Elemente der Mathematik 78 (2023), 171–173
DOI 10.4171/EM/485

Short note

Hermite's identity and the quadratic reciprocity law

Franz Lemmermeyer

In this note, we give a proof of the quadratic reciprocity law based on Gauss's Lemma and Hermite's identity, which is related to other proofs using distribution relations (see Kubota [3]).

Let $p = 2m + 1$ and $q = 2n + 1$ be odd primes, and let $A = \{1, 2, \dots, m\}$ and $B = \{1, 2, \dots, n\}$ denote two half systems modulo p and q, respectively.

For each $a \in A$, we have $qa \equiv r_a \bmod p$ for some $0 < r_a < p$, hence either $r_a \in A$ or $p - r_a \in A$. In particular, $r_a \equiv \varepsilon_a a' \bmod p$, where $\varepsilon_a = \pm 1$ and $a' \in A$. Taking the product of these congruences, we find

$$q^{\frac{p-1}{2}} \cdot m! \equiv \prod \varepsilon_a a' \bmod p,$$

and since $m! = \prod a'$ and $q^{\frac{p-1}{2}} \equiv (\frac{q}{p}) \bmod p$ (here $(\frac{a}{p})$ denotes the Legendre symbol), we obtain

$$\Big(\frac{q}{p}\Big) = \prod_{a \in A} \varepsilon_a.$$

Now $\varepsilon_a = 1$ if $0 < r_a < \frac{p}{2}$, and $\varepsilon_a = -1$ otherwise; on the other hand, we see that

$$\Big\lfloor \frac{2qa}{p} \Big\rfloor - 2\Big\lfloor \frac{qa}{p} \Big\rfloor = \begin{cases} 0 & \text{if } r_a < \frac{p}{2}, \\ 1 & \text{if } r_a > \frac{p}{2}, \end{cases}$$

where $\lfloor x \rfloor$ denotes the largest integer $\le x$. Thus $\varepsilon_a = (-1)^{\lfloor \frac{2qa}{p} \rfloor}$, and we have proved the following lemma.

Lemma 1 (Gauss's Lemma).

$$\Big(\frac{q}{p}\Big) = (-1)^M \quad \textit{for } M = \sum_{a \in A} \Big\lfloor \frac{2qa}{p} \Big\rfloor.$$

Next we transform the sum M modulo 2.

Lemma 2. *We have*

$$\sum_{a\in A}\left\lfloor\frac{2qa}{p}\right\rfloor \equiv \sum_{a\in A}\left\lfloor\frac{qa}{p}\right\rfloor \bmod 2.$$

Proof. The terms $\lfloor\frac{2qa}{p}\rfloor$ with $a < \frac{p}{4}$ occur as $\lfloor\frac{q\cdot 2a}{p}\rfloor$ in the sum on the right. We pair the remaining terms $\lfloor\frac{2qa}{p}\rfloor$ with $a > \frac{p}{4}$ with the terms $\lfloor\frac{qa}{p}\rfloor$ with odd values of a in the sum on the right by pairing $\lfloor\frac{2qa}{p}\rfloor$ with $\lfloor\frac{q(p-2a)}{p}\rfloor$. The claim follows from the observation that the sum of these two terms is even; this in turn follows from

$$\begin{aligned}\left\lfloor\frac{2qa}{p}\right\rfloor + \left\lfloor\frac{q(p-2a)}{p}\right\rfloor &= \left\lfloor\frac{2qa}{p}\right\rfloor + \left\lfloor q - \frac{2qa}{p}\right\rfloor \\ &= \left\lfloor\frac{2qa}{p}\right\rfloor + q - 1 - \left\lfloor\frac{2qa}{p}\right\rfloor = q - 1,\end{aligned}$$

and we are done.

Here we have used the fact that $\lfloor a - x\rfloor = a - 1 - \lfloor x\rfloor$ for all natural numbers a and real numbers $x \in \mathbb{R} \setminus \mathbb{Z}$. In fact, for all real x with $0 < x < 1$, we have $\lfloor a - x\rfloor = a - 1 = a - 1 - \lfloor x\rfloor$, and the claim follows from the fact that both sides have period 1. ■

We remark that Lemma 2 may be avoided by replacing Gauss's Lemma with Eisenstein's Lemma (see [1]), which uses the half system $A' = \{2, 4, \ldots, p-1\}$.

Now we know that

$$\left(\frac{q}{p}\right) = (-1)^{\mu} \quad \text{for } \mu = \sum_{a\in A}\left\lfloor\frac{qa}{p}\right\rfloor \quad \text{and} \quad \left(\frac{p}{q}\right) = (-1)^{\nu} \quad \text{for } \nu = \sum_{b\in B}\left\lfloor\frac{pb}{q}\right\rfloor.$$

This implies

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

For proving that $\mu + \nu = \frac{p-1}{2}\frac{q-1}{2}$ (from which quadratic reciprocity follows), we use Hermite's identity.

Lemma 3. *For all real values $x \ge 0$ and all natural numbers $n \ge 1$, we have*

$$\lfloor x\rfloor + \left\lfloor x + \frac{1}{n}\right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n}\right\rfloor = \lfloor nx\rfloor. \tag{1}$$

Hermite [2] proved this identity using generating functions; the elementary proof given here can be found in [4, Chapter 12].

Proof. Consider the function

$$f(x) = \lfloor x\rfloor + \left\lfloor x + \frac{1}{n}\right\rfloor + \cdots + \left\lfloor x + \frac{n-1}{n}\right\rfloor - \lfloor nx\rfloor.$$

It is immediately seen that $f(x + \frac{1}{n}) = f(x)$ and that $f(x) = 0$ for $0 \le x < \frac{1}{n}$. Thus $f(x) = 0$ for all real values of x, and this proves the claim. ■

Applying Hermite's identity (1) with $x = \frac{a}{p}$ and $n = q$ to the sum μ and using the fact that $\lfloor \frac{a}{p} + \frac{b}{q} \rfloor = 0$ whenever $a \in A$ and $b \in B$, we find

$$\begin{aligned}\mu &= \sum_{a\in A}\Big\lfloor \frac{aq}{p}\Big\rfloor = \sum_{a\in A}\sum_{b=0}^{q-1}\Big\lfloor \frac{a}{p} + \frac{b}{q}\Big\rfloor = \sum_{a\in A}\sum_{b=n+1}^{q-1}\Big\lfloor \frac{a}{p} + \frac{b}{q}\Big\rfloor \\ &= \sum_{a\in A}\sum_{b=1}^{n}\Big\lfloor \frac{a}{p} + \frac{q-b}{q}\Big\rfloor = \sum_{a\in A}\sum_{b\in B}\Big(\Big\lfloor \frac{a}{p} - \frac{b}{q} + 1\Big\rfloor\Big)\end{aligned}$$

and, similarly,

$$\nu = \sum_{b=1}^{m}\Big\lfloor \frac{bp}{q}\Big\rfloor = \sum_{a\in A}\sum_{b\in B}\Big\lfloor \frac{b}{q} - \frac{a}{p} + 1\Big\rfloor.$$

Clearly, $\lfloor \frac{a}{p} - \frac{b}{q} + 1 \rfloor = 1$ if $\frac{a}{p} - \frac{b}{q} > 0$ and $\lfloor \frac{a}{p} - \frac{b}{q} + 1 \rfloor = 0$ if $\frac{a}{p} - \frac{b}{q} < 0$; this implies that $\lfloor \frac{a}{p} - \frac{b}{q} + 1 \rfloor + \lfloor \frac{b}{q} - \frac{a}{p} + 1 \rfloor = 1$, and we find

$$\mu + \nu = \sum_{a\in A}\sum_{b\in B}\Big\lfloor \frac{a}{p} - \frac{b}{q} + 1\Big\rfloor + \sum_{a\in A}\sum_{b\in B}\Big\lfloor \frac{b}{q} - \frac{a}{p} + 1\Big\rfloor = \frac{p-1}{2}\frac{q-1}{2}.$$

This completes our proof.

Acknowledgement. I thank François Brunault for his comments on the first draft of this note.

References

[1] G. Eisenstein, Geometrischer Beweis des Fundamentaltheorems für die quadratischen Reste. *J. Reine Angew. Math.* **28** (1844), 246–248

[2] C. Hermite, Sur quelques conséquences arithmétiques des formules de la théorie des fonctions elliptiques. *Acta Math.* **5** (1884), 297–330; *Oeuvres* **4** (1917), 138–168

[3] T. Kubota, Anwendung Jacobischer Thetafunktionen auf die Potenzreste. *Nagoya Math. J.* **19** (1961), 1–13

[4] S. Savchev and T. Andreescu, *Mathematical miniatures*. Mathematical Association of America Press, Washington, 2003

Franz Lemmermeyer
Mörikeweg 1, 73489 Jagstzell, Germany
hb3@uni-heidelberg.de