GAUSS'S FIFTH PROOF OF THE LAW OF QUADRATIC RECIPROCITY

STEVEN H. WEINTRAUB

ABSTRACT. We present an exposition of Gauss's fifth proof of the Law of Quadratic Reciprocity.

Gauss first proved the Law of Quadratic Reciprocity in [1]. He developed Gauss's Lemma in [2], in his third proof. He gave his fifth proof in [3]. These works are all available in German translation in [4]. We present Gauss's fifth proof here. Except for minor changes of notation, this is almost verbatim from this translation of his fifth proof (further translated into English).

Lemma 1. *(Gauss's Lemma) Let p be an odd prime and k an arbitrary integer not divisible by p. Consider the smallest positive remainders when $k, 2k, \ldots, ((p-1)/2)k$ are divided by p and suppose that s of them are greater than $p/2$. Then k is a quadratic residue or a quadratic nonresidue $\pmod{p}$ according as s is even or odd.*

Proof. Let $a, b, c, d, \ldots$ be those remainders than are less than $p/2$ and $a', b', c', d', \ldots$ be the others. Then $p-a', p-b', p-c', p-d', \ldots$ are all less than $p/2$, and are all distinct from $a, b, c, d, \ldots$, so that all of these, taken together, are equal to $1, 2, 3, 4, \ldots, (p-1)/2$, up to reordering. Setting $1 \cdot 2 \cdot 3 \cdot 4 \cdots (p-1)/2 = R$,

$$R = abcd \cdots (p-a')(p-b')(p-c')(p-d') \cdots,$$

and hence

$$(-1)^s R = abcd \cdots (a'-p)(b'-p)(c'-p)(d'-p) \cdots.$$

Furthermore

$$Rk^{(p-1)/2} \equiv abcd \cdots a'b'c'd' \cdots \equiv abcd \cdots (a'-p)(b'-p)(c'-p)(d'-p) \cdots \pmod{p},$$

and hence

$$Rk^{(p-1)/2} \equiv R(-1)^s \pmod{p}.$$

Thus $k^{(p-1)/2} \equiv \pm 1 \pmod{p}$, where the positive or negative sign is taken as s is even or odd, and hence by [1, Article 106] the proof of the lemma is complete.[1] □

Theorem 2. *Let p and q be distinct odd integers that are relatively prime to each other. Let n be the number of integers such that the least positive remainder when $p, 2p, 3p, \ldots, ((q-1)/2)p$ is divided by q is greater than $q/2$, and let m be the number of integers such that the least positive remainder when $q, 2q, 3q, \ldots, ((p-1)/2)q$ is divided by p is greater than $p/2$. Then either the three integers n, m, and $((p-1)(q-1)/4)$ are all even or else one of them is even and the other two are odd.*

2000 *Mathematics Subject Classification.* 11A15, Secondary 01A55.

Key words and phrases. Quadratic reciprocity, Gauss.

[1]This is Euler's theorem that k is a quadratic residue $\pmod{p}$ if $k^{(p-1)/2} \equiv 1 \pmod{p}$, and k is a quadratic nonresidue $\pmod{p}$ if $k^{(p-1)/2} \equiv -1 \pmod{p}$. Gauss credits Euler and gives his own proof, which, as he notes, is a slightly simplified version of Euler's proof.

Proof. Let $r = ((p-1)/2)((q-1)/2)$. For integers k and y, let $\bar{y}_k$ be the smallest non-negative remainder when y is divided by k. For a set S, let $|S|$ denote the cardinality of S.

Let

$$F_{\text{low}} = \{1,\ldots,(p-1)/2\}, \quad F_{\text{high}} = \{(p+1)/2,\ldots,p-1)\},$$
$$G_{\text{low}} = \{1,\ldots,(q-1)/2\}, \quad G_{\text{high}} = \{(q+1)/2,\ldots,q-1)\}.$$

Then

$$|\{x \in F_{\text{low}} \mid \overline{qx}_p \in F_{\text{high}}\}| = m,$$
$$|\{x \in G_{\text{low}} \mid \overline{px}_q \in G_{\text{high}}\}| = n.$$

Let

$$H_{\text{low}} = \{1,\ldots,(pq-1)/2\}, \quad H_{\text{high}} = \{(pq+1)/2,\ldots,pq-1)\}.$$

Divide H_{low} into 8 subsets:

$$I_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p \in F_{\text{low}}, \bar{x}_q \in G_{\text{low}}\},$$
$$II_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p \in F_{\text{low}}, \bar{x}_q \in G_{\text{high}}\},$$
$$III_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p \in F_{\text{high}}, \bar{x}_q \in G_{\text{low}}\},$$
$$IV_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p \in F_{\text{high}}, \bar{x}_q \in G_{\text{high}}\},$$
$$V_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p = 0, \bar{x}_q \in G_{\text{low}}\},$$
$$VI_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p = 0, \bar{x}_q \in G_{\text{high}}\},$$
$$VII_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p \in F_{\text{low}}, \bar{x}_q = 0\},$$
$$VIII_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p \in F_{\text{high}}, \bar{x}_q = 0\}.$$

Denote the cardinalities of $I_{\text{low}},\ldots,VIII_{\text{low}}$ by $\alpha_{\text{low}}, \beta_{\text{low}}, \gamma_{\text{low}}, \delta_{\text{low}}, \varepsilon_{\text{low}}, \zeta_{\text{low}}, \eta_{\text{low}}, \theta_{\text{low}}$.

Note that

$$VI_{\text{low}} = \{x \in \{p, 2p, \ldots, ((q-1)/2)p\} \mid \bar{x}_q > q/2\}, \text{ so } \zeta_{\text{low}} = n,$$
$$VIII_{\text{low}} = \{x \in \{q, 2q, \ldots, ((p-1)/2)q\} \mid \bar{x}_p > p/2\}, \text{ so } \theta_{\text{low}} = m.$$

In a similar fashion we may divide H_{high} into 8 subsets $I_{\text{high}},\ldots,VIII_{\text{high}}$ with cardinalities $\alpha_{\text{high}},\ldots,\theta_{\text{high}}$.

Since F_{low} has $(p-1)/2$ elements and Since G_{low} has $(q-1)/2$ elements, we see[2] that $I_{\text{low}} \cup I_{\text{high}}$ has $((p-1)/2)((q-1)/2) = r$ elements, i.e., $\alpha_{\text{low}} + \alpha_{\text{high}} = r$. Similarly $\beta_{\text{low}} + \beta_{\text{high}} = \gamma_{\text{low}} + \gamma_{\text{high}} = \delta_{\text{low}} + \delta_{\text{high}} = r$.

Now if $x \in I_{\text{low}}$, then $\bar{x}_{pq} < pq/2, \bar{x}_p < p/2, \bar{x}_q < q/2$. Then $\overline{pq-x}_{pq} > pq/2, \overline{pq-x}_p > p/2, \overline{pq-x}_q > q/2$, and hence $pq - x \in IV_{\text{high}}$, and vice versa. Thus we have a 1-to-1 correspondence between the elements of I_{low} and IV_{high}, so $\alpha_{\text{low}} = \delta_{\text{high}}$. Similarly $\beta_{\text{low}} = \gamma_{\text{high}}, \gamma_{\text{low}} = \beta_{\text{high}}, \delta_{\text{low}} = \alpha_{\text{high}}$.

Combining these two observations gives the equations

$$\alpha_{\text{low}} + \delta_{\text{low}} = r \tag{1}$$
$$\beta_{\text{low}} + \gamma_{\text{low}} = r. \tag{2}$$

Now $II_{\text{low}} \cup IV_{\text{low}} \cup VI_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_q \in G_{\text{high}}\}$. But this is just the set of integers $\{yq + z \mid y = 0,\ldots,(p-3)/2, z \in G_{\text{high}}\}$. There are $(p-1)/2$ choices for y and $(q-1)/2$ choices for z, so we see that $\beta_{\text{low}} + \delta_{\text{low}} + \zeta_{\text{low}} = ((p-1)/2)((q-1)/2) = r$. Similarly

[2] by the Chinese Remainder Theorem

$III_{\text{low}} \cup IV_{\text{low}} \cup VIII_{\text{low}} = \{x \in H_{\text{low}} \mid \bar{x}_p \in F_{\text{high}}\}$ gives $\gamma_{\text{low}} + \delta_{\text{low}} + \theta_{\text{low}} = r$. Since $\zeta_{\text{low}} = n$ and $\theta_{\text{low}} = m$, this gives the equations

$$\beta_{\text{low}} + \delta_{\text{low}} + n = r \tag{3}$$

$$\gamma_{\text{low}} + \delta_{\text{low}} + m = r. \tag{4}$$

Taking $2(1)+(2)-(3)-(4)$ gives the first of the four equations (the others follow similarly)

$$\begin{aligned} 2\alpha_{\text{low}} &= r+m+n \\ 2\beta_{\text{low}} &= r+m-n \\ 2\gamma_{\text{low}} &= r-m+n \\ 2\delta_{\text{low}} &= r-m-n \end{aligned}$$

and the theorem immediately follows. □

Corollary 3. *(The Law of Quadratic Reciprocity[3]) Let p and q be distinct odd primes.*
(1) If at least one of p and q is congruent to $1 \pmod 4$*, then either both p and q are quadratic residues modulo each other, or neither of them is.*
(2) If p and q are both congruent to $3 \pmod 4$*, then exactly one of p and q is a quadratic residue modulo the other.*

Proof. If at least one of p and q is congruent to $1 \pmod 4$, then $((p-1)(q-1)/4)$ is even, so n and m are either both even or both odd, and hence either both p and q are quadratic residues modulo each other, or neither of them is. If both p and q are congruent to $3 \pmod 4$, then $((p-1)(q-1)/4)$ is odd, so one of n and m must be even and the other odd, and hence exactly one of p and q is a quadratic residue modulo the other. □

References

[1] C.-F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, 1801.

[2] C.-F. Gauss, Theorematis arithmetici demonstratio nova, *Commentationes soc. reg. sc. Gottingensis* **XVI**, 1808.

[3] C.-F. Gauss, Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae, *Commentationes soc. reg. sc. Gottingensis recentiores* **IV**, 1818.

[4] C.-F. Gauss, *Untersuchungen über höhere Arithmetik* (trans. H. Maser), American Mathematical Society/Chelsea, Providence 2006.

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, BETHLEHEM, PA 18015-3174, USA
Email address: shw2@lehigh.edu

[3] Throughout his work Gauss simply calls this the Fundamental Theorem (in the Theory of Quadratic Residues).