(*September 27, 2015*)

Gauss sums and harmonic analysis

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

[This document is
http://www.math.umn.edu/~garrett/m/mfms/notes_2015-16/06e_Gauss_sums.pdf]

In the context of harmonic analysis on finite abelian groups, *Gauss sums* reflect the interaction of *addition* and *multiplication* on the finite ring $\mathbb{Z}/N$. We need a few basic facts.

Let ψ be an *additive character* $\psi : \mathbb{Z}/N \to \mathbb{C}^\times$ on the additive group of $\mathbb{Z}/N$, and require that ψ *not* be well-defined modulo N' for any proper divisor N' of N.

Let χ be a *multiplicative character* $\chi : (\mathbb{Z}/N)^\times \to \mathbb{C}^\times$, extended by 0 to non-invertible elements of $\mathbb{Z}/N$. The corresponding Gauss sum is essentially an inner product in space of $\mathbb{C}$-valued functions on $\mathbb{Z}/N$:

$$g(\chi,\psi) \;=\; \sum_{x \bmod N} \chi(x)\cdot\psi(x)$$

The character χ is *primitive* mod N if it is *not* well-defined on $\mathbb{Z}/N'$ for any proper divisor N' of N. Then say that χ has *conductor* N. This distinction has immediate consequences:

[0.0.1] Claim: $g(\chi,\psi) = 0$ for χ *not* primitive mod N.

Proof: Non-primitivity means that there is N' a proper divisor of N such that χ is well-defined modulo N'. This means that $\chi(1+kN') = \chi(1) = 1$ for all $k \in \mathbb{Z}$. Then

$$g(\chi,\psi) \;=\; \sum_{x \bmod N} \chi(x)\cdot\psi(x) \;=\; \sum_{x \bmod N} \chi(x(1+kN')^{-1})\cdot\psi(x)$$

where the inverse means in $\mathbb{Z}/N$. Replacing x by $x(1+kN')$ gives

$$g(\chi,\psi) \;=\; \sum_{x \bmod N} \chi(x)\cdot\psi(x(1+kN')) \;=\; \sum_{x \bmod N} \chi(x)\cdot\psi(x)\cdot\psi(x\cdot kN')$$

By the *cancellation lemma*, summing $\psi(xkN')$ over k mod N/N' produces either N/N' or 0 depending whether $k \to \psi(xkN')$ is the trivial character or not. The character $k \to \psi(xkN')$ is trivial exactly when $N|xN'$. Since N' is a *proper* divisor of N, this can happen only when x has a non-trivial common factor with N. But then $\chi(x) = 0$. Thus,

$$\frac{N}{N'}\cdot g(\chi,\psi) \;=\; \sum_{k \bmod N/N'} g(\chi,\psi) \;=\; \sum_{k \bmod N/N'} \Big(\sum_{x \bmod N} \chi(x)\cdot\psi(x)\cdot\psi(x\cdot kN')\Big)$$

$$=\; \sum_{x \bmod N} \chi(x)\cdot\psi(x)\,\Big(\sum_{k \bmod N/N'} \psi(x\cdot kN')\Big) \;=\; \sum_{x \bmod N} 0 \;=\; 0$$

since in every summand either $\chi(x) = 0$ or the inner sum over k is 0. ///

[0.0.2] Claim: For primitive χ mod N,

$$|g(\chi,\psi)|^2 \;=\; N$$

Proof: Start the computation in the obvious fashion, writing $\psi(a) = e^{2\pi i a/N}$. Let Σ' denote sum over $(\mathbb{Z}/N)^\times$, and Σ'' denote sum over $\mathbb{Z}/N - (\mathbb{Z}/N)^\times$.

$$\Big|\sum_{a \bmod N} \chi(a)\,\psi(a)\Big|^2 \;=\; {\sum_{a,b}}'\; \chi(a)\,\psi(a)\,\overline{\chi}(b)\,\psi(-b)$$

Replacing a by ab, this becomes

$$\sum_{a,b}{}' \chi(a)\, \psi\big((a-1)\cdot b\big)$$

We claim that, because χ has conductor N (and not smaller!)

$$\sum_{a}{}' \chi(a)\, \psi((a-1)\cdot b) \;=\; 0 \qquad\qquad (\text{for } \gcd(b,N) > 1)$$

To see this, let p be a prime dividing $\gcd(b,N)$. That N is the conductor of χ is to say that χ is *primitive* mod N, meaning that χ does not factor through *any* quotient $\mathbb{Z}/(N/p)$. That is, there is some $\eta = 1 \bmod N/p$ such that $\chi(\eta) \neq 1$.

Since $p|b$, and $\eta = 1 \bmod N/p$,

$$(a\eta - 1)\cdot b \;=\; (a-1)b + a(\eta-1)b \;=\; (a-1)b \bmod N$$

Thus, replacing a by ηa,

$$\sum_{a}{}' \chi(a)\, \psi((a-1)\cdot b) \;=\; \sum_{a}{}' \chi(a\eta)\, \psi((a\eta-1)\cdot b) \;=\; \chi(\eta) \sum_{a}{}' \chi(a)\, \psi((a-1)\cdot b)$$

Thus, the sum over a is 0. Thus, we can drop the coprimality constraint:

$$\sum_{a,b}{}' \chi(a)\, \psi\big((a-1)\cdot b\big) \;=\; \sum_{a,b} \chi(a)\, \psi\big((a-1)\cdot b\big)$$

For $a \neq 1$, the inner sum over b is 0, because the sum of a non-trivial character over a finite group is 0. For $a = 1$ the sum over b gives N. ///
