QUADRATIC REPROCITY AND THE THETA FUNCTION

TERENCE TAO

Abstract. We give the standard proof of the quadratic reciprocity law using Theta functions.

1. Introduction

Define the *theta function* $\vartheta(s)$ for any $\mathrm{Re}(s) > 0$ by the formula

$$\vartheta(s) := \sum_{n=-\infty}^{\infty} e^{-\pi n^2 s}.$$

It is easy to see that this converges to an analytic function on the right-half plane $\mathrm{Re}(s) > 0$. Since the Fourier transform of $f(x) = e^{-\pi x^2 s}$ is $\hat{f}(\xi) = s^{-1/2} e^{-\pi \xi^2/s}$ (where we use the standard branch of the square root on the right-half plane, an easy application of the Poisson summation formula leads to the *functional equation*

$$\vartheta(s) = s^{-1/2} \vartheta(1/s). \tag{1}$$

Now we investigate the limiting behavior of $\vartheta(s)$ as s approaches the imaginary axis. We introduce the *Gauss sum*

$$S(\frac{a}{q}) := \frac{1}{q} \sum_{r=0}^{q-1} e^{-2\pi i a r^2/q} = \frac{1}{q} \sum_{r \in \mathbf{Z}/q\mathbf{Z}} e^{-2\pi i a r^2/q};$$

since the function $r \mapsto e^{-2\pi i a r^2/q}$ is periodic with period q, we see that $S(\frac{a}{q}) = S(\frac{ka}{kq})$ for any $k \geq 1$, so the notation is well-defined. Note that S is periodic modulo 1, so that only the residue class of a modulo q is relevant.

Lemma 1.1. *For any rational number p/q with $q > 0$, we have*

$$\lim_{\varepsilon \to 0} \varepsilon^{1/2} \vartheta(i\frac{p}{q} + \varepsilon) = S(\frac{p}{2q}).$$

Proof We have

$$\varepsilon^{1/2} \vartheta(i\frac{p}{q} + \varepsilon) = \sum_{n=-\infty}^{\infty} e^{-i\pi p n^2/q} \varepsilon^{1/2} e^{-\pi \varepsilon n^2}.$$

Writing $n = 2qm + r$, where $0 \leq r < 2q - 1$, observe that $\pi p n^2/q$ and $\pi p r^2/q$ differ by an integer multiple of 2π. We thus have

$$\varepsilon^{1/2} \vartheta(i\frac{p}{q} + \varepsilon) = \sum_{r=0}^{2q-1} e^{-i\pi p n^2/q} \sum_{m=-\infty}^{\infty} \varepsilon^{1/2} e^{-\pi \varepsilon (2qm+r)^2}.$$

1991 *Mathematics Subject Classification.* 42B15, 35L05.

Writing $x = \varepsilon^{1/2}(2qm + r)$, we can write this as

$$\varepsilon^{1/2}\vartheta(i\frac{p}{q} + \varepsilon) = \frac{1}{2q}\sum_{r=0}^{2q-1} e^{-i\pi pn^2/q} \sum_{x \in \varepsilon^{1/2}(2q\mathbf{Z}+r)} e^{-\pi x^2}\Delta x$$

where $\Delta x = 2q\varepsilon^{1/2}$ is the spacing of x. Taking limits, and noting that the Riemann sum converges to the Riemann integral, we conclude

$$\lim_{\varepsilon\to 0} \varepsilon^{1/2}\vartheta(i\frac{p}{q} + \varepsilon) = \frac{1}{2q}\sum_{r=0}^{2q-1} e^{-i\pi pn^2/q} \int_{-\infty}^{\infty} e^{-\pi x^2}\, dx.$$

Since the integral equals 1, the claim follows. ∎

We remark that an easy perturbation argument also gives

$$\lim_{\varepsilon\to 0} \varepsilon^{1/2}\vartheta(i\frac{p}{q} + \varepsilon + O(\varepsilon^2)) = S(\frac{p}{2q}),$$

i.e. one can vary the approach region to $i\frac{p}{q}$ a little bit. Now from (1) we have

$$\vartheta(i\frac{p}{q} + \varepsilon) = (i\frac{p}{q} + \varepsilon)^{-1/2}\vartheta(-i\frac{q}{p} + \frac{q^2}{p^2}\varepsilon + O(\varepsilon^2)).$$

(Here we allow the $O()$ errors to depend on p, q.) Multiplying by $\varepsilon^{1/2}$ and taking limits as $\varepsilon \to 0$ using the above lemma, we obtain for $p, q > 0$ *Schaar's identity*

$$\sqrt{q}S(\frac{p}{2q}) = e^{-\pi i/4}\sqrt{p}\overline{S(\frac{q}{2p})}.$$

Applying Schaar's identity for $p = 2$ we obtain

$$S(\frac{1}{q}) = \frac{1}{\sqrt{q}}e^{-\pi i/4}\sqrt{2}\overline{S(\frac{q}{4})}.$$

The right-hand side can be computed explicitly, leading to the formulae

$$S(\frac{1}{q}) = \begin{cases} \frac{-1-i}{\sqrt{q}} & \text{when } q = 0 \mod 4 \\ \frac{1}{\sqrt{q}} & \text{when } q = 1 \mod 4 \\ 0 & \text{when } q = 2 \mod 4 \\ \frac{-i}{\sqrt{q}} & \text{when } q = 3 \mod 4. \end{cases} \tag{2}$$

The other Gauss sums can now be computed by a couple change of variable tricks. Firstly observe that

$$S(\frac{an^2}{q}) = S(\frac{a}{q}) \text{ whenever } n \text{ is coprime to } q. \tag{3}$$

This is simply because the map $r \mapsto n^2 r$ is a permutation of $\mathbf{Z}/q\mathbf{Z}$ in this case. In particular, we see that $S(\frac{a}{q}) = S(\frac{1}{q})$ whenever a is a non-zero quadratic residue modulo q. Next, a simple Fourier series computation shows that if q is square-free, then

$$\sum_{a=0}^{q-1} S(\frac{a}{q}) = 1.$$

Since $S(0) = 1$, we conclude in particular that

$$\sum_{a=1}^{q-1} S(\frac{a}{q}) = 0.$$

Now suppose q is prime. Then the numbers between 1 and $q-1$ split equally into quadratic residues and quadratic non-residues. We already know that $S(\frac{a}{q}) = S(\frac{1}{q})$ when a is a quadratic residue, and the value of $S(\frac{a}{q})$ must be the same for all quadratic non-residues thanks to (3). Thus $S(\frac{a}{q}) = -S(\frac{1}{q})$ for all quadratic non-residues. In other words we have

$$S(\frac{a}{q}) = \left(\frac{a}{q}\right) S(\frac{1}{q}) \tag{4}$$

whenever q is prime and a is coprime to q, where the *Jacobi symbol* $\left(\frac{a}{q}\right)$ is defined to equal 1 when a is a quadratic residue modulo p, and -1 when it is not a quadratic residue modulo p.

Next, we observe the identity

$$S(\frac{a}{pq}) = S(\frac{ap}{q})S(\frac{aq}{p})$$

whenever p, q are coprime. This reflects the fact (from the Chinese remainder theorem) that every residue class r in $\mathbf{Z}/pq\mathbf{Z}$ can be written uniquely as $r = pr_1 + qr_2$ where $0 \leq r_1 < q$ and $0 \leq r_2 < p$. Inserting this into the definition of the Gauss sum we obtain the claim. Applying this in particular to $a = 1$ and with p, q being distinct odd primes and using (4) we obtain

$$S(\frac{1}{pq}) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) S(\frac{1}{p})S(\frac{1}{q})$$

which when combined with (4) leads to Gauss's famous law of quadratic reciprocity:

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

Another identity in a similar spirit is

$$S(\frac{a}{p} + \frac{b}{q}) = S(\frac{a}{p})S(\frac{b}{q})$$

whenever p, q are coprime; this is again a consequence of the Chinese remainder theorem, essentially asserting that the distribution of an/p and bn/q modulo 1 are completely independent of each other. This implies the previous identity, since

$$S(\frac{ap}{q})S(\frac{aq}{p}) = S(\frac{ap}{q} + \frac{aq}{p}) = S(\frac{a(p^2+q^2)}{pq}) = S(\frac{a(p+q)^2}{pq}) = S(\frac{a}{pq}).$$

Department of Mathematics, UCLA, Los Angeles, CA 90024
E-mail address: tao@math.ucla.edu