Appendix 14A: Gauss sums

For a given Dirichlet character $\chi \pmod q$ we define the *Gauss sum*, $g(\chi)$, by

$$g(\chi) := \sum_{a=1}^{q} \chi(a) e^{2i\pi a/q}.$$

Note that the summand $\chi(a)e^{2i\pi a/q}$ depends only on the value of $a \pmod q$. Gauss sums play an important role in number theory and have some beautiful properties.

14.7. Identities for Gauss sums

By making the change of variable $a \equiv nb \pmod q$ for some integer n with $(n,q)=1$, the variable b runs through a complete system of residues mod q as a does. Therefore we obtain the surprising identity

$$\sum_{b=1}^{q} \chi(b) e^{2i\pi nb/q} = \overline{\chi(n)} \sum_{b=1}^{q} \chi(nb) e^{2i\pi nb/q} = \overline{\chi}(n) g(\chi). \tag{14.7.1}$$

Therefore if q is prime and χ is non-principal then

$$\phi(q)|g(\chi)|^2 = \sum_{\substack{1\le n\le q\\(n,q)=1}} |\overline{\chi}(n)g(\chi)|^2 = \sum_{n=0}^{q-1} \left| \sum_{b=1}^{q} \chi(b) e^{2i\pi nb/q} \right|^2,$$

since the $n=0$ sum equals $\sum_{b=1}^{q} \chi(b) = 0$. Expanding the square we obtain

$$\sum_{b=1}^{q} \chi(b) \sum_{c=1}^{q} \overline{\chi}(c) \sum_{n=0}^{q-1} e^{2i\pi n(b-c)/q} = q \sum_{b=1}^{q} |\chi(b)|^2 = q\phi(q),$$

since $\sum_{n=0}^{q-1} e^{2i\pi na/q} = 0$ unless q divides a. Therefore we have proved that

$$|g(\chi)|^2 = q.$$

To better use this we have

$$\overline{g(\chi)} = \sum_{a=1}^{q} \overline{\chi}(a) e^{-2i\pi a/q} = \chi(-1) g(\overline{\chi})$$

by (14.7.1), so that $g(\chi)g(\overline{\chi}) = \chi(-1)|g(\chi)|^2 = \chi(-1)q$. In particular if $\chi = (\cdot/q)$, so that $\chi = \overline{\chi}$ then

$$g((\cdot/q))^2 = (-1/q)q.$$

Taking the square root, it remains to determine which sign gives the value of $g((\cdot/q))$. It took Gauss four years to figure this out, so we will simply state his result:

$$g((\cdot/q)) = \begin{cases} \sqrt{q} & \text{if } q \equiv 1 \pmod 4; \\ i\sqrt{q} & \text{if } q \equiv 3 \pmod 4. \end{cases} \tag{14.7.2}$$

Another proof of the law of quadratic reciprocity. Let $q^* = (-1/q)q$ and $g = g((\cdot/q))$. Now

$$g^p = \left(\sum_{a=1}^{q} \left(\frac{a}{q}\right) e^{2i\pi a/q} \right)^p \equiv \sum_{a=1}^{q} \left(\frac{a}{q}\right)^p e^{2i\pi ap/q} \pmod p,$$

as $(x_1 + \cdots + x_q)^p \equiv x_1^p + \cdots + x_q^p \pmod p$. Then, by (14.7.1), we have

$$g^p \equiv \sum_{a=1}^{q} \left(\frac{a}{q}\right) e^{2i\pi ap/q} = \left(\frac{p}{q}\right) g \pmod p.$$

We may divide through by g as $(g^2, p) = (q, p) = 1$, so that

$$\begin{aligned} \left(\frac{p}{q}\right) &\equiv g^{p-1} = (g^2)^{(p-1)/2} = (q^*)^{(p-1)/2} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} q^{(p-1)/2} \equiv (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod p, \end{aligned}$$

by Euler's criterion. Both sides are integers equal to 1 or -1 and differ by a multiple of p, which is ≥ 3, and so they must be equal. That is, we obtain Theorem 8.5, the law of quadratic reciprocity.

14.8. Dirichlet L-functions at $s = 1$

We now use (14.7.1) to try to find a simple expression for $L(1, \chi)$. We again let q be prime so that $\sum_{b=1}^{q} \chi(b) = 0$, and therefore the identity (14.7.1) holds for all integers n (not just those n coprime to q). Assuming that there are no convergence issues in swapping the orders of summation, we have

$$g(\chi)L(1, \overline{\chi}) = \sum_{n\geq 1} \frac{g(\chi)\overline{\chi}(n)}{n} = \sum_{n\geq 1} \frac{\sum_{b=1}^{q-1} \chi(b) e^{2i\pi nb/q}}{n} = \sum_{b=1}^{q-1} \chi(b) \sum_{n\geq 1} \frac{e^{2i\pi nb/q}}{n}$$

The sum over n is the Taylor series for $-\log(1-t)$ with $t = e^{2i\pi nb/q}$ (since each $t \neq 1$). Therefore

$$g(\chi)L(1, \overline{\chi}) = -\sum_{b=1}^{q-1} \chi(b) \log(1 - e^{2i\pi nb/q}).$$

Exercise 14.8.1. (a) Prove that $\arg(1-e^{i\theta}) \in (-\frac{\pi}{2}, \frac{\pi}{2})$.
(b) Deduce that if $0 < \theta < 2\pi$ then $\log(1-e^{i\theta}) - \log(1-e^{-i\theta}) = i(\theta - \pi) \in (-\pi, \pi)$.

Now assume that $\chi(-1) = -1$ and add the b and $q-b$ terms in the sum above, so that by the last exercise we have

$$2g(\chi)L(1,\overline{\chi}) = -\sum_{b=1}^{q-1} \chi(b)(\log(1-e^{2i\pi b/q}) - \log(1-e^{-2i\pi b/q})) = -i\sum_{b=1}^{q-1} \chi(b)(2\pi b/q - \pi).$$

The second sum on the right-hand side is 0, and so multiplying through by $-g(\overline{\chi})$, we obtain

$$qL(1,\overline{\chi}) = \frac{i\pi g(\overline{\chi})}{q} \sum_{b=1}^{q-1} \chi(b)b$$

as $-g(\chi)g(\overline{\chi}) = q$.

Now let $\chi = (\cdot/q)$ with prime $q \equiv 3 \pmod 4$ where $q > 3$, so that $\overline{\chi} = \chi$. Dirichlet's class number formula (given in section 12.15 of appendix 12D with $d = -q$) reads $\pi h(-q) = \sqrt{q}L(1,\chi)$ and therefore the last displayed formula becomes

$$h(-q) = -\frac{1}{q}\sum_{b=1}^{q-1} \chi(b)b.$$

since $g((\cdot/q)) = i\sqrt{q}$ by (14.7.2). This is precisely Jacobi's conjecture, stated as (12.15.1).

14.9. Jacobi sums

Let χ and ψ be characters mod q and define the *Jacobi sum*

$$j(\chi,\psi) := \sum_{\substack{r,s \pmod q \\ r+s\equiv 1 \pmod q}} \chi(r)\psi(s).$$

To evaluate this sum we state the condition "$r+s \equiv 1 \pmod q$" in term of a sum, so that

$$\begin{aligned} j(\chi,\psi) &= \sum_{r,s \pmod q} \chi(r)\psi(s) \cdot \frac{1}{q}\sum_{k=0}^{q-1} e^{2i\pi\frac{k}{p}(r+s-1)} \\ &= \frac{1}{q}\sum_{k=0}^{q-1} e^{-2i\pi\frac{k}{q}} \left(\sum_{r \pmod q} \chi(r)e^{2i\pi\frac{kr}{q}} \right) \left(\sum_{s \pmod q} \psi(s)e^{2i\pi\frac{ks}{q}} \right) \\ &= \frac{1}{q}\sum_{k=0}^{q-1} e^{-2i\pi\frac{k}{q}} \left(\overline{\chi}(k)g(\chi)\right)\left(\overline{\psi}(k)g(\psi)\right) \\ &= \frac{\overline{\chi\psi}(-1)}{q} g(\overline{\chi\psi})g(\chi)g(\psi). \end{aligned}$$

If q is prime and each of χ, ψ and $\overline{\chi\psi}$ is non-principal, then we know that $|g(\overline{\chi\psi})| = |g(\chi)| = |g(\psi)| = \sqrt{q}$, so that $|j(\chi,\psi)| = \sqrt{q}$. By its definition $j(\chi,\psi)$ is an algebraic integer, and belongs to the field defined by the values of χ and ψ.

14.10. The diagonal cubic, revisited

Let p be a prime $\equiv 1 \pmod 3$. Since the group of characters mod p is isomorphic to the multiplicative group of reduced residues mod p, we know that there are two characters $\chi, \chi^2 \pmod p$ of order 3. We can establish the analogy to Corollary 8.1.1 for cubic residues:

Exercise 14.10.1. Prove that if $p \nmid a$ then

$$\#\{x \pmod p : ax^3 \equiv u \pmod p\} = 1 + \chi(a^{-1}u) + \chi^2(a^{-1}u).$$

By exercise 14.10.1, $N(a,b,c)$ equals the sum over triples $u, v, w \pmod p$ for which $u + v + w \equiv 0 \pmod p$, of

$$(1 + \chi(a^{-1}u) + \chi^2(a^{-1}u))\,(1 + \chi(b^{-1}v) + \chi^2(b^{-1}v))\,(1 + \chi(c^{-1}w) + \chi^2(c^{-1}w)).$$

We again multiply the triples out. The first product, $1 \cdot 1 \cdot 1$, sums to p^2. Any other product that contains a 1 sums to 0, since the remaining variables can be summed independently (and each independent sum is of the shape $\sum_t \chi(t) = 0$). Therefore

$$N(a,b,c) = p^2 + \sum_{1 \le i,j,k \le 2} \sum_{\substack{u,v,w \pmod p \\ u+v+w \equiv 0 \pmod p}} \chi^i(a^{-1}u)\chi^j(b^{-1}v)\chi^k(c^{-1}w).$$

We may assume $u \not\equiv 0 \pmod p$ since those summands equal 0. Therefore we can write $v = -ur, w = -us$ and separate out the sum $\sum_{u \pmod p} \chi^{i+j+k}(u)$. This equals 0 when 3 does not divide $i + j + k$. This therefore leaves us with only the terms where $i = j = k$, in which case the sum over u equals $p-1$. For $i = j = k = 1$ we have

$$\sum_{\substack{u,v,w \pmod p \\ u+v+w \equiv 0 \pmod p}} \chi(uvw) = (p-1) \sum_{\substack{r,s \pmod p \\ r+s \equiv 1 \pmod p}} \chi(rs) = (p-1)j(\chi,\chi),$$

and likewise for χ^2. Therefore

$$N(a,b,c) = p^2 + (p-1)(\overline{\chi}(d)j(\chi,\chi) + \chi(d)j(\overline{\chi},\overline{\chi})),$$

where $d = abc$. In section 14.9 we proved that $j(\chi,\chi)$ is an algebraic integer in $\mathbb{Q}(\frac{1+\sqrt{-3}}{2})$ of norm p, so we can write $\overline{\chi}(d)j(\chi,\chi) = \frac{u+v\sqrt{-3}}{2}$ with $u \equiv v \pmod 2$, and $u^2 + 3v^2 = 4p$. We therefore recover the result,

$$N(a,b,c) = p^2 + (p-1)u,$$

that we established in section 14.4. Moreover by calculating $j(\chi,\chi)$ we can determine the sign of b.