

THE RECIPROCITY OF GAUSS SUMS VIA THE RESIDUE THEOREM

GERGELY HARCOS

We shall use the residue theorem to prove a reciprocity property of Gauss sums, and then derive from this property the law of quadratic reciprocity.

Definition. For $a, b, c \in \mathbb{Z}$ with $a, c \geq 1$ and ac even, we define the normalized Gauss sum

$$G(a, b, c) := \frac{1}{\sqrt{c}} \sum_{n \bmod c} e\left(\frac{an^2 + 2bn}{2c}\right).$$

Here $e(z) := e^{2\pi iz}$ as usual.

Theorem. Let $a, b, c \in \mathbb{Z}$ with $a, c \geq 1$ and ac even. Then

$$G(a, b, c) = e\left(\frac{1}{8} - \frac{b^2}{2ac}\right) \overline{G(c, b, a)}.$$

Proof. Consider the entire function

$$f(z) := e\left(\frac{az^2 + 2bz}{2c}\right), \quad z \in \mathbb{C},$$

and the directed line \mathcal{L} parametrized as $t \mapsto -1/2 + e(1/8)t$ for $t \in \mathbb{R}$.

By the residue theorem,

$$\begin{aligned} \sqrt{c}G(a, b, c) &= \sum_{n=0}^{c-1} e\left(\frac{an^2 + 2bn}{2c}\right) \\ &= \int_{c+\mathcal{L}} \frac{f(z)}{e(z)-1} dz - \int_{\mathcal{L}} \frac{f(z)}{e(z)-1} dz \\ &= \int_{\mathcal{L}} \frac{f(z+c) - f(z)}{e(z)-1} dz. \end{aligned}$$

As ac is even, we have that

$$f(z+c) = e\left(\frac{az^2 + 2acz + ac^2 + 2bz + 2bc}{2c}\right) = e\left(\frac{az^2 + 2acz + 2bz}{2c}\right) = f(z)e(az),$$

and hence

$$\begin{aligned} \frac{f(z+c) - f(z)}{e(z)-1} &= f(z) \frac{e(az) - 1}{e(z)-1} \\ &= \sum_{m=0}^{a-1} f(z)e(mz) \\ &= \sum_{m=0}^{a-1} e\left(\frac{az^2 + 2bz + 2cmz}{2c}\right) \\ &= \sum_{m=0}^{a-1} e\left(\frac{(az + b + cm)^2 - (b + cm)^2}{2ac}\right). \end{aligned}$$

It follows that

$$\sqrt{c}G(a, b, c) = \sum_{m=0}^{a-1} e\left(\frac{-(b+cm)^2}{2ac}\right) \int_{\mathcal{L}} e\left(\frac{(az + b + cm)^2}{2ac}\right) dz.$$

By the residue theorem, the last integral is independent of b and m , and equals

$$\int_{e^{(1/8)\mathbb{R}}} e\left(\frac{az^2}{2c}\right) dz = e\left(\frac{1}{8}\right) \sqrt{\frac{c}{a}} \int_{\mathbb{R}} e^{-\pi t^2} dt = e\left(\frac{1}{8}\right) \sqrt{\frac{c}{a}}.$$

Therefore,

$$G(a, b, c) = e\left(\frac{1}{8}\right) \frac{1}{\sqrt{a}} \sum_{m=0}^{a-1} e\left(\frac{-(b+cm)^2}{2ac}\right) = e\left(\frac{1}{8} - \frac{b^2}{2ac}\right) \overline{G(c, b, a)}. \quad \square$$

Corollary 1 (Gauss). *Let c be a positive integer. Then*

$$\frac{1}{\sqrt{c}} \sum_{n \bmod c} e\left(\frac{n^2}{c}\right) = \begin{cases} 1, & c \equiv 1 \pmod{4}; \\ 0, & c \equiv 2 \pmod{4}; \\ i, & c \equiv 3 \pmod{4}; \\ 1+i, & c \equiv 0 \pmod{4}. \end{cases}$$

Proof. By the Theorem,

$$\frac{1}{\sqrt{c}} \sum_{n \bmod c} e\left(\frac{n^2}{c}\right) = G(2, 0, c) = e\left(\frac{1}{8}\right) \overline{G(c, 0, 2)} = \frac{1+i}{2} \left(1 + e\left(-\frac{c}{4}\right)\right).$$

The right-hand side here equals the right-hand side in the previous display. \square

Corollary 2 (Gauss). *Let p and q be two distinct odd primes. Then*

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

Proof. If r (resp. s) runs through a complete set of residues modulo p (resp. q), then $qr + ps$ runs through a complete set of residues modulo pq . Therefore,

$$\begin{aligned} \sum_{n \bmod pq} e\left(\frac{n^2}{pq}\right) &= \sum_{\substack{r \bmod p \\ s \bmod q}} e\left(\frac{(qr + ps)^2}{pq}\right) \\ &= \sum_{\substack{r \bmod p \\ s \bmod q}} e\left(\frac{qr^2}{p} + \frac{ps^2}{q}\right) \\ &= \left(\sum_{r \bmod p} e\left(\frac{qr^2}{p}\right)\right) \left(\sum_{s \bmod q} e\left(\frac{ps^2}{q}\right)\right) \\ &= \left(\left(\frac{q}{p}\right) \sum_{t \bmod p} e\left(\frac{t^2}{p}\right)\right) \left(\left(\frac{p}{q}\right) \sum_{u \bmod q} e\left(\frac{u^2}{q}\right)\right) \\ &= \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) \left(\sum_{t \bmod p} e\left(\frac{t^2}{p}\right)\right) \left(\sum_{u \bmod q} e\left(\frac{u^2}{q}\right)\right). \end{aligned}$$

Evaluating the Gauss sums on the two sides by Corollary 1, the result follows. \square