be the number of elements $j \in (1, 2, \dots, \frac{p-1}{2})$ such that $aj \equiv r \pmod{p}$ with $\frac{p-1}{2} < r \leq p-1$. Then $\left(\frac{a}{p}\right) = (-1)^N$.*

Proof. Let b be the element of F_p corresponding to a . We write out the minimal positive residues mod p as

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

if we reduce modulo p then we can write out $F_p - \{0\}$ as

$$1, 2, \dots, \frac{p-1}{2}, -1, -2, \dots, -\frac{p-1}{2}.$$

Now if $1 \leq i \leq \frac{p-1}{2}$ and $bi \equiv u_i \pmod{p}$ which we take to be in the range $1 \leq u_i \leq p-1$. We note that $b(-i) \equiv -u_i \pmod{p}$. We define v_i as follows. If $1 \leq u_i \leq \frac{p-1}{2}$ then $v_i = u_i$. If $\frac{p-1}{2} < u_i < p$ then we define v_i by $u_i \equiv -v_i \pmod{p}$ with $1 \leq v_i \leq \frac{p-1}{2}$. Then if $\sigma_b(i) = v_i$ then $\sigma_b(-i) = -v_i$ and if $\sigma_b(i) = -v_i$ then $\sigma_b(-i) = v_i$. Thus if T is the set of $1 \leq i \leq \frac{p-1}{2}$ and $\frac{p-1}{2} < u_i < p$ then if $i \in T$ then $\sigma_b(i) = -v_i$. Assume that $T = \{j_1, \dots, j_N\}$. We multiply σ_b by the product of N transpositions that interchange v_i and $-v_i$ for $i \in T$

$$(v_{j_1}(-v_{j_1})) \cdots (v_{j_N}(-v_{j_N}))\sigma_b$$

and get the permutation μ

$$\begin{array}{cccccccc} 1 & 2 & \dots & \frac{p-1}{2} & -1 & -2 & \dots & -\frac{p-1}{2} \\ v_1 & v_2 & \dots & v_{\frac{p-1}{2}} & -v_1 & -v_2 & \dots & -v_{\frac{p-1}{2}} \end{array}$$

this permutation has sign equal to 1 by 4. in Theorem 2 since if we write $S_1 = \{1, 2, \dots, \frac{p-1}{2}\}$ and $S_2 = \{-1, \dots, -\frac{p-1}{2}\}$ then if we label S_2 by $a_1 = -1, a_2 = -2, \dots, a_{\frac{p-1}{2}} = -\frac{p-1}{2}$ then we see that μ is of the form of 4. in Theorem 2 with the same permutation on both parts. Thus

$$\text{sgn}(\sigma_b) = \text{sgn}((v_{j_1}(-v_{j_1})) \cdots (v_{j_N}(-v_{j_N}))) = (-1)^N$$

by part 3 of Theorem 2. ■

Here is an example of the method of proof of the above lemma. We assume that $p = 7$ we take $b = 3$. Then the multiples are 3, 6, 9 - 3, -6, -9 if we reduce modulo 7 we have 3, 6, 2, -3, -6, -2 now if we replace the elements larger than $\frac{p-1}{2} = 3$ by a negative residue we replace 6 by -1 thus we get

$$\begin{array}{cccccc} 1 & 2 & 3 & -1 & -2 & -3 \\ 3 & -1 & 2 & -3 & 1 & -2 \end{array}$$

If we multiply this by the transposition of 1 and -1 we have

$$\begin{array}{cccccc} 1 & 2 & 3 & -1 & -2 & -3 \\ 3 & 1 & 2 & -3 & -1 & -2 \end{array}$$

We now have 3 definitions of the Legendre symbol we will now give a fourth. For this we need a new notation: if a is a real number then we set $[a] = \max\{j \in \mathbb{Z} | j \leq a\}$. Thus $[\frac{25}{4}] = 6$.

Lemma 10 *If $a \in \mathbb{Z}$ and $p \nmid a$ set*

$$U(a, p) = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ai}{p} \right].$$

Then $\left(\frac{a}{p}\right) = (-1)^{U(a,p)} (-1)^{\frac{p^2-1}{8}(a-1)}$. In particular, if a is odd then $\left(\frac{a}{p}\right) = (-1)^{U(a,p)}$.

Proof. We note that the division algorithm can be rephrased as

$$ja = \left[\frac{ja}{p} \right] p + r_j$$

with $0 \leq r_j < p$. If $1 \leq j \leq \frac{p-1}{2}$ then $r_j \neq 0$. since p doesn't divide j or a . Let $T = \{j | \frac{p-1}{2} < r_j < p\}$. Then if $j \in T$ we can write $r_j = p - s_j$ with $1 \leq s_j \leq \frac{p-1}{2}$. We therefore see that

$$\sum_{j=1}^{\frac{p-1}{2}} ja = p \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ai}{p} \right] + \sum_{j \notin T} r_j + p|T| - \sum_{j \in T} s_j.$$

Now the set of elements $\{r_j | j \notin T\} \cup \{s_j | j \in T\} = \{1, 2, \dots, \frac{p-1}{2}\}$. Thus

$$\sum_{j \notin T} r_j - \sum_{j \in T} s_j = \sum_{j=1}^{\frac{p-1}{2}} j - 2 \sum_{j \in T} s_j.$$

If we observe that $\sum_{j=1}^{\frac{p-1}{2}} j = \frac{p-1}{2} \frac{p+1}{2}$ then we have

$$\frac{p^2 - 1}{8}(a - 1) = p \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ai}{p} \right] + p|T| - 2 \sum_{j \in T} s_j.$$

If we consider this equation modulo 2 taking account of the fact that $p \equiv 1 \pmod{2}$ we have $\frac{p^2-1}{8}(a-1) \equiv \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ai}{p} \right] + |T| \pmod{2}$. This implies that $|T| + \frac{p^2-1}{8}(a-1) \equiv U(a, p) \pmod{2}$. Thus by Gauss' Lemma (Lemma 9) we have

$$\left(\frac{a}{p} \right) (-1)^{\frac{p^2-1}{8}(a-1)} = (-1)^{|T|} (-1)^{\frac{p^2-1}{8}(a-1)} = (-1)^{U(a, p)}.$$

■

Quadratic Reciprocity.

We are finally ready to state and prove the Law of Quadratic Reciprocity. This theorem is usually attributed to Gauss who gave the first proof of the theorem and in the course of his life gave 7 proofs. However, both Legendre and Euler had thought that the "law" was very probable and each gave at least one incorrect proof.

Theorem 11 *Let p and q be distinct odd primes then*

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

Proof. We consider the set S of all pairs (i, j) with $1 \leq i \leq \frac{p-1}{2}$ and $1 \leq j \leq \frac{q-1}{2}$. If $(i, j) \in S$ we assert that $qi \neq pj$. Since if $qi = pj$ then since $p \neq q$ the equality would imply that $q|j$ but j is not 0 and is too small. Thus if $(i, j) \in S$ then $qi \neq pj$. Let $A = \{(i, j) \in S | qi > pj\}$ and $B = \{(i, j) \in S | qi < pj\}$ then S is the disjoint union of A and B . We will now count the number of elements of A . We count the number with first coordinate i . If $(i, j) \in A$ then $qi > pj$. This implies that $\frac{qi}{p} > j$. Thus $\left[\frac{qi}{p}\right] \geq j \geq 1$ and since $\frac{qi}{p} > \left[\frac{qi}{p}\right]$ we see that every such j appears. Hence the number of elements of A with first coordinate i is $\left[\frac{qi}{p}\right]$. Hence the number of elements in A is

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{qi}{p}\right] = U(q, p)$$

(see Lemma 10). The same argument implies that the number of elements in B is $U(p, q)$. But S has $\frac{p-1}{2} \frac{q-1}{2}$ elements. Hence

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

The result now follows since $(-1)^{U(p,q)} = \left(\frac{p}{q}\right)$ and $(-1)^{U(q,p)} = \left(\frac{q}{p}\right)$. ■

We will now show how one can use this result as a powerful tool for the computation of Legendre symbols. Consider,

$$\left(\frac{11}{131}\right) = (-1)^{5 \cdot 65} \left(\frac{131}{11}\right) = - \left(\frac{10}{11}\right) = - \left(\frac{2}{11}\right) \left(\frac{5}{11}\right) = -(-1)^{\frac{121-1}{8}} \left(\frac{5}{11}\right)$$

by Corollary 8. But $120 = 15 \cdot 8$ so we have

$$\left(\frac{11}{131}\right) = \left(\frac{5}{11}\right) = (-1)^{2 \cdot 5} \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1.$$

Thus 11 is a square in F_{131} .

Exercises.

1. Write the permutation

$$\begin{array}{ccccccc} 1 & 2 & 3 & \dots & n-2 & n-1 & n \\ 2 & 3 & 4 & \dots & n-1 & n & 1 \end{array}$$

as a product of transpositions.

2. Prove that if S has $1 \leq n < \infty$ elements then the number of permutations of S is $n!$. Use this to prove that if $n \geq 2$ then $n^n > n!$. (Hint. How many functions are there from S to S ?)

3. Compute the sign of the following permutation by counting the descents and by writing it as a product of transpositions

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 6 & 8 & 2 & 4 & 1 & 5 \end{array}$$

4. What is the sign of the permutation

$$\begin{array}{cccccccc} 1 & 2 & \dots & k & k+1 & k+2 & \dots & 2k \\ 1 & 3 & \dots & 2k-1 & 2 & 4 & \dots & 2k \end{array}$$

5. Let q be an odd prime. Show that 2 is a quadratic residue modulo q if and only if $q = 8l \pm 1$.

6. Let p, q be odd primes. Show that if $q|(2^p - 1)$ then $p|(q-1)$ and $q = 8l \pm 1$ for some integer l . (Hint: Is 2 a quadratic residue mod q ?)

7. Calculate the following Legendre symbols:

a) $\left(\frac{31}{641}\right)$. b) $\left(\frac{7}{79}\right)$. c) $\left(\frac{105}{1009}\right)$.

8. Let p be an odd prime. Let $a, b, c \in F_p$ with $a \neq 0$ and let $f(t) = at^2 + bt + c$ then f has a root in F_p if and only if $\left(\frac{a^2 - 4bc}{p}\right) \neq -1$. How many roots does $f(t)$ have in F_p if $\left(\frac{a^2 - 4bc}{p}\right) = 1$?

9. Let p be an odd prime show that the smallest positive integer that is not a square modulo p is a prime.

10. Prove that if p is an odd prime with $p > 3$ then the congruence $x^2 \equiv 3 \pmod{p}$ has a solution if and only if $p \equiv \pm 1 \pmod{3}$. Show that if p is a prime such that $p \equiv \pm 1 \pmod{3}$ and $p \equiv -1 \pmod{4}$ then two solutions to

$$x^2 \equiv 3 \pmod{p}$$

are $\pm 3^{\frac{p+1}{4}}$.

11. Use Lemma 10 to calculate $\left(\frac{2}{p}\right)$ for p an odd prime.

12. Derive the first part of problem 10 above from Lemma 10.

13. A Fermat prime is a prime $q = 2^r + 1$ with r a positive integer. Use the law of quadratic reciprocity to show that if $q = 2^r + 1$ is an odd prime then r must be even and $\left(\frac{3}{q}\right) = -1$.

The Jacobi symbol

As it turns out the arguments in the previous two sections on the Legendre symbol work equally well for the (more general) Jacobi symbol. We will describe the modifications in this section. Let $b \in \mathbb{Z}$ be an odd number with $b > 1$. We will set $R_b = \mathbb{Z}/b\mathbb{Z}$. If $a \in \mathbb{Z}$ and $\gcd(a, b) = 1$ we note that multiplication by a defines a permutation of $R_b - \{0\}$ which we denote by $\sigma_{a,b}$. Then we define the Jacobi symbol $\left(\frac{a}{b}\right) = \text{sgn}(\sigma_{a,b})$. If $b = 1$ we set $\left(\frac{a}{1}\right) = 1$ and if $\gcd(a, b) \neq 1$ then set $\left(\frac{a}{b}\right) = 0$. Lemma 7 implies that if b is a prime then the Jacobi symbol agrees with the Legendre symbol.

Lemma 12 *The if $a \equiv a' \pmod{b}$ then Jacobi symbol $\left(\frac{a}{b}\right) = \left(\frac{a'}{b}\right)$. If b is positive and odd then*

$$\left(\frac{a_1}{b}\right) \left(\frac{a_2}{b}\right) = \left(\frac{a_1 a_2}{b}\right).$$

Proof. The first assertion is a direct consequence of the definition. If $b = 1$ or if any one of the terms in the asserted equality is 0 then the equality is obviously true. In all the other cases $b > 1$ and $\gcd(a_1, b) = \gcd(a_2, b) = 1$ and the result follows from $\sigma_{a_1, b} \sigma_{a_2, b} = \sigma_{a_1 a_2, b}$. ■

Theorem 13 *If $b \in \mathbb{Z}_{>0}$ is odd then $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.*

Proof. We may assume that $b > 1$. The proof is exactly the same as that of Corollary 8 with σ_2 replaced by $\sigma_{2,b}$, p replaced by b , $k = \frac{b-1}{2}$ and Lemma 7 replaced by the definition of the Jacobi symbol. ■

Lemma 14 *Let b be odd and $b > 1$ and let $a \in \mathbb{Z}$ be such that $\gcd(a, b) = 1$. Let N be the number of elements $j \in (1, 2, \dots, \frac{b-1}{2})$ such that $aj \equiv r \pmod{b}$ with $\frac{b-1}{2} < r \leq b-1$. Then $\left(\frac{a}{b}\right) = (-1)^N$.*

Proof. The proof is the same as that of Lemma 9 however since the notation in that proof overlaps that in the above statement we will give the details. We write out the minimal positive residues mod b as

$$1, 2, \dots, \frac{b-1}{2}, b-1, b-2, \dots, b - \frac{b-1}{2}$$

if we reduce modulo b then we can write out $R_b - \{0\}$ as

$$1, 2, \dots, \frac{b-1}{2}, -1, -2, \dots, -\frac{b-1}{2}.$$

Now if $1 \leq i \leq \frac{b-1}{2}$ and $ai \equiv u_i \pmod{b}$ which we take to be in the range $1 \leq u_i \leq b-1$. We note that $a(-i) \equiv -u_i \pmod{b}$. We define v_i as follows. If $1 \leq u_i \leq \frac{b-1}{2}$ then $v_i = u_i$. If $\frac{b-1}{2} < u_i < b$ then we define v_i by $u_i \equiv -v_i \pmod{b}$ with $1 \leq v_i \leq \frac{b-1}{2}$. Then if $\sigma_{a,b}(i) = v_i$ then $\sigma_{a,b}(-i) = -v_i$ and if $\sigma_{a,b}(i) = -v_i$ then $\sigma_{a,b}(-i) = v_i$. Thus if T is the set of $1 \leq i \leq \frac{b-1}{2}$ and $\frac{b-1}{2} < u_i < b$ then if $i \in T$ then $\sigma_{a,b}(i) = -v_i$. Assume that $T = \{j_1, \dots, j_N\}$. We multiply $\sigma_{a,b}$ by the product of N transpositions, $(v_i(-v_i))$ that interchange v_i and $-v_i$ for $i \in T$

$$(v_{j_1}(-v_{j_1})) \cdots (v_{j_N}(-v_{j_N}))\sigma_b$$

and get the permutation μ given by

$$\begin{array}{cccccccc} 1 & 2 & \dots & \frac{b-1}{2} & -1 & -2 & \dots & -\frac{b-1}{2} \\ v_1 & v_2 & \dots & v_{\frac{b-1}{2}} & -v_1 & -v_2 & \dots & -v_{\frac{b-1}{2}} \end{array}$$

this permutation has sign equal to 1 by (4) in Theorem 2 since if we write $S_1 = \{1, 2, \dots, \frac{b-1}{2}\}$ and $S_2 = \{-1, \dots, -\frac{b-1}{2}\}$ then if we label S_2 by $a_1 = -1, a_2 = -2, \dots, a_{\frac{b-1}{2}} = -\frac{b-1}{2}$ then we see that μ is of the form of (4) in Theorem 2 with the same permutation on both parts. Thus

$$\text{sgn}(\sigma_{a,b}) = \text{sgn}((v_{j_1}(-v_{j_1})) \cdots (v_{j_N}(-v_{j_N}))) = (-1)^N$$

by part (3) of Theorem 2. ■

We also have

Lemma 15 *If b is odd and $b > 1$ and if $a \in \mathbb{Z}_{>0}$ and $\gcd(a, b) = 1$ set*

$$U(a, b) = \sum_{i=1}^{\frac{b-1}{2}} \left[\frac{ai}{b} \right]$$

then $\left(\frac{a}{b}\right) = (-1)^{U(a,b)}(-1)^{(a-1)\frac{b^2-1}{8}}$. In particular, if a is odd then $\left(\frac{a}{b}\right) = (-1)^{U(a,b)}$.

Proof. As above the proof of this result is essentially the same as that of Lemma 10 if we replace p by b . We will go through the argument since the steps are the same but some of the justifications are different. We note that the division algorithm can be rephrased as

$$ja = \left[\frac{ja}{b} \right] b + r_j$$

with $0 \leq j < b$. If $1 \leq j \leq \frac{b-1}{2}$ then $r_j \neq 0$. since $\gcd(a, b) = 1$ and j is too small for b to divide it. Let $T = \{j | \frac{b-1}{2} < r_j < b\}$. Then if $j \in T$ we can write $r_j = b - s_j$ with $1 \leq s_j \leq \frac{b-1}{2}$. We note that

$$\sum_{j=1}^{\frac{b-1}{2}} j = \frac{\frac{b-1}{2}(\frac{b-1}{2} + 1)}{2} = \frac{b^2 - 1}{8}.$$

$$\sum_{j=1}^{\frac{b-1}{2}} ja = b \sum_{i=1}^{\frac{b-1}{2}} \left[\frac{ai}{b} \right] + \sum_{j \notin T} r_j + b|T| - \sum_{j \in T} s_j.$$

Now the set of elements $\{r_j | j \notin T\} \cup \{s_j | j \in T\} = \{1, 2, \dots, \frac{b-1}{2}\}$. Thus

$$\sum_{j \notin T} r_j - \sum_{j \in T} s_j = \sum_{j=1}^{\frac{b-1}{2}} j - 2 \sum_{j \in T} s_j = \frac{b^2 - 1}{8} - 2 \sum_{j \in T} s_j.$$

Also $\sum_{j=1}^{\frac{b-1}{2}} ja = a \sum_{j=1}^{\frac{b-1}{2}} j = a \frac{b^2-1}{8}$ thus.

$$\frac{b^2 - 1}{8}(a - 1) = b \sum_{i=1}^{\frac{b-1}{2}} \left[\frac{ai}{b} \right] + b|T| - 2 \sum_{j \in T} s_j.$$

If we consider this equation modulo 2 taking account of the fact that $b \equiv 1 \pmod{2}$ we have $\frac{b^2-1}{8}(a-1) \equiv \sum_{i=1}^{\frac{b-1}{2}} \left[\frac{ai}{b} \right] + |T| \pmod{2}$. This implies that $|T| + \frac{b^2-1}{8}(a-1) \equiv U(a, b) \pmod{2}$. Thus by Lemma 14 we have

$$\left(\frac{a}{b} \right) (-1)^{\frac{b^2-1}{8}(a-1)} = (-1)^{|T|} (-1)^{\frac{b^2-1}{8}(a-1)} = (-1)^{U(a, b)}.$$

■

Finally we have the reciprocity theorem.

Theorem 16 *Let a and b be odd numbers such that $\gcd(a, b) = 1$ with $a, b > 1$ then*

$$\left(\frac{a}{b} \right) \left(\frac{b}{a} \right) = (-1)^{\frac{a-1}{2} \frac{b-1}{2}}.$$

Proof. The proof is essentially the same as that of Theorem 11 we will give the details since the change in notation could be confusing. We consider the set S of all pairs (i, j) with $1 \leq i \leq \frac{a-1}{2}$ and $1 \leq j \leq \frac{b-1}{2}$. If $(i, j) \in S$ we assert that $bi \neq aj$. Since if $ai = bj$ then since $\gcd(a, b) = 1$ the equality would imply that $a|j$ but j is not 0 and is too small. Thus if $(i, j) \in S$ then $bi \neq aj$. Let $A = \{(i, j) \in S | bi > aj\}$ and $B = \{(i, j) \in S | bi < aj\}$ then S is the disjoint union of A and B . We will now count the number of elements of A by counting the number with first coordinate i . If $(i, j) \in A$ then $bi > aj$. This implies that $\frac{bi}{a} > j$. Thus $\lceil \frac{bi}{a} \rceil \geq j \geq 1$ and since $\frac{bi}{a} > \lceil \frac{bi}{a} \rceil$ (since $a \nmid (bi)$). we see that every such j appears. Hence the number of elements of A with first coordinate i is $\lceil \frac{bi}{a} \rceil$. Hence the number of elements in A is $\sum_{i=1}^{\frac{a-1}{2}} \lceil \frac{bi}{a} \rceil = U(b, a)$. The same argument implies that the number of elements in B is $U(a, b)$. But S has $\frac{a-1}{2} \frac{b-1}{2}$ elements. Hence

$$(-1)^{U(a,b)} (-1)^{U(b,a)} = (-1)^{\frac{a-1}{2} \frac{b-1}{2}}.$$

The result now follows since $(-1)^{U(a,b)} = \left(\frac{a}{b}\right)$ and $(-1)^{U(b,a)} = \left(\frac{b}{a}\right)$. ■

This theorem implies that our definition of the Jacobi symbol is equivalent to the standard one (see Rose, pp.71-72 and do Exercise 17). The above reciprocity law allows us to compute Legendre symbols without prime factorization (except for the highest power of 2 which is obvious if we write out numbers base 2). Here is an example. You can check that 7919 and 8387 are primes. Thus we have

$$\begin{aligned} \left(\frac{8387}{7919}\right) &= \left(\frac{468}{7919}\right) = \left(\frac{2^2 \cdot 117}{7919}\right) = \left(\frac{2}{7919}\right)^2 \left(\frac{117}{7919}\right) \\ &= \left(\frac{117}{7919}\right) = \left(\frac{7919}{117}\right) = \left(\frac{80}{117}\right) = \left(\frac{2^4}{117}\right) \left(\frac{5}{117}\right) = \left(\frac{5}{117}\right) \\ &= \left(\frac{117}{5}\right) = \left(\frac{2}{5}\right) = -1. \end{aligned}$$

Exercises.

14. Write out the details of the proof of Theorem 12.
15. Calculate the following Legendre symbols using the Jacobi symbol.
 - a) $\left(\frac{2357}{5279}\right)$.

b) $\left(\frac{3181}{6133}\right)$.

16. Why is it a good idea to write numbers in base 2 in the calculation of Jacobi symbols?

17. Show (using the theorems above) that our definition of the Jacobi symbol is equivalent with that in Rose.