Quadratic Reciprocity

The law of quadratic reciprocity can be proved in many ways. We give here a somewhat unusual proof, due to Conway, after Scholz.

The Legendre symbol $\left(\frac{a}{p}\right)$ is a special case of the Jacobi symbol $\left(\frac{a}{n}\right)$. We consider also the *Zolotarev symbol* $\left(\frac{a}{n}\right)$. Eventually we shall find that the Jacobi symbol and Zolotarev symbol are the same, but in the short term we add subscripts L, J, or Z, to make clear in which sense the symbol is meant.

If $(a, n) = 1$ and n is odd, then the *Zolotarev symbol* is defined to be the sign of the permutation $x \mapsto ax$ on a complete system of residues modulo n. For example, the permutation $x \mapsto 7x \pmod{15}$ has the cycle structure (0)(1 7 4 13)(2 14 8 11)(3 6 12 9)(5)(10); hence $\left(\frac{7}{15}\right)_Z = -1$.

Lemma 1. *If* $(a, p) = 1$ *and* p *is prime, then* $\left(\frac{a}{p}\right)_Z = \left(\frac{a}{p}\right)_L$.

Proof. Let h be the order of a modulo p. The cycle decomposition of the permutation $x \mapsto ax \pmod{p}$ consists of one 1-cycle (0) together with $(p-1)/h$ cycles each of length h. Such a cycle has sign $(-1)^{h-1}$, so the permutation has sign $(-1)^{(h-1)(p-1)/h} = (-1)^{(p-1)/h}$. But $2 \mid (p-1)/h$ if and only if $h \mid (p-1)/2$, which is equivalent to saying that $a^{(p-1)/2} \equiv 1 \pmod{p}$. By Euler's criterion this is equivalent to a being a quadratic residue modulo p.

Lemma 2. *If* $a \equiv b \pmod{n}$, $n > 0$, $(a, n) = 1$, *then* $\left(\frac{a}{n}\right)_Z = \left(\frac{b}{n}\right)_Z$.

Proof. The permutation $x \mapsto ax \pmod{n}$ is indistinguishable from the permutation $x \mapsto bx \pmod{n}$.

Lemma 3. *If* n *is odd and* $n > 0$, *then*

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

The right hand side above can be expressed more concisely as $(-1)^{(n-1)/2}$.

Proof. Since n is assumed to be odd, the map $x \mapsto -x$ has one 1-cycle (0) and $(n-1)/2$ 2-cycles of the form $(x\ -x)$.

Lemma 4. *If* $(ab, n) = 1$ *and* $n > 0$, *then*

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

If g is a primitive root modulo p, then the permutation $x \mapsto gx \pmod{p}$ consists of one 1-cyle and one $p-1$ cycle. If $p > 2$ then $p-1$ is even, so the permutation is odd, which is to say that its sign is -1. In symbols, $\left(\frac{g}{p}\right)_Z = -1$. By the above it follows that $\left(\frac{g^k}{p}\right)_Z = (-1)^k$. This provides a second proof of Lemma 1.

Proof. The permutation $x \mapsto abx \pmod{n}$ is the composition of the permutation $x \mapsto ax \pmod{n}$ with the permutation $x \mapsto bx \pmod{n}$.

Lemma 5. *Suppose that* $(a, n) = 1$ *and that* n *is odd and positive. Let*

$$\mathcal{P} = \{1,\ 2,\ \ldots,\ (n-1)/2\}, \qquad \mathcal{N} = \{-1,\ -2,\ \ldots,\ -(n-1)/2\}.$$

Let K *be the number of* $k \in \mathcal{P}$ *such that* $ak \in \mathcal{N} \pmod{n}$*. Then*

$$\left(\frac{a}{n}\right)_Z = (-1)^K.$$

Proof. We call members of $\mathcal{P}$ 'positive', and members of $\mathcal{N}$ 'negative'. Let $\epsilon_k = 1$ if k and ak are both positive or both negative, and let $\epsilon_k = -1$ if one of k and ak is positive and the other negative. We note that $\epsilon_k = \epsilon_{-k}$. Let π^+ be the permutation that leaves members of $\mathcal{N}$ fixed, and that maps $\mathcal{P}$ to itself by the formula $k \mapsto \epsilon_k ak$. Let π^- be the permutation that leaves members of $\mathcal{P}$ fixed, and maps $\mathcal{N}$ to itself by the formula $k \mapsto \epsilon_k ak$. Finally, let π^* be the product of those transpositions $(ak, -ak)$ for which $k \in \mathcal{P}$ and $ak \in \mathcal{N}$. Then our permutation is $\pi^*\pi^+\pi^-$. The permutations π^+ and π^- are the same, except that they act on different sets. More precisely, if σ denotes the 'sign change permutation' $k \mapsto -k \pmod{n}$ then $\pi^- = \sigma\pi^+\sigma$. Thus π^+ and π^- are conjugate permutations. They have the same cycle structure, and hence the same parity. Consequently $\pi^+\pi^-$ is an even permutation. Since π^* is the product of K transpositions, we have the stated result.

For example, in the case of the permutation $x \mapsto 7x \pmod{15}$, we have

$$\begin{aligned}
\pi^+ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 6 & 2 & 5 & 3 & 4 \end{pmatrix} = (\ 1\ \ 7\ \ 4\ \ 2)(\ 3\ \ 6)(\ 5), \\
\pi^- &= \begin{pmatrix} -1 & -2 & -3 & -4 & -5 & -6 & -7 \\ -7 & -1 & -6 & -2 & -5 & -3 & -4 \end{pmatrix} = (-1\ -7\ -4\ -2)(-3\ -6)(-5), \\
\pi^* &= (1\ -1)(2\ -2)(3\ -3).
\end{aligned}$$

Lemma 6. *Suppose that* n *is odd, that* $n > 0$*, that* $(a, n) = 1$*, and that* $a > 0$*. Then*

$$\left(\frac{a}{n}\right)_Z = (-1)^K$$

where K *is the number of integers lying in the intervals* $((r - \frac{1}{2})\frac{n}{a}, \frac{rn}{a})$, $r = 1, 2, \ldots, [a/2]$.

Proof. Suppose that $1 \le k \le (n-1)/2$. If k lies in an interval of the form $(\frac{rn}{a}, (r + \frac{1}{2})\frac{n}{a})$ then $rn < ak < (r + \frac{1}{2})n$, which is to say that $ak \in \mathcal{P} \pmod{n}$. On the other hand, if $1 \le k \le (n-1)/2$ and k lies in an interval of the form $((r - \frac{1}{2})\frac{n}{a}, \frac{rn}{a})$ then $(r - \frac{1}{2})n < ak < rn$, which is to say that $ak \in \mathcal{N} \pmod{n}$. Thus the result follows from the preceding lemma.

Lemma 7. *If* $a > 0$, $(m, 2a) = 1$, $m > 0$, $n > 0$, *and* $m \equiv \pm n \pmod{4a}$, *then*

$$\left(\frac{a}{m}\right)_Z = \left(\frac{a}{n}\right)_Z.$$

Proof. We consider two cases.
Case 1. $m \equiv n \pmod{4a}$. Let $(a_r, b_r) = ((r - \frac{1}{2})\frac{m}{a}, \frac{rm}{a})$, and correspondingly put $(\alpha_r, \beta_r) = ((r - \frac{1}{2})\frac{n}{a}, \frac{rn}{a})$. Let t be the integer defined by the relation $n = m + 4at$, and put $\xi_r = b_r + (4r-2)t$. Thus $\alpha_r < \xi_r < \beta_r$. The interval (α_r, ξ_r) is just the interval (a_r, b_r), translated by the integral amount $(4r-2)t$. Hence these two intervals contain the same number of integers. On the other hand, $\beta_r - \xi_r = 2t$, an integer, so the interval (ξ_r, β_r) contains exactly $2t$ integers. Hence the number of integers in (α_r, β_r) is the number of integers in (a_r, b_r) plus $2t$. Thus the two numbers have the same parity, and the result follows by Lemma 6.
Case 2. $m \equiv -n \pmod{4a}$. Let (a_r, b_r) and (α_r, β_r) be defined as in the preceding case. Let t be an integer defined by the relation $m + n = 4at$, and set $\gamma_r = 4rt - (r - \frac{1}{2})\frac{m}{a}$. Thus $\alpha_r < \beta_r < \gamma_r$. Since $\alpha_r = (4r-2)t - (r - \frac{1}{2})\frac{m}{a} = \gamma_r - 2t$, the interval (α_r, γ_r) contains exactly $2t$ integers. The number of integers in (α_r, β_r) is therefore $2t$ minus the number of integers in the interval (β_r, γ_r). But the number of integers in this latter interval is the same as the number of integers in the interval

$$(-\gamma_r, -\beta_r) = ((r - \tfrac{1}{2})\frac{m}{a} - 4rt, \frac{rm}{a} - 4rt) = (a_r - 4rt, b_r - 4rt).$$

But this is just the interval (a_r, b_r), translated by the integral amount $-4rt$. Hence the number of integers in (a_r, b_r) plus the number of integers in (α_r, β_r) is $2t$. Hence the two counts have the same parity, so the result follows by Lemma 6.

Lemma 8. *If* n *is odd and positive, then*

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

It is sometimes convenient to write the right hand side above in the more compact form $(-1)^{(n^2-1)/8}$.

Proof. Clearly $\left(\frac{2}{1}\right)_Z = 1$. Also, the map $x \mapsto 2x \pmod 3$ has cycle decomposition $(0)(1\ 2)$, so $\left(\frac{2}{3}\right)_Z = -1$. By Lemma 7 it follows that $\left(\frac{2}{5}\right)_Z = \left(\frac{2}{3}\right)_Z = -1$ and that $\left(\frac{2}{7}\right)_Z = \left(\frac{2}{1}\right)_Z = 1$. Since n is odd, n is congruent modulo 8 to one of 1, 3, 5, or 7. Hence the result follows from Lemma 7.

Theorem 1. *If* m *and* n *are odd positive relatively prime integers, then*

$$\left(\frac{m}{n}\right)_Z \left(\frac{n}{m}\right)_Z = \begin{cases} -1 & \text{if } m \equiv n \equiv 3 \pmod{4}, \\ 1 & \text{otherwise.} \end{cases}$$

It is sometimes convenient to write the right hand side above in the form $(-1)^{\frac{m-1}{2}\,\frac{n-1}{2}}$.

Proof. We consider two cases.
Case 1. $m \equiv -n \pmod 4$. Then $m+n$ is a positive multiple of 4, say $m+n = 4a$. Hence

$$\begin{aligned}
\left(\frac{m}{n}\right)_Z &= \left(\frac{4a}{n}\right)_Z && \text{(by Lemma 2, since } m \equiv 4a \pmod n\text{)},\\
&= \left(\frac{a}{n}\right)_Z && \text{(by Lemma 4, since } \left(\tfrac{4}{n}\right)_Z = \left(\tfrac{2}{n}\right)_Z^2 = 1\text{)},\\
&= \left(\frac{a}{m}\right)_Z && \text{(by Lemma 7, since } m \equiv -n \pmod{4a}\text{)},\\
&= \left(\frac{4a}{m}\right)_Z && \text{(by Lemma 4, since } \left(\tfrac{4}{m}\right)_Z = \left(\tfrac{2}{m}\right)_Z^2 = 1\text{)},\\
&= \left(\frac{n}{m}\right)_Z && \text{(by Lemma 2, since } n \equiv 4a \pmod m\text{)}.
\end{aligned}$$

Case 2. $m \equiv n \pmod 4$. By exchanging m and n, if necessary, we may assume that $m \geq n$. If $m = n$ then by the hypothesis that m and n are relatively prime we deduce that $m = n = 1$. The identity is obviously true in this case. Otherwise $m > n$, and $m - n$ is a positive multiple of 4, say $m - n = 4a$. Then

$$\begin{aligned}
\left(\frac{m}{n}\right)_Z &= \left(\frac{4a}{n}\right)_Z && \text{(by Lemma 2, since } m \equiv 4a \pmod n\text{)},\\
&= \left(\frac{a}{n}\right)_Z && \text{(by Lemma 4, since } \left(\tfrac{4}{n}\right)_Z = \left(\tfrac{2}{n}\right)_Z^2 = 1\text{)},\\
&= \left(\frac{a}{m}\right)_Z && \text{(by Lemma 7, since } m \equiv n \pmod{4a}\text{)},\\
&= \left(\frac{4a}{m}\right)_Z && \text{(by Lemma 4, since } \left(\tfrac{4}{m}\right)_Z = \left(\tfrac{2}{m}\right)_Z^2 = 1\text{)},\\
&= \left(\frac{-n}{m}\right)_Z && \text{(by Lemma 2, since } 4a \equiv -n \pmod m\text{)},\\
&= \left(\frac{n}{m}\right)_Z (-1)^{(m-1)/2} && \text{(by Lemmas 3 and 4)}.
\end{aligned}$$

Theorem 2. *If* $m > 0$, $n > 0$, *and* $(2a, mn) = 1$, *then*

$$\left(\frac{a}{mn}\right)_Z = \left(\frac{a}{n}\right)_Z \left(\frac{a}{n}\right)_Z.$$

Suppose that n is odd, and write $n = p_1 p_2 \cdots p_r$. The Jacobi symbol is defined to be

$$\left(\frac{a}{n}\right)_J = \left(\frac{a}{p_1}\right)_L \left(\frac{a}{p_2}\right)_L \cdots \left(\frac{a}{p_r}\right)_L.$$

Thus by Lemma 1 and Theorem 2 it follows that

$$\left(\frac{a}{n}\right)_Z = \left(\frac{a}{n}\right)_J$$

whenever $(2a, n) = 1$ and $n > 0$.

Proof. We consider four cases.
Case 1. a is odd and positive. Then

$$\begin{aligned}\left(\frac{a}{mn}\right)_Z &= \left(\frac{mn}{a}\right)_Z(-1)^{\frac{a-1}{2}\frac{mn-1}{2}} && \text{(by Theorem 1)},\\ &= \left(\frac{m}{a}\right)_Z\left(\frac{n}{a}\right)_Z(-1)^{\frac{a-1}{2}\frac{mn-1}{2}} && \text{(by Lemma 4)},\\ &= \left(\frac{a}{m}\right)_Z\left(\frac{a}{n}\right)_Z(-1)^{\frac{a-1}{2}\frac{m-1}{2}}(-1)^{\frac{a-1}{2}\frac{n-1}{2}}(-1)^{\frac{a-1}{2}\frac{mn-1}{2}} && \text{(by Theorem 1)},\end{aligned}$$

and the result follows on noting that

$$\frac{a-1}{2}\frac{m-1}{2}+\frac{a-1}{2}\frac{n-1}{2}+\frac{a-1}{2}\frac{mn-1}{2}=\frac{a-1}{2}\Big(\frac{m+1}{2}\frac{n+1}{2}-1\Big)2$$

is an even integer.
Case 2. a is even and positive. Then $mn + a$ is odd, so we observe that

$$\begin{aligned}\left(\frac{a}{mn}\right)_Z &= \left(\frac{mn+a}{mn}\right)_Z && \text{(by Lemma 2)},\\ &= \left(\frac{mn+a}{m}\right)_Z\left(\frac{mn+a}{n}\right)_Z && \text{(by Case 1)},\\ &= \left(\frac{a}{m}\right)_Z\left(\frac{a}{n}\right)_Z && \text{(by Lemma 2)}.\end{aligned}$$

Case 3. $a = -1$.

$$\begin{aligned}\left(\frac{-1}{mn}\right)_Z &= (-1)^{\frac{mn-1}{2}} && \text{(by Lemma 3)},\\ &= \left(\frac{-1}{m}\right)_Z\left(\frac{-1}{n}\right)_Z(-1)^{\frac{mn-1}{2}+\frac{m-1}{2}+\frac{n-1}{2}} && \text{(by Lemma 3)}.\end{aligned}$$

But

$$\frac{mn-1}{2}+\frac{m-1}{2}+\frac{n-1}{2}=2\Big(\frac{m+1}{2}\frac{n+1}{2}-1\Big)$$

is an even integer, so we are done.
Case 4. $a < 0$. Then $-a > 0$, so by Cases 1 and 2,

$$\left(\frac{-a}{mn}\right)_Z=\left(\frac{-a}{m}\right)_Z\left(\frac{-a}{n}\right)_Z.$$

We combine this with the result of Case 3 to obtain the desired identity, by three applications of Lemma 4.

Quadratic Reciprocity

EXERCISES

1. Show that if $m > 0$, $n > 0$, $a < 0$, $(2a, m) = 1$, and $m \equiv n \pmod{4a}$, then $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$.

2. Show that if $m > 0$, $n > 0$, $a < 0$, $(2a, m) = 1$, and $m \equiv -n \pmod{4a}$, then $\left(\frac{a}{m}\right) = -\left(\frac{a}{n}\right)$.

3. Show that if $m > 0$, $n > 0$, $a \equiv 1 \pmod 4$, $(2a, mn) = 1$, and $m \equiv n \pmod a$, then $\left(\frac{a}{m}\right) = \left(\frac{a}{n}\right)$.

4. Suppose that $(a, m) = 1$ and that $m > 0$ is odd and bas at least two distinct prime factors. Show that the permutation $x \mapsto ax \pmod m$ of the reduced residue classes modulo m is always even.

***5.** Describe $\left(\frac{a}{n}\right)_Z$ when $(a, n) = 1$, $n > 0$, and n is even.