GAUSS SUMS

ALLAN LIND JENSEN

for Neil Koblitz: Introduction to Elliptic Curves and Modular Forms, Chapter 4, Section 2

Definitions and first results

Let $n > 0$ be an odd integer. The Gauss sums are defined by

$$S(n) = \sum_{j=1}^{n} \left(\frac{j}{n}\right) e^{2\pi i j/n} \ . \tag{1}$$

I will soon be proven, that is n fails to be square-free, then $S(n) = 0$. Otherwise,

Theorem 1. *(Gauss) When n is a square-free odd integer*

$$S(n) = \varepsilon_n \sqrt{n}, \tag{2}$$

where

$$\varepsilon_n = \begin{cases} 1 & \text{if} \quad n \equiv 1 \mod 4 \\ i & \text{if} \quad n \equiv 3 \mod 4 \end{cases} \tag{3}$$

We need the more general sum

$$S(n, l) = \sum_{j=1}^{n} \left(\frac{j}{n}\right) e^{2\pi i l j/n} = \sum_{j \in \ \mathbb{Z}/n\mathbb{Z}} \left(\frac{j}{n}\right) e^{2\pi i l j/n}. \tag{4}$$

If $(l, n) = 1$, then the map $x \mapsto lx$ is $1 - 1$ in $\mathbb{Z}/n\mathbb{Z}$. Thus

$$S(n, l) = \left(\frac{l}{n}\right) \sum_{j \in \ \mathbb{Z}/n\mathbb{Z}} \left(\frac{lj}{n}\right) e^{2\pi i l j/n} = \left(\frac{l}{n}\right) S(n, 1) \ , \tag{5}$$

or more generally, still assuming $(n, l) = 1$

$$S(n, la) = \left(\frac{l}{n}\right) S(n, a) \ . \tag{6}$$

To find the values of the Gauss sums for general n, we first reduce to prime powers.

Theorem 2. *Assume that m and n are coprime, $(m, n) = 1$. Then*

$$S(mn, l) = \left(\frac{m}{n}\right) \left(\frac{n}{m}\right) S(m, l) S(n, l) \tag{7}$$

The idea of the proof is to parametrize $j = hm + kn$, where $h \in \mathbb{Z}/n\mathbb{Z}$ and $k \in \mathbb{Z}/m\mathbb{Z}$. This works, because the map

$$j \mapsto (j \bmod n, j \bmod m) \mapsto (m^{-1} \bmod n, k^{-1} \bmod m) \times (j \bmod n, j \bmod m)$$

is $1-1$. The first is $1-1$ by the Chinese remainder theorem, the second, because $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ and vice versa.

$$\begin{aligned} S(mn,l) &= \sum_{j\in\mathbb{Z}/mn\mathbb{Z}} \left(\frac{j}{mn}\right) e^{2\pi i l j/mn} \\ &= \sum_{h\in\mathbb{Z}/n\mathbb{Z}} \sum_{k\in\mathbb{Z}/m\mathbb{Z}} \left(\frac{hm+kn}{m}\right)\left(\frac{hm+kn}{n}\right) e^{2\pi i l(hm+kn)/mn} \\ &= \sum_{h,k} \left(\frac{kn}{m}\right)\left(\frac{hm}{n}\right) e^{2\pi i l h/n} e^{2\pi i l k/m} \\ &= \left(\frac{n}{m}\right)\left(\frac{m}{n}\right) \sum_h \left(\frac{h}{n}\right) e^{2\pi i l h/n} \sum_k \left(\frac{k}{m}\right) e^{2\pi i l k/m} \end{aligned}$$

□

You can probably see, how this in conjuction with (2) implies the quadratic reciprocity theorem. Following this line of thought leads to

Theorem 3. *Let $m, n > 0$ be odd, positive integers, that are mutually prime. Then*

$$S(mn,l) = \frac{S(m,l)}{\varepsilon_m} \cdot \frac{S(n,l)}{\varepsilon_n} \cdot \varepsilon_{mn} \ . \tag{8}$$

Prime powers

Now, We are ready to work on $S(p^\nu, l)$. The case $\nu = 1$ is covered by (5), which remains true even if $p|l$. In that case, $S(p,l) = \sum_j \left(\frac{j}{p}\right) \cdot 1 = 0$.

Assume that $\nu \geq 2$. We parametrize $j = ap + b$, where $0 \leq a < p^{\nu-1}$ and $1 \leq b \leq p$, and compute

$$\begin{aligned} S(p^\nu, l) &= \sum_{a=0}^{p^{\nu-1}-1} \sum_{b=1}^{p} \left(\frac{ap+b}{p}\right)^\nu e^{2\pi i l a/p^{\nu-1}} e^{2\pi i l b/p^\nu} \\ &= \sum_{a=0}^{p^{\nu-1}-1} e^{2\pi i l a/p^{\nu-1}} \sum_{b=1}^{p} \left(\frac{b}{p}\right)^\nu e^{2\pi i l b/p^\nu}, \end{aligned}$$

Unless $p^{\nu-1}|l$, the first sum vanishes; if $p^{\nu-1} \nmid l$, then $e^{2\pi i l/p^{\nu-1}}$ is a non-trivial root of unity, and we sum over a number of full circles.

We have established,

$$\text{If } \nu \geq 2 \text{ and } p^{\nu-1} \nmid l, \text{ then } G(p^\nu, l) = 0 \ . \tag{9}$$

As a special case $S(p^2) = S(p^2, 1) = 0$, which implies that $S(n) = 0$, if n is divisible by an integral square.

Finally, write $l = \lambda p^{\nu-1}$, obtaining

$$S(p^\nu, \lambda p^{n-1}) = \sum_{a=1}^{p^{\nu-1}} 1^{a\lambda} \sum_{b=1}^{p} \left(\frac{b}{p}\right)^\nu e^{2\pi i \lambda b/p} \ .$$

There is the special case $p|\lambda$, and we must distinguish between even and odd values of ν. The inner sum yields

$\sum_{b=1}^p \left(\frac{b}{p}\right)^\nu e^{2\pi i\lambda b/p}$	$p\vert\lambda$	$p\nmid\lambda$
$2\vert\nu$	$p-1$	-1
$2\nmid\nu$	0	$S(p,\lambda)$

and the Gauss sum of prime powers becomes

$$
\begin{array}{c|c|c}
S(p^\nu,\lambda p^{\nu-1}) & p|\lambda & p\nmid\lambda \\
\hline
2|\nu & p^\nu - p^{\nu-1} & -p^{\nu-1} \\
2\nmid\nu & 0 & p^{\nu-1}S(p,\lambda)
\end{array}
\tag{10}
$$

It turns out, that (10) also holds for $\nu = 1$.

The Gauss sums needed in the book

From now on, n and n_i represent odd integers.

The formula (10 can be reformulated the following way

$$
S(p^h, p^{2\nu}) = \begin{cases} 0 & \text{if} \quad h > 2\nu+1 \\ p^{2\nu}S(p,1) & \text{if} \quad h = 2\nu+1 \\ 0 & \text{if} \quad 0 < h < 2\nu, \text{ odd} \\ p^{h-1}\cdot(p-1) & \text{if} \quad 0 < h \le 2\nu, \text{ even} \\ 1 & \text{if} \quad h = 0 \end{cases} \tag{11}
$$

and

$$
S(p^h, p^{2\nu-1}) = \begin{cases} 0 & \text{if} \quad h > 2\nu \\ -p^{2\nu-1} & \text{if} \quad h = 2\nu \\ 0 & \text{if} \quad 0 < h \le 2\nu-1, \text{ odd} \\ p^{h-1}\cdot(p-1) & \text{if} \quad 0 < h \le 2\nu-1, \text{ even} \\ 1 & \text{if} \quad h = 0 \end{cases} \tag{12}
$$

Lemma 1. *(p. 188-9) If l is squarefree, write $n = n_0 n_1^2$, where n_0 is squarefree. Then*

$$
S(n,l) = \begin{cases} \varepsilon_n \left(\frac{l}{n_0}\right)\mu(n_1)\sqrt{n} & \textit{if} \quad n_1|l \\ 0 & \textit{otherwise,} \end{cases} \tag{13}
$$

where μ is the Möbius function.

Write $n_1 = \prod p_i^{\nu_i}$. Then

$$
S(n,l)\varepsilon_n^{-1} = S(n_0,l)\varepsilon_{n_0}^{-1}\prod S(p_i^{2\nu_i},l)\varepsilon_{p_i^{2\nu_i}}^{-1} \;.
$$

Of course, $\varepsilon_{p_i^{2\nu_i}} = 1$ and $\varepsilon_{n_0 n_1^2} = \varepsilon_{n_0}$.

If some $p_i \nmid l$ then $S(p_i^{2\nu_i}, l) = 0$. Since l is squarefree, it also vanishes if $\nu_i \geq 2$ It also vanishes, if $p_i|n_0$, but in that case $\left(\frac{l}{n_0}\right) = 0$.

In case $n_1|l$, and no prime $p_i|n_0$, we apply $S(p_i^2, l) = -p_i$, obtaining

$$
S(n,l) = \left(\frac{l}{n_0}\right)\sqrt{n_0}\;\varepsilon_n\prod(-p_i) = \left(\frac{l}{n_0}\right)\varepsilon_n\sqrt{n_0}\;\mu(n_1)n_1 \;.
$$

$\square$

Computation of $b_{l_0 p^{2\nu}}/b_{l_0}$

The final challenge is to derive the expressions for $b_{l_0 p^{2\nu}}/b_{l_0}$, where $p \nmid l_0$ or $p||l_0$.

The easy case is $p = 2$. For odd n, formula (6) results in

$$S(l_0 2^{2\nu}) = \left(\frac{2^{2\nu}}{n}\right) S(n, 1_0) = \left(\frac{2^{\nu}}{n}\right)^2 S(n, 1_0) = S(n, l_0) \ , \tag{14}$$

Thus

$$b_{l_0 4^\nu} = C \cdot l_0^{k/2-1} 2^{(k-2)\nu} \sum_n \varepsilon_n n^{-k/2} S(n, -l_0) = 2^{(k-2)\nu} b_{l_0}$$

The case: Odd $p||l_0$**.**

Write $l_0 = \tilde{l}_0 p$, so that $l = \tilde{l}_0 p^{2\nu+1}$, allowing $\nu = 0$. In (2.7) we write $n = n_0 p^h$, where $p \nmid n_0$, so that

$$\begin{aligned}
b_{\tilde{l}_0 p^{2\nu+1}} &= C \left(\tilde{l}_0 p^{2\nu+1}\right)^{\frac{k}{2}-1} \sum_n \varepsilon_n^k n^{-\frac{k}{2}} S(n, -l) \\
&= C l_0^{\frac{k}{2}-1} p^{\nu\cdot(ki-2)} \sum_{n_0, h} \varepsilon_{n_0 p^h}^k n_0^{-\frac{k}{2}} p^{-\frac{hk}{2}} S(n_0 p^h, -\tilde{l}_0 p^{2\nu+1}) \\
&= C l_0^{\frac{k}{2}-1} p^{\nu\cdot(ki-2)} \sum_{n_0, h} \varepsilon_{n_0 p^h}^{k+1} n_0^{-\frac{k}{2}} p^{-\frac{hk}{2}} S(n_0, -\tilde{l}_0 p^{2\nu+1}) S(p^h, -\tilde{l}_0 p^{2\nu+1}) \varepsilon_{p^h}^{-1} \varepsilon_{n_0}^{-1} \\
&= C l_0^{\frac{k}{2}-1} p^{\nu\cdot(ki-2)} \sum_{n_0} \left(\frac{p}{n_0}\right) \varepsilon_{n_0}^{-1} n_0^{-\frac{k}{2}} S(n_0, -\tilde{l}_0) \sum_h \varepsilon_{n_0 p^h}^{k+1} \varepsilon_{p^h}^{-1} p^{-\frac{hk}{2}} \left(\frac{-\tilde{l}_0}{p}\right)^h S(p^h, h^{2\nu+1})
\end{aligned}$$

The value of $S(p^h, h^{2\nu+1})$ is only non-zero, when h is even. Thus

$$\begin{aligned}
b_{\tilde{l}_0 p^{2\nu+1}} &= C l_0^{\frac{k}{2}-1} p^{\nu\cdot(ki-2)} \sum_{p \nmid n} \left(\frac{p}{n}\right) \varepsilon_n^k n^{-\frac{k}{2}} \sum_h p^{\frac{hk}{2}} S(p^h, p^{2\nu+1}) \\
&= C l_0^{\frac{k}{2}-1} p^{\nu\cdot(ki-2)} \sum_{p \nmid n} \left(\frac{p}{n}\right) \varepsilon_n^k n^{-\frac{k}{2}} \cdot \left(1 + \sum_{j=1}^{\nu} p^{-kj} \cdot (p^{2j} - p^{2j-1}) + p^{-k(\nu+1}(-p^{2\nu+1})\right)
\end{aligned}$$

The parenthesis can be reduced to

$$\sum_{j=0}^{\nu} p^{(2-k)j} - \sum_{j=1}^{\nu+1} p^{(2-k)j-1} = p^{\nu\cdot(ki-2)} \left(1 - p^{1-k}\right) \sum_{j=0}^{\nu} p^{(2-k)j} \ .$$

Finally, we obtain

$$\frac{b_{l_0 p^{2\nu}}}{b_{l_0}} = p^{\nu\cdot(ki-2)} \sum_{j=0}^{\nu} p^{(2-k)j} = \sum_{j=0}^{\nu} p^{(k-2)j} \ , \tag{15}$$

which is the formula just above (2.24).

The case: Odd $p \nmid l_0$.

We compute

$$\begin{aligned} b_{l_0p^{2\nu}} &= C\left(l_0p^{2\nu}\right)^{\frac{k}{2}-1}\sum_{n_0,h}\varepsilon^k_{n_0p^h}(n_0p^h)^{-\frac{k}{2}}S(n_0p^h,-l_0p^{2\nu}) \\ &= Cl_0^{\frac{k}{2}-1}p^{(k-2)\nu}\sum_{n_0,h}\varepsilon^{k+1}_{n_0p^h}n_0^{-\frac{k}{2}}p^{-\frac{hk}{2}}S(n_0,-l_0p^{2\nu})S(p^h,-l_0p^{2\nu})\varepsilon^{-1}_{n_0}\varepsilon^{-1}_{p^h} \\ &= Cl_0^{\frac{k}{2}-1}p^{(k-2)\nu}\sum_{n_0}\varepsilon^{-1}_{n_0}n_0^{-\frac{k}{2}}S(n_0,-l_0)\sum_h\varepsilon^{k+1}_{n_0p^h}p^{-\frac{hk}{2}}\left(\frac{-l_0}{p}\right)^hS(p^h,p^{2\nu})\varepsilon^{-1}_{p^h}\end{aligned}$$

There is only *one* odd value of h for which $S(p^h,p^{2\nu})\neq 0$, i.e. $h=2\nu+1$. In the evaluation of this term we need the observation, that since $k+1$ is even, and $\lambda=\frac{k-1}{2}$, we can apply $\varepsilon_n^2=\left(\frac{-1}{n}\right)$ to obtain

$$\varepsilon^{k+1}_{pn}=\left(\frac{-1}{pn}\right)^{\lambda+1}=\left(\frac{-1}{p}\right)^{\lambda+1}\left(\frac{-1}{n}\right)^{\lambda+1}=\left(\frac{-1}{p}\right)^{\lambda+1}\cdot\varepsilon^{k+1}_n\ .$$

The odd addend of the sum gives

$$\varepsilon^{k+1}_{n_0p}p^{-k\nu-\frac{k}{2}}\left(\frac{-l_0}{p}\right)p^{2\nu}\varepsilon_p\sqrt{p}\varepsilon_p^{-1}=\left(\frac{-1}{p}\right)^{\lambda+1}\varepsilon^{k+1}_{n_0}\left(\frac{-l_0}{p}\right)p^{-(k-2)\nu-\lambda}=\varepsilon^{k+1}_{n_0}\chi(p)p^{-(k-2)\nu-\lambda}\ .$$

where $\chi=\chi_{(-)^\lambda l_0}$. Including the even values leads to

$$b_{\tilde{l}_0p^{2\nu}}=Cl_0^{\frac{k}{2}-1}p^{\nu\cdot(k-2)}\sum_{p\nmid n}\varepsilon^k_{n_0}n^{-\frac{k}{2}}S(n_0,-l_0)\left(1+\chi(p)p^{-(k-2)\nu-\lambda}+\sum_{j=1}^{\nu}p^{-kj}\left(p^{2j}-p^{2j-1}\right)\right) \tag{16}$$

This is basically (2.28). We obtain

$$\begin{aligned}\frac{b_{\tilde{l}_0p^{2\nu}}}{b_{\tilde{l}_0}} &= \frac{p^{(k-2)\nu}\left(1+\chi(p)p^{-\lambda}+\sum_{j=1}^{\nu}\left(p^{(2-k)j}-p^{(2-k)j-1}\right)\right)}{1+\chi(p)p^{-\lambda}} \\ &= \frac{\sum_{j=0}^{\nu}p^{(k-2)j}-\sum_{j=0}^{\nu-1}p^{(k-2)j-1}+\chi(p)p^{-\lambda}}{1+\chi(p)p^{-\lambda}} \\ &= \sum_{j=0}^{\nu}p^{(k-2)j}-\chi(p)p^{\lambda-1}\sum_{j=0}^{\nu-1}p^{(k-2)j}\end{aligned}$$

The verification of the last expression is elementary, but not trivial. One needs the relation $k=2\lambda+1$.