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.

Let $p = 2m+1$ and $q = 2n+1$ be odd primes, and let $A = \{1, 2, \ldots m\}$ and $B = \{1, 2, \ldots n\}$ 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 $q^{\frac{p-1}{2}} \equiv (\frac{q}{p}) \bmod p$ 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

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

Thus $\varepsilon_a = (-1)^{\lfloor \frac{2qa}{p} \rfloor}$, and we have proved

Lemma 1 (Gauss's Lemma)**.**

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

Next we transform the sum M modulo 2.

Lemma 2. *We have*

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

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 $\lfloor \frac{2qa}{p} \rfloor + \lfloor \frac{q(p-2a)}{p} \rfloor = \lfloor \frac{2qa}{p} \rfloor + \lfloor q - \frac{2qa}{p} \rfloor = \lfloor \frac{2qa}{p} \rfloor + q - 1 - \lfloor \frac{2qa}{p} \rfloor = q - 1$, and we are done.

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

Now we know that

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

This implies

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

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*

$$\lfloor x \rfloor + \Big\lfloor x + \frac{1}{n} \Big\rfloor + \ldots + \Big\lfloor x + \frac{n-1}{n} \Big\rfloor = \lfloor nx \rfloor. \tag{2}$$

Hermite [1] proved this identity using generating functions; the elementary proof given here can be found in [2, Ch. 12].

Proof. Consider the function

$$f(x) = \lfloor x \rfloor + \Big\lfloor x + \frac{1}{n} \Big\rfloor + \ldots + \Big\lfloor x + \frac{n-1}{n} \Big\rfloor - \lfloor nx \rfloor.$$

It is immediately seen that $f(x+\frac1n) = f(x)$ and that $f(x) = 0$ for $0 \le x < \frac1n$. Thus $f(x) = 0$ for all real values of x, and this proves the claim. $\square$

Applying Hermite's identity (2) 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

$$\begin{aligned}
\mu &= \sum_{a\in A} \Big\lfloor \frac{aq}{p} \Big\rfloor = \sum_{a\in A}\sum_{b=0}^{q-1} \Big\lfloor \frac{a}{p} + \frac{b}{q} \Big\rfloor = \sum_{a\in A}\sum_{b=n+1}^{q-1} \Big\lfloor \frac{a}{p} + \frac{b}{q} \Big\rfloor \\
&= \sum_{a\in A}\sum_{b=1}^{n} \Big\lfloor \frac{a}{p} + \frac{q-b}{q} \Big\rfloor = \sum_{a\in A}\sum_{b\in B} \Big(\Big\lfloor \frac{a}{p} - \frac{b}{q} + 1 \Big\rfloor \Big) \qquad \text{and, similarly,} \\
\nu &= \sum_{b=1}^{m} \Big\lfloor \frac{bp}{q} \Big\rfloor = \sum_{a\in A}\sum_{b\in B} \Big\lfloor \frac{b}{q} - \frac{a}{p} + 1 \Big\rfloor.
\end{aligned}$$

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

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

References

[1] Ch. Hermite, *Sur quelques conséquences arithmétiques des formules de la théorie des fonctions elliptiques*, Extrait du Bulletin de l'Acad. Sci. St. Pétersb. XXIX., Acta Math. **5** (1884), 297–330; Oeuvres **4** (1917), 138–168

[2] S. Savchev, T. Andreescu, *Mathematical miniatures*, MAA 2003

Mörikeweg 1, 73489 Jagstzell
Email address: hb3@uni-heidelberg.de