ACTA ARITHMETICA
Online First version

Yet another proof of the quadratic reciprocity law

by

ALFRED CZOGAŁA and PRZEMYSŁAW KOPROWSKI (Katowice)

Among all mathematical results it is the quadratic reciprocity law which possibly has the highest number of published proofs. The web page http://www.rzuser.uni-heidelberg.de/∼hb3/fchrono.html lists a total of 246 (at the time of writing) distinct proofs. In this paper we present yet another proof, based on some basic facts from group theory. The group-theoretical approach to the subject is not completely new. To the best of our knowledge the first proof of this genre was presented in [2]. The idea of our proof is to some extent inspired by Rousseau's proof [3].

If $(G,+)$ is a finite abelian group, then the quotient group $G/2G$ can be treated as a linear space over $\mathbb{F}_2$. Recall that 2-*rank* of G, denoted $\operatorname{rank}_2 G$, is the dimension of this vector space. Equivalently, since every finite abelian group is a direct sum of cyclic groups, the 2-rank of G is the number of cyclic summands of even orders. Denote by G_2 the subgroup of G consisting of all elements of orders not exceeding 2:

$$G_2 := \{g \in G \mid 2g = 0\}.$$

Then G_2 is an elementary 2-group isomorphic to $G/2G$. It follows that the 2-rank of G is the dimension of G_2 treated as an $\mathbb{F}_2$-linear space. In particular G_2 is isomorphic to $\mathbb{F}_2^{\operatorname{rank}_2 G}$ and we have:

OBSERVATION 1. *With the above notation,* $\operatorname{rank}_2 G = \log_2 |G_2|$.

LEMMA 2. *Let $(G,+)$ be a finite abelian group and $a := \sum_{g\in G} g$ the sum of all elements in G.*

- *If* $\operatorname{rank}_2 G \neq 1$, *then* $a = 0$.
- *If* $\operatorname{rank}_2 G = 1$, *then a has order* 2 *in G.*

2010 *Mathematics Subject Classification*: 11A15, 20K01.
Key words and phrases: quadratic reciprocity law.
Received 21 March 2018; revised 30 June 2018.
Published online *.

Proof. Let G_2 be as above. For every $g \in G \setminus G_2$, we have $g \neq -g$. Combining such elements into pairs $(g, -g)$ we obtain

$$a = \sum_{g\in G} g = \sum_{g\in G_2} g.$$

In particular, if G has an odd number of elements, then $\operatorname{rank}_2 G = 0$ and $a = 0$, as claimed.

Now assume that $|G|$ is even and denote $m := \operatorname{rank}_2 G$. Recall that the linear spaces G_2 and $\mathbb{F}_2^m$ are isomorphic. If $m = 1$, then $\sum_{v\in\mathbb{F}_2} v = 1$ and so $a = \sum_{g\in G_2} g$ is the unique element of G of order 2. On the other hand, if $m > 1$ then for every $i \le m$ in the vector space $\mathbb{F}_2^m$ there are precisely 2^{m-1} vectors whose ith coordinate is 1. It follows that the ith coordinate of $\sum_{v\in\mathbb{F}_2^m} v$ equals $2^{m-1} \cdot 1 = 0$, so this sum is the null vector. Using our isomorphism $G_2 \cong \mathbb{F}_2^m$ we see that $a = \sum_{g\in G_2} g = 0$, as desired. ∎

From now on let p, q be two distinct (but fixed) prime numbers. Denote by G the direct product $\mathbb{F}_p^\times \times \mathbb{F}_q^\times$ of invertibles modulo p and modulo q. Consider the subgroup $\Gamma := \{(1,1), (-1,-1)\}$ of G and set $\overline{G} := G/\Gamma$.

Lemma 3. *With the above notation:*

- *If* $p \equiv q \equiv 1 \pmod 4$, *then* $\operatorname{rank}_2 \overline{G} > 1$.
- *If either* $p \equiv 3 \pmod 4$ *or* $q \equiv 3 \pmod 4$, *then* $\operatorname{rank}_2 \overline{G} = 1$.

Proof. The group $G = \mathbb{F}_p^\times \times \mathbb{F}_q^\times$ is isomorphic to $A = C_{p-1} \times C_{q-1}$, where $C_k := \mathbb{Z}/k\mathbb{Z}$ is a cyclic group with k elements. The isomorphism maps Γ onto the subgroup $B := \{(0,0), ((p-1)/2, (q-1)/2)\}$ of A.

Using Observation 1, let us compute the 2-rank of $\overline{G}$ by counting the number of elements of order ≤ 2 in A/B. If $p \equiv q \equiv 1 \pmod 4$, then A/B contains at least three such elements, namely the cosets (modulo B) of $(0,0)$, $((p-1)/2, 0) \equiv (0, (q-1)/2)$ and $((p-1)/4, (q-1)/4)$. Therefore $\operatorname{rank}_2 \overline{G} = \operatorname{rank}_2(A/B) > 1$.

On the other hand, if either $p \equiv 3 \pmod 4$ or $q \equiv 3 \pmod 4$, then the only elements of A/B whose orders do not exceed 2 are the cosets of $(0,0)$ and $((p-1)/2, 0)$. Thus, in this case $\operatorname{rank}_2 \overline{G} = \operatorname{rank}_2(A/B) = 1$. ∎

Borrowing an idea from [3], we consider a set $\mathcal{L}$ of representatives of all cosets of Γ in G. Let

$$\mathcal{L} := \{(k \bmod p, k \bmod q) : 0 < k < pq/2,\ p \nmid k,\ q \nmid k\}.$$

The following fact was proved in [3]. We re-prove it here to make this paper self-contained.

Lemma 4. *The product of all elements of* $\mathcal{L}$ *equals*

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

Proof. The definition of $\mathcal{L}$ is symmetric in p, q, and so is the assertion of the lemma. Hence it suffices to prove the equality at the first coordinate. Indeed,

$$\prod_{(k,k)\in\mathcal{L}} k = \frac{\prod_{k<pq/2,\, p\nmid k} k}{\prod_{k<pq/2,\, q\,|\, k} k}$$
$$= \frac{\big(\prod_{0<k<p} k\big)\cdot\big(\prod_{0<k<p} (p+k)\big)\cdots\big(\prod_{0<k<p} \big(\frac{q-3}{2}\cdot p+k\big)\big)}{(q)(2q)\cdots\big(\frac{p-1}{2}\cdot q\big)}\cdot \prod_{0<k<p/2}\left(\frac{q-1}{2}\cdot p+k\right).$$

Each product in the numerator is equal to $(p-1)!$, and hence to -1 by Wilson's theorem. Analogously, the last product is equal to $\big(\frac{p-1}{2}\big)!$. Finally, the denominator equals

$$(q)(2q)\cdots\left(\frac{p-1}{2}\cdot q\right) = q^{(p-1)/2}\cdot\left(\frac{p-1}{2}\right)! = \left(\frac{q}{p}\right)\cdot\left(\frac{p-1}{2}\right)!$$

by Euler's criterion. All in all, the formula simplifies to $(-1)^{(q-1)/2}\cdot\big(\frac{q}{p}\big)$. ■

We are now ready to present the new proof of the quadratic reciprocity law.

Proof of the quadratic reciprocity law. We will consider all the possible remainders of p, q modulo 4. First assume that $p \equiv q \equiv 1 \pmod 4$. Then $\operatorname{rank}_2 \overline{G} > 1$ by Lemma 3, and so Lemma 2 implies that the product of all elements from $\mathcal{L}$ lies in Γ. Thus, both coordinates are either all 1 or all -1. In particular, the first coordinate is the same as the second one, hence

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

by Lemma 4. This shows that $\big(\frac{q}{p}\big) = \big(\frac{p}{q}\big)$.

Conversely, assume that at least one of the two primes is congruent to 3 modulo 4. Then $\operatorname{rank}_2 \overline{G} = 1$, and so by Lemma 2 the product of all elements of $\mathcal{L}$ has order 2 in the quotient group $\overline{G}$. Thus the product equals $(1,-1)\cdot\Gamma$ $= (-1,1)\cdot\Gamma$. In particular, the two coordinates are opposite to each other:

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

Now, if $p \not\equiv q \pmod 4$, then $(-1)^{(q-1)/2} = -(-1)^{(p-1)/2}$ and again we have $\big(\frac{q}{p}\big) = \big(\frac{p}{q}\big)$. On the other hand, if $p \equiv q \equiv 3 \pmod 4$, then $(-1)^{(q-1)/2} = (-1)^{(p-1)/2}$ and so $\big(\frac{q}{p}\big) = -\big(\frac{p}{q}\big)$. This concludes the proof. ■

Acknowledgements. The authors were informed by Chandan Dalawat that Lemma 2 appeared earlier in his paper on Wilson's theorem (see [1, Lemma 2.1]). We wish to thank him for pointing this out.

References

[1] Ch. Dalawat, *Wilson's theorem*, J. Théor. Nombres Bordeaux 21 (2009), 517–521.
[2] W. Duke and K. Hopkins, *Quadratic reciprocity in a finite group*, Amer. Math. Monthly 112 (2005), 251–256.
[3] G. Rousseau, *On the quadratic reciprocity law*, J. Austral. Math. Soc. Ser. A 51 (1991), 423–425.

Alfred Czogała, Przemysław Koprowski
Institute of Mathematics
University of Silesia
Bankowa 14
40-007 Katowice, Poland
E-mail: alfred.czogala@us.edu.pl
przemyslaw.koprowski@us.edu.pl

Abstract (will appear on the journal's web site only)

We present a new proof of the celebrated quadratic reciprocity law. Our proof is based on group theory.