Christopher Hillar

General Quadratic Gauss Sums (*Dirichlet*)

Let a, b be non-zero integers, b > 0, and (a,b) = 1. Now, let

$$G(a,b) \;=\; \sum_{x \bmod b} \xi_b^{\,ax^2} \;=\; \sum_{x \bmod b} e^{\frac{2\pi i}{b} ax^2}$$

Where ξ_b is a b^{th} root of unity. This type of sum is called a Quadratic Gauss Sum. We intend to evaluate this sum explicitly. As an example, with a = 1 and b = 3, we have:

$$G(1,3) \;=\; \xi_3^{\,0} + \xi_3^{\,1} + \xi_3^{\,1}$$

But since $\xi_3 \;=\; \dfrac{-1+\sqrt{-3}}{2}$, we have that

$$G(1,3) \;=\; \sqrt{-3}$$

Although we have seen in class such objects, a general theorem exists stating exactly what these G(a,b) are…and not just what happens when you square them.

<u>Reduction to Gauss Sum in class</u>:

In the proof of quadratic reciprocity, given an odd prime p, we needed to know the square value of the following sum:

$$g(p) \;=\; \sum_{a \bmod p} \left(\frac{a}{p}\right) \cdot \xi_p^{\,a}$$

It turns out that the general quadratic gauss sums and the one above are very related. In fact, g(p) = G(1,p).

Proof:

Let r denote the non-zero quadratic residues, and let n denote the non-zero non-quadratic residues. Notice that the map $x \to x^2$ covers the quadratic residues twice. Hence,

(1)
$$\sum_{x \bmod p} \xi_p^{\,x^2} \;=\; 1 + 2\sum_{r} \xi_p^{\,r}$$

But also, we obviously have:

(2)
$$0 \;=\; \sum_{y \bmod p} \xi_p^{\,y} \;=\; 1 + \sum_{r} \xi_p^{\,r} + \sum_{n} \xi_p^{\,n}$$

Combining these two relations finally gives us what we want,

(3)
$$\sum_{x \bmod p} \xi_p^{\,x^2} \;=\; \sum_{r} \xi_p^{\,r} - \sum_{n} \xi_p^{\,n} \;=\; \sum_{a \bmod p} \left(\frac{a}{p}\right) \cdot \xi_p^{\,a}$$

∎

In order to prove the general theorem, we must do some algebraic reductions to reduce the problem to that of computing G(1,b).

Step 1: If p is an odd prime, G(a,p) = $\left(\frac{a}{p}\right)$G(1,p).

Proof:

If $a \equiv c^2$ (mod p) for some c, then we notice that $ax^2 \equiv (cx)^2$ (mod p). But it is easy to see that as x ranges over the set {0, 1, 2, …, p-1}, so will cx. Hence, in this case, G(a,p) = G(1,p).

In the second case, a ≠ square mod p, we must show that G(a,p) = -G(1,p). We first notice that if a is not a square, ax^2 will also not be a square mod p. This is obvious from the fact that

$$-1 = \left(\frac{a}{p}\right)\left(\frac{x^2}{p}\right) = \left(\frac{ax^2}{p}\right)$$

Thus, the set of numbers $\{ax^2\} = a\{x^2\}$ where x ranges over {0, 1, 2, …, p-1} will cover the non-quadratic residues twice. Hence,

$$\sum_{x \bmod p} x_p^{ax^2} = 1 + 2\sum_n x_p^{\,n}$$

Where n denotes the non-residues. Combining this with (2) and (3), gives us that

$$\sum_{x \bmod p} x_p^{ax^2} = -\sum_r x_p^{\,r} + \sum_n x_p^{\,n} = -\sum_{x \bmod p} x_p^{x^2} = -G(1,p)$$

ÿ

The following steps of reduction fall along the same lines as above, and for sake of time, we omit them.

Step 2: Let p be an odd prime, and r an integer ≥ 2, then $G(a,p^r) = pG(a,p^{r-2})$.

Step 3: Let b,c > 0, (b,c) = 1, and (a,bc) = 1. Then G(a,bc) = G(ab,c)·G(ac,b).

Step 4: Let b be odd, b > 0. Then G(a,b) = $\left(\frac{a}{p}\right)$G(1,b).

Step 5: Let a be odd. Then

$$G(a,2^r) = \begin{cases} \left(\dfrac{-2^r}{a}\right) G(1,2^r) & a \equiv 1 \pmod 4 \\[2ex] \left(\dfrac{-2^r}{a}\right) i\, G(1,2^r) & a \equiv 3 \pmod 4 \end{cases}$$

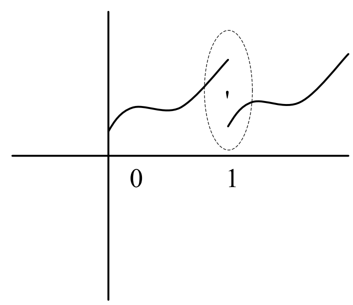
Hence, the value of G(a,b) is completely determined if we can somehow calculate G(1,b). We now do this. (From *Dirichlet*).

Theorem: $$G(1,b) = \begin{cases} (1+i)\sqrt{b} & b \equiv 0 \pmod 4 \\ \sqrt{b} & b \equiv 1 \pmod 4 \\ 0 & b \equiv 2 \pmod 4 \\ i\sqrt{b} & b \equiv 3 \pmod 4 \end{cases}$$

We first need a fact from Fourier analysis.

If q is a function which is smooth except for ordinary discontinuities, then the Fourier series converges pointwise to the midpoint of the discontinuity. In particular, if q is continuously differentiable on the interval [0,1], then

$$\frac{q(0)+q(1)}{2} = \sum_{m \in Z} c_m$$



Where c_m is the m^{th} Fourier coefficient,

$$c_m = \int_0^1 q(x)\, e^{-2pimx}\, dx$$

We shall use the function, f(x) = $e^{2pix^2/b}$.

Letting $f_k(x) = f(x+k)$ {k = 0, 1, 2, …, b-1}, then by definition we have,

$$G(1,b) = \sum_{x \bmod b} e^{\frac{2pi}{b}x^2} = \sum_{x \bmod b} f(x) = \sum_{k=0}^{b-1} \frac{f_k(0)+f_k(1)}{2}$$

Hence, if $\theta = f_0 + f_1 + f_2 + \ldots + f_{b-1}$, by the above theorem, we need only compute the sum of the Fourier coefficients of θ to get the value of G(1,b).

So we have:

$$G(1,b) = \sum_{m \in Z} \sum_{k=0}^{b-1} \int_0^1 f_k(x)\, e^{-2pimx}\, dx$$

$$= \sum_{m \in Z} \int_0^b e^{2pix^2/b}\, e^{-2pimx}\, dx$$

To get this equality above, we need to prove that

$$\sum_{k=0}^{b-1} \int_0^1 f_k(x)\, e^{-2pimx}\, dx \;=\; \int_0^b e^{2pix^2/b}\, e^{-2pimx}\, dx$$

Induction works here. For b = 1, it is true, and for n+1, we have that

$$\sum_{k=0}^{n} \int_0^1 f_k(x)\, e^{-2pimx} dx \;=\; \int_0^n e^{2pix^2/b}\, e^{-2pimx} dx \;+\; \int_0^1 e^{2pi(x+n)^2/b}\, e^{-2pimx} dx$$

Making the change of variables, v = x+n, we get that

$$\int_0^1 e^{2pi(x+n)^2/b}\, e^{-2pimx} dx \;=\; \int_n^{n+1} e^{2pi(v)^2/b}\, e^{-2pimv} dv$$

As desired (because $e^{-2pim(v-n)} = e^{-2pimv} e^{2pimn}$, but $e^{2pimn} = 1$). Hence, the result is true for all n, namely, it is true for n = b-1.

So our computation amounts to finding

$$\sum_{m \in \mathrm{Z}} \int_0^b e^{2pi\left(x^2 - bmx\right)/b} dx$$

Completing the square in the above expression gives us that

$$x^2 - bmx \;=\left(x - \frac{bm}{2}\right)^2 - \frac{b^2 m^2}{4}$$

So our sum is just

$$= \;\sum_{m \in \mathrm{Z}} e^{-pibm^2/2} \int_0^b e^{2pi(x - bm/2)^2/b} dx$$

If m is even, then $e^{-pibm^2/2}$ = 1, and if m is odd, we have that $e^{-pibm^2/2}$ = i^{-b}. The first is due to the fact that

$$e^{-pibm^2/2} = \left(e^{-pib}\right)^{m^2/2} \;=\; \left((-1)^b\right)^{m^2/2} \;=\; 1$$

And if m is odd, we get that

$$e^{-pibm^2/2} \;=\; \left(e^{pi/2}\right)^{-bm^2} \;=\; \left(\mathrm{z}_{\,4}\right)^{-bm^2} \;=\; (i)^{-bm^2} \;=\; i^{-b}.$$

This last equality is due to the fact that m odd implies $m^2 \equiv 1 \pmod 4$.

So we split up the sum into two parts corresponding to odd and even m. Set m = 2r, and examine the sum:

$$\sum_r \int_0^b e^{2pi(x-br)^2/b} dx$$

Letting u = x – br, we get

$$\sum_r \int_{-br}^{b-br} e^{2piu^2/b} du$$

Notice that this sum is just a way of breaking up the integral,

$$\int_{-\infty}^{\infty} e^{2piu^2/b} du$$

Performing the same trivial calculation for m = 2r+1, gives us the same result. Hence, we must have that

$$G(1,b) = \left(1+i^{-b}\right)\int_{-\infty}^{\infty} e^{2piu^2/b} du = \left(1+i^{-b}\right) I_b$$

Provided, of course, that the indefinite integral, I_b, above exists. We do this by examining the tail ends of I_b. Letting 0 < A < B, we set $t = u^2$, dt = 2udu, to get that

$$\int_A^B e^{2piu^2/b} du = \int_{A^2}^{B^2} e^{2pit/b} \frac{dt}{2\sqrt{t}}$$

An integration by parts gives us that the integral above is just

$$\int_{A^2}^{B^2} e^{2pit/b} \frac{dt}{2\sqrt{t}} = \frac{b}{2pi}\left[\frac{e^{2piB^2/b}}{2\sqrt{B^2}} - \frac{e^{2piA^2/b}}{2\sqrt{A^2}} + \int_{A^2}^{B^2} e^{2pit/b} \frac{dt}{4\sqrt{t^3}}\right]$$

Which in absolute value is less than or equal to

$$\left|\frac{b}{2pi}\right|\left(\frac{1}{2B} + \frac{1}{2A} + \int_{A^2}^{B^2} \frac{dt}{4\sqrt{t^3}}\right)$$

Since,

$$\int_{A^2}^{B^2} \frac{dt}{4\sqrt{t^3}} = -\frac{1}{2\sqrt{B^2}} + \frac{1}{2\sqrt{A^2}}$$

we notice that as you take B to infinity, and then A to infinity, these tail ends approach 0.

Finally, we know that I_b exists, but we must still compute it. If we let $t = \frac{u}{\sqrt{b}}, dt = \frac{du}{\sqrt{b}}$, we get

$$\int_{-\infty}^{\infty} e^{2piu^2/b} du = \sqrt{b}\int_{-\infty}^{\infty} e^{2pit^2} dt = \sqrt{b}\, I$$

Where we can find I from the relation, G(1,1) = 1 = $\left(1+i^{-1}\right)\int_{-\infty}^{\infty} e^{2piu^2/1}du = \left(1+i^{-1}\right)I$.

Hence,

$$G(1,b) = \left(1+i^{-b}\right)I_b = \frac{1+i^{-b}}{1+i^{-1}}\sqrt{b}$$

Which takes on the values { $(1+i)\sqrt{b}$, $\sqrt{b}$, 0, $i\sqrt{b}$ } when b ≡ {0,1,2,3} respectively (mod 4).

Therefore, we have determined the exact value of the quadratic gauss sum.

ÿ