# Modular divisor functions and quadratic reciprocity

Richard Steiner

The ordinary divisor function $\tau$ is the function defined on positive integers as follows: $\tau(n)$ is the number of positive integer factors of $n$. It is well known that $n$ has an integer square root if and only if $\tau(n)$ is odd. Indeed, the factors less than $\sqrt{n}$ correspond to the factors greater than $\sqrt{n}$ under the transformation $i \mapsto n/i$, so that there is an even number of factors distinct from $\sqrt{n}$, and it follows that $\tau(n)$ is odd if and only if $\sqrt{n}$ is an integer. In this note we give a similar characterization for squares modulo an odd prime number, and we use this characterization to give a proof of the law of quadratic reciprocity. There are very many proofs of this law (see Lemmermeyer [1, Appendix B] for a list), and the proof given here is similar to several earlier ones; in particular, the calculations are somewhat like those in the proof of Rousseau [2]. But the proof given here is in a sense more direct than most comparable proofs, because it bypasses Euler's criterion; see the remarks at the end of the note.

## 1. The basic result.

Consider the congruence

$$x^2 \equiv a \bmod p,$$

where $p$ is an odd prime number and where $a$ is an integer not divisible by $p$. If the congruence has an integer solution $x$, then we say that $a$ is a *quadratic residue* modulo $p$ and we write $(\frac{a}{p}) = 1$; if the congruence has no integer solutions then we say that $a$ is a *quadratic nonresidue* modulo $p$ and write $(\frac{a}{p}) = -1$. The symbol $(\frac{a}{p})$ is called a *Legendre symbol.*

We can evaluate the Legendre symbol $(\frac{a}{p})$ by using the desymmetrized congruence $xy \equiv a \bmod p$. To do this, let $\tau(a,p)$ be the number of ordered pairs of integers $(x,y)$ such that

$$0 < x < \tfrac{1}{2}p, \quad 0 < y < \tfrac{1}{2}p, \quad xy \equiv a \bmod p;$$

we think of $\tau(-,p)$ as a modular divisor function. We get the following result.

Proposition 1. *Let $p$ be an odd prime number and let $a$ be an integer not divisible by $p$. Then $a$ is a quadratic residue modulo $p$ if and only if $\tau(a,p)$ is odd.*

Proof. If $(x,y)$ is a pair counting towards $\tau(a,p)$, then $(y,x)$ is also a pair counting towards $\tau(a,p)$. It follows that there is an even number of pairs $(x,y)$ with $x \neq y$ counting towards $\tau(a,p)$. If $a$ is a quadratic residue modulo $p$, so that $a \equiv x_0^2 \bmod p$ for some integer $x_0$, then

$$x^2 \equiv a \bmod p \iff x \equiv \pm x_0 \bmod p,$$

so there is a unique integer $x$ with $0 < x < \frac{1}{2}p$ such that $x^2 \equiv a \bmod p$, and it follows that $\tau(a,p)$ is odd. If $a$ is not a quadratic residue modulo $p$ then there are no integers $x$ such that $x^2 \equiv a \bmod p$, and it follows that $\tau(a,p)$ is even. This completes the proof. □

## 2. The law of quadratic reciprocity.

The law of quadratic reciprocity relates two Legendre symbols of the form $(\frac{q}{p})$ and $(\frac{p}{q})$. We will state the law, and then give a proof based on Proposition 1.

Theorem 2. *Let $p$ and $q$ be distinct odd prime numbers, and let*

$$\tilde{p} = \tfrac{1}{2}(p-1), \quad \tilde{q} = \tfrac{1}{2}(q-1).$$

*Then $(\frac{q}{p}) = (\frac{p}{q})$ if and only if $\tilde{p}\tilde{q}$ is even.*

Proof of Theorem 2. Given an integer $n$ with $|n| < \frac{1}{2}pq$, we define a pair of integers $\bigl(\rho(n), \rho'(n)\bigr)$ as follows: if $n$ is divisible by $p$ then $\rho(n) = 0$; if $n$ is not divisible by $p$ then $\rho(n)$ is the unique integer such that

$$0 < |\rho(n)| < \tfrac{1}{2}p, \quad n\rho(n) \equiv q \bmod p;$$

if $n$ is divisible by $q$ then $\rho'(n) = 0$; if $n$ is not divisible by $q$ then $\rho'(n)$ is the unique integer such that

$$0 < |\rho'(n)| < \tfrac{1}{2}q, \quad n\rho'(n) \equiv p \bmod q.$$

For distinct integers $n_1$ and $n_2$ in the interval $(-\frac{1}{2}pq, \frac{1}{2}pq)$ we have $n_1 \not\equiv n_2 \bmod p$ or $n_1 \not\equiv n_2 \bmod q$, from which it follows that $\rho(n_1) \neq \rho(n_2)$ or $\rho'(n_1) \neq \rho'(n_2)$. The pairs $\bigl(\rho(n), \rho'(n)\bigr)$ therefore take distinct values, so they take each of the $pq$ possible values exactly once. In particular, let $S$ be the set of integers $n$ with $|n| < \frac{1}{2}pq$ such that $\rho(n)\rho'(n) < 0$; then $S$ has $2\tilde{p}\tilde{q}$ members. Clearly $n \in S$ if and only if $-n \in S$, so half of the members of $S$ are positive; thus there are $\tilde{p}\tilde{q}$ integers $n$ with $0 < n < \frac{1}{2}pq$ such that $\rho(n)\rho'(n) < 0$.

Now let $T$ be the set of integers $n$ with $0 < n < \frac{1}{2}pq$ such that $\rho(n) > 0$. Let $u$ be the number of integers $n$ in $T$ such that $\rho'(n) = 0$, let $v$ be the number such that $\rho'(n) > 0$, and let $w$ be the number such that $\rho'(n) < 0$, so that $T$ has $u + v + w$ members all together. We will show that the value of $u + v + w$ determines the value of $(\frac{q}{p})$. Indeed the members $n$ of $T$ which are less than $\frac{1}{2}p$ correspond to the pairs $(x, y)$ which count towards $\tau(q,p)$ (take $x = n$ and $y = \rho(n)$), so $T$ has $\tau(q,p)$ members less than $\frac{1}{2}p$. On the other hand, the interval $(\frac{1}{2}p, \frac{1}{2}pq)$ has length $p\tilde{q}$, so the equation $\rho(n) = i$ has $\tilde{q}$ solutions with $\frac{1}{2}p < n < \frac{1}{2}pq$ for each given integer $i$ with $1 \leq i \leq \tilde{p}$, and it follows that $T$ has $\tilde{p}\tilde{q}$ members greater than $\frac{1}{2}p$. Since $T$ has $u + v + w$ members all together, this gives us

$$\tau(q,p) + \tilde{p}\tilde{q} = u + v + w.$$

From Proposition 1 we see that $(\frac{q}{p}) = 1$ if and only if $u + v + w - \tilde{p}\tilde{q}$ is odd.

Next we show that $u$ is odd. Indeed, $u$ is the number of multiples $n$ of $q$ with $0 < n < \frac{1}{2}pq$ such that $\rho(n) > 0$. These multiples correspond to the pairs $(x, y)$ which count towards $\tau(1,p)$ (take $x = n/q$ and $y = \rho(n)$), so $u = \tau(1,p)$. Since 1 is a quadratic residue modulo $p$, it follows from Proposition 1 that $u$ is odd. Therefore $(\frac{q}{p}) = 1$ if and only if $v + w - \tilde{p}\tilde{q}$ is even.

Analogously, let $w'$ be the number of integers $n$ with $0 < n < \frac{1}{2}pq$ such that $\rho(n) < 0$ and $\rho'(n) > 0$; then $(\frac{p}{q}) = 1$ if and only if $v + w' - \tilde{p}\tilde{q}$ is even, and it follows that $(\frac{q}{p}) = (\frac{p}{q})$ if and only if $w + w'$ is even. But $w + w'$ is the number of integers $n$ with $0 < n < \frac{1}{2}pq$ such that $\rho(n)\rho'(n) < 0$, so $w + w' = \tilde{p}\tilde{q}$ as already observed. Therefore $(\frac{q}{p}) = (\frac{p}{q})$ if and only if $\tilde{p}\tilde{q}$ is even. This completes the proof. □

## 3. Remarks.

This section is intended to explain the relationships between some of the proofs of the law of quadratic reciprocity.

The result of Proposition 1 can be expressed as a formula

$$(\tfrac{a}{p}) = (-1)^{\tau(a,p)-1} \tag{1}$$

giving the value of the Legendre symbol $(\frac{a}{p})$. We will now derive some other formulae.

First, let $U_p$ be the set of nonzero integers $n$ such that $|n| < \frac{1}{2}p$, and let $\rho_p^a$ be the permutation of $U_p$ given by

$$i\rho_p^a(i) \equiv a \bmod p.$$

We see that $U_p$ has $\tau(a,p)$ positive members with positive images under $\rho_p^a$, so $U_p$ has $\frac{1}{2}(p-1) - \tau(a,p)$ positive members with negative images under $\rho_p^a$. Clearly $\rho_p^a(-i) = -\rho_p^a(i)$ for all $i$ in $U_p$, so the sign of $\rho_p^a$ is $(-1)^{[(p-1)/2]-\tau(a,p)}$. Writing $\operatorname{sgn}\sigma$ for the sign of a permutation $\sigma$, we see that

$$(\tfrac{a}{p}) = (-1)^{(p-3)/2} \operatorname{sgn}\rho_p^a. \tag{2}$$

We could also prove this by observing that $\rho_p^a$ is an involution of a $(p-1)$-element set with $(\frac{a}{p}) + 1$ fixed points.

Next, let $\pi_p^a$ be the permutation of $U_p$ given by

$$\pi_p^a(i) \equiv ai \bmod p.$$

We have $\pi_p^a = \rho_p^a\rho_p^1$, so $\operatorname{sgn}\pi_p^a = \operatorname{sgn}\rho_p^a \operatorname{sgn}\rho_p^1$. We also have $\operatorname{sgn}\rho_p^1 = (-1)^{(p-3)/2}$, because 1 is a quadratic residue modulo $p$. This gives us *Zolotarev's lemma*,

$$(\tfrac{a}{p}) = \operatorname{sgn}\pi_p^a. \tag{3}$$

Next, let $\mu(a,p)$ be the number of integers $i$ in $U_p$ such that $i > 0$ and $\pi_p^a(i) < 0$. Then the sign of $\pi_p^a$ is $(-1)^{\mu(a,p)}$, because $\pi_p^a(-i) = -\pi_p^a(i)$ for all $i$. This gives us *Gauss's lemma*,

$$(\tfrac{a}{p}) = (-1)^{\mu(a,p)}. \tag{4}$$

We could also get this formula directly from (1) by showing that

$$\mu(a,p) \equiv \tau(a,p) + \tau(1,p) \bmod 2.$$

Finally, we note that the integers $\pi_p^a(i)$ for $0 < i < \frac{1}{2}p$ are obtained by choosing either $j$ or $-j$ for $0 < j < \frac{1}{2}p$, and that the number of negative choices is $\mu(a,p)$. Multiplying these integers together shows that $a^{(p-1)/2}N \equiv (-1)^{\mu(a,p)}N \bmod p$, where $N = [\frac{1}{2}(p-1)]!$. This gives us *Euler's criterion*,

$$(\tfrac{a}{p}) \equiv a^{(p-1)/2} \bmod p. \tag{5}$$

Formulae (1)–(5) all give the same information in different ways, and (3)–(5) are often proved essentially as consequences of (1). There are many proofs of the law of quadratic reciprocity based on (3), (4), or (5); see [1, Appendix B]. The proof given here, based directly on (1), perhaps provides a short cut; at any rate, I hope that it is illuminating.

## References

[1] F. Lemmermeyer, *Reciprocity Laws from Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[2] G. Rousseau, On the quadratic reciprocity law, *J. Aust. Math. Soc. Ser. A* **51** (1991) 423–425.

Department of Mathematics, Faculty of Information and Mathematical Sciences, University of Glasgow, University Gardens, Glasgow, Great Britain G12 8QW

*E-mail address*: `r.steiner@maths.gla.ac.uk`