# 18.785 Analytic Number Theory Problem Set #4

Holden Lee

2/21/11

## Problem 1 *(Nonvanishing Poincaré series)*

The $n$th Fourier coefficient of $P_n(z)$, the Poincaré series of weight $k$, is

$$p(n,n) = 1 + \frac{2\pi}{i^k h} \sum_{c>0} c^{-1} S_\Gamma(n/h, n/h; c) J_{k-1}\left(\frac{2\pi n}{ch}\right).$$

To show that the Poincaré series does not vanish, it suffices to show $p(n,n) \neq 0$. For this, it suffices to show that $|A| < 1$ where $A = \frac{2\pi}{i^k h} \sum_{c>0} c^{-1} S_\Gamma(n/h, n/h; c) J_{k-1}\left(\frac{2\pi n}{ch}\right)$. Note that any $c$ in the sum is an integer because $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$.

We assume $k > 4$ and the smallest $c$ is greater than 1 (so at least 2). Below $C_1, C_2, \ldots$ will represent constants.

First, [2, 4.1] gives the bound

$$J_k(x) \leq (2\pi k)^{-\frac{1}{2}} \left(\frac{ex}{2k}\right)^k.$$

Hence (noting $h \geq 1$),

$$J_{k-1}\left(\frac{4\pi n}{ch}\right) \leq (2\pi(k-1))^{-\frac{1}{2}} \left(\frac{2\pi e n}{(k-1)ch}\right)^{k-1} \leq C_1 (2\pi e)^k \frac{n^{k-1}}{(k-1)^{k-\frac{1}{2}} c^{k-1}}.$$

From Proposition 4.9.1,

$$|S_\Gamma(m,n;c)| \leq c^2 \cdot c(s,s)^{-1}.$$

Putting these two estimates together, and letting $c_0 = c(s,s)$,

$$\begin{aligned} A &\leq C_2 (2\pi e)^k \frac{n^{k-1}}{c_0 (k-1)^{k-\frac{1}{2}}} \sum_{c \geq c_0} \frac{1}{c^{k-3}} \\ &\leq C_2 (2\pi e)^k \frac{n^{k-1}}{c_0 (k-1)^{k-\frac{1}{2}}} \int_{c_0 - 1}^{\infty} \frac{1}{x^{k-3}}\, dx \\ &= C_2 (2\pi e)^k \frac{n^{k-1}}{c_0 (k-1)^{k-\frac{1}{2}}} \frac{(c_0-1)^{-k+4}}{k-4}. \end{aligned} \tag{1}$$

This is at most 1 if

$$\begin{aligned}
&n^{k-1} \le C_3(2\pi e)^{-k}(k-1)^{k-\frac{1}{2}}(k-4)c_0^{-1}(c_0-1)^{k-4} \\
&\Leftarrow n \le C_4 k(c_0-1) \\
&\Leftarrow n \le C_5 k c_0.
\end{aligned}$$

Thus if $n \le C_5 k c_0$ then $P_n(z)$ does not vanish.

If instead $c_0 = 1$, then by letting $n \le Ckc_0 = Ck$ with appropriate $C$, we may assume that term $c = 1$ in the sum (1) is less than a constant, say $\frac{1}{2}$, since

$$C_2(2\pi k)^k \frac{n^{k-1}}{(k-1)^{k-\frac{1}{2}}} \frac{1}{c_0^{k-4}} \le C_2(2\pi e)^k \frac{C(Ck)^{k-1}}{(k-1)^{k-\frac{1}{2}}} \le C_2(2\pi eC)^k \left(\frac{k}{k-1}\right)^{k-1} \le C_2(2\pi eC)^k \cdot e.$$

Then it suffices for the rest of the terms to sum to at most $\frac{1}{2}$. Replacing the lower limit in the integral estimate with $c_0$, the proof goes the same as before with modified constants.

## Problem 2 *(Kloosterman sums)*

**(A)** $S(m,n;c) = S(n,m;c)$
The definition of $S(m,n;c)$ is symmetric in both $m$ and $n$:

$$S(n,m;c) = \sum_{d_1 d_2 \equiv 1 \,(\mathrm{mod}\, c)} e\left(\frac{nd_1 + md_2}{c}\right).$$

**(B)** $S(an,m;c) = S(n,am;c)$ **if** $\gcd(a,c) = 1$

$$\begin{aligned}
S(an,m;c) &= \sum_{d_1 d_2 \equiv 1 \,(\mathrm{mod}\, c)} e\left(\frac{and_1 + md_2}{c}\right) \\
&= \sum_{d \,(\mathrm{mod}^\times c)} e\left(\frac{and + m\overline{d}}{c}\right) \\
&= \sum_{d \,(\mathrm{mod}^\times c)} e\left(\frac{an(\overline{a}d) + m\overline{\overline{a}d}}{c}\right) \qquad (2) \\
&= \sum_{d \,(\mathrm{mod}^\times c)} e\left(\frac{nd + am\overline{d}}{c}\right) \\
&= \sum_{d_1 d_2 \equiv 1 \,(\mathrm{mod}\, c)} e\left(\frac{nd_1 + amd_2}{c}\right) \\
&= S(n,am;c)
\end{aligned}$$

In (2), we replaced $d$ with $\overline{a}d$; this is legitimate since $\gcd(a,c) = 1$ and as $d$ ranges over the units modulo $c$, so does $\overline{a}d$.

**(C)** $S(n,m,c) = \sum_{d \mid \gcd(c,m,n)} dS(mnd^{-2}, 1; cd^{-1})$
We prove this for $c = p^r$ a prime power.

**Lemma 2.1:**

$$\sum_{d\,(\mathrm{mod}^{\times} p^r)} e\left(\frac{d}{p^r}\right) = \begin{cases} -1, & r > 1 \\ 0, & r = 1. \end{cases}$$

*Proof.* For $r = 1$, just note that the sum of roots of unity $\sum_{d\,(\mathrm{mod}\,p)} e\left(\frac{d}{p}\right) = 0$.

For $r > 1$, using the fact that the sum of $k$th roots of unity is 0 for any $k > 1$,

$$\sum_{d\,(\mathrm{mod}^{\times} p^r)} e\left(\frac{d}{p^r}\right) = \sum_{d\,(\mathrm{mod}\,p^r)} e\left(\frac{d}{p^r}\right) - \sum_{d\,(\mathrm{mod}\,p^{r-1})} e\left(\frac{d}{p^{r-1}}\right) = 0 - 0 = 0.$$

□

**Lemma 2.2:** Suppose $p|m$ and $r \geq 2$. Then $S(m, 1; p^r) = 0$.

*Proof.* Write $m = p^k l$ with $p \nmid l$. Consider two cases.

1. $k < r$: Then

$$\begin{aligned} S(m, 1; p^r) &= \sum_{d\,(\mathrm{mod}^{\times} p^r)} e\left(\frac{p^k l d + \overline{d}}{p^r}\right) \\ &= \sum_{x\,(\mathrm{mod}\,p^k)} \sum_{a\,(\mathrm{mod}^{\times} p^{r-k})} e\left(\frac{p^k l(p^{r-k}x + a) + \overline{p^{r-k}x + a}}{p^r}\right) \\ &= \sum_{a\,(\mathrm{mod}^{\times} p^{r-k})} \sum_{x\,(\mathrm{mod}\,p^k)} e\left(\frac{p^k l a + \overline{p^{r-k}x + a}}{p^r}\right) \end{aligned} \tag{3}$$

   As $x$ ranges from 1 to $p^k$, $\overline{p^{r-k}x + a}$ attains the values $\overline{a} + p^{r-k}b$ for all $b\,(\mathrm{mod}\,p^k)$. Now the $e\left(\frac{p^k l a + \overline{a} + p^{r-k}b}{p^r}\right)$ for $a$ fixed and $b$ varying modulo $p^k$ are equally spaced on the unit circle so sum to 0. Hence the inner sum in (3) is 0.

2. $k \geq r$: Then

$$\begin{aligned} S(m, 1; p^r) &= \sum_{d\,(\mathrm{mod}^{\times} p^r)} e\left(\frac{p^k l \overline{d} + d}{p^r}\right) \\ &= \sum_{d\,(\mathrm{mod}^{\times} p^r)} e\left(\frac{d}{p^r}\right) \\ &= 0 \end{aligned}$$

   by Lemma 2.1.

□

Let $\gcd(n,m,c)=p^k$. Write $n=p^kn'$ and $m=p^km'$; note that $p$ does not divide both $m'$ and $n'$.

Then

$$\begin{aligned}\sum_{d|\gcd(c,m,n)} dS(mnd^{-2},1;cd^{-1}) &= \sum_{d|p^k} dS(m'n'p^{2k}d^{-2},1;p^rd^{-1})\\ &= \sum_{i=0}^{k} p^iS(m'n'p^{2k-2i},1;p^{r-i})\end{aligned}$$

If $k<r$ then all terms except the last are 0 by Lemma 2.2, so this equals

$$\begin{aligned}p^kS(m'n',1;p^{r-k}) &= p^kS(m',n';p^{r-k}) &(4)\\ &= p^k\sum_{d\,(\mathrm{mod}^\times p^{r-k})} e\left(\frac{m'd+n'\overline{d}}{p^{r-k}}\right)\\ &= \sum_{d\,(\mathrm{mod}^\times p^{r})} e\left(\frac{p^km'd+p^kn'\overline{d}}{p^{r}}\right) &(5)\\ &= S(m,n;c)\end{aligned}$$

In (4) we used (B), noting that one of $m',n'$ is relatively prime to $p$, and in (5) we note that the invertible residues modulo $p^r$ cover the invertible residues modulo $p^{r-k}$, $p^k$ times.

If instead $k=r$ then all terms except the last two are 0 by Lemma 2.2, and the sum equals

$$\begin{aligned}p^rS(m'n',1;1)+p^{r-1}S(m'n'p^2,1;p) &= p^r-p^{r-1}\\ &= \varphi(p^r)\\ &= S(p^rm',p^rn';p^r).\end{aligned}$$

Note we used $S(m'n',1;p)=\sum_{d\,(\mathrm{mod}^\times p)} e\left(\frac{d}{p}\right)=-1$ by Lemma 2.1.

**(D)** $S(m,n;c)=S(\overline{d_1}m,\overline{d_1}n;d_2)S(\overline{d_2}m,\overline{d_2}n;d_1)$

Denote by $f(r_1,r_2)$ the unique residue modulo $d_1d_2$ which is congruent to $r_1$ modulo $d_2$ and $r_2$ modulo $d_1$. (It's well defined by the Chinese Remainder Theorem.)

$$\begin{aligned}S(\overline{d_1}m,\overline{d_1}n;d_2)S(\overline{d_2}m,\overline{d_2}n;d_1) &= \sum_{a_1\,(\mathrm{mod}^\times d_2)} e\left(\frac{m\overline{d_1}a_1+n\overline{d_1}\overline{a_1}}{d_2}\right)\sum_{a_2\,(\mathrm{mod}^\times d_1)} e\left(\frac{m\overline{d_2}a_2+n\overline{d_2}\overline{a_2}}{d_1}\right)\\ &= \sum_{\substack{a_1\,(\mathrm{mod}^\times d_2)\\ a_2\,(\mathrm{mod}^\times d_1)}} e\left(\frac{(m\overline{d_1}a_1d_1+m\overline{d_2}a_2d_2)+(n\overline{d_1}\overline{a_1}d_1+m\overline{d_2}\overline{a_2}d_2)}{d_1d_2}\right)\\ &= \sum_{\substack{a_1\,(\mathrm{mod}^\times d_2)\\ a_2\,(\mathrm{mod}^\times d_1)}} e\left(\frac{f(ma_1,ma_2)+f(n\overline{a_1},n\overline{a_2})}{d_1d_2}\right).\end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{a_1 \,(\mathrm{mod}^\times d_2)\\ a_2 \,(\mathrm{mod}^\times d_1)}} e\left(\frac{mf(a_1,a_2)+n\overline{f(a_1,a_2)}}{d_1d_2}\right)\\
&= \sum_{a\,(\mathrm{mod}^\times d_1d_2)} e\left(\frac{ma+n\bar{a}}{d_1d_2}\right)\\
&= S(m,n;c).
\end{aligned}
$$

We used the fact that the units modulo $d_1d_2$ are exactly the residues which are units both modulo $d_1$ and modulo $d_2$, by the Chinese Remainder Theorem.

## Problem 3 *(Salié sum)*

### (A)

**Lemma 3.1:** Suppose $2m$ is relatively prime to $c$. Then

$$\left(\frac{m}{c}\right) g(n,c) = g(mn,c).$$

*Proof.* From [1, 4.8], $g(n,c) = \varepsilon_c \left(\frac{n}{c}\right)\sqrt{c}$ where

$$\varepsilon_c = \begin{cases} 1, & c \equiv 1 \pmod 4\\ i, & c \equiv 3 \pmod 4. \end{cases}$$

Hence

$$\left(\frac{m}{c}\right) g(n,c) = \varepsilon_c \left(\frac{m}{c}\right)\left(\frac{n}{c}\right)\sqrt{c} = \varepsilon_c \left(\frac{mn}{c}\right)\sqrt{c} = g(mn,c).$$

□

**Lemma 3.2** (Ramanujan sum)**:** Let $\zeta_q$ be a primitive $q$th root of unity, and let

$$c_q(n) = \sum_{a\,(\mathrm{mod}^\times q)} \zeta_q^{an}.$$

Then

$$c_q(n) = \sum_{d|\gcd(q,n)} d\mu\left(\frac{q}{d}\right).$$

*Proof.* Let $\eta_q(n) = \sum_{k=1}^{q} \zeta_q^{kn}$. Since all $q$th roots of unity are primitive $d$th roots of unity for exactly one $d|q$,

$$\eta_q(n) = \sum_{d|q} c_d(n).$$

By Möbius inversion,

$$c_q(n) = \sum_{d|q} \mu\left(\frac{q}{d}\right)\eta_d(n).$$

But the sum $\eta_q(n) = \sum_{k=1}^{d} \zeta_d^{nk}$ is 0 unless $d|n$, in which case it equals $d$ (each term being 1). This gives the lemma. □

$$
\begin{aligned}
\hat{F}(y) &= \sum_{x \,(\mathrm{mod}\, c)} \sum_{d \,(\mathrm{mod}^{\times} c)} \left(\frac{d}{c}\right) e\left(\frac{m\overline{d} + ndx^2}{c}\right) e\left(\frac{-yx}{c}\right) \\
&= \sum_{d \,(\mathrm{mod}^{\times} c)} \sum_{x \,(\mathrm{mod}\, c)} \left(\frac{d}{c}\right) e\left(\frac{nd\left(x - \frac{y}{2nd}\right)^2 - \frac{y^2-4mn}{4nd}}{c}\right) \\
&= \sum_{d \,(\mathrm{mod}^{\times} c)} \sum_{t \,(\mathrm{mod}\, c)} \left(\frac{d}{c}\right) e\left(\frac{ndt^2 - \frac{y^2-4mn}{4nd}}{c}\right) \\
&= \sum_{d \,(\mathrm{mod}^{\times} c)} \left(\frac{d}{c}\right) g(nd, c) e\left(\frac{-\frac{y^2-4mn}{4nd}}{c}\right) \\
&= \sum_{d \,(\mathrm{mod}^{\times} c)} g(nd^2, c) e\left(\frac{-(y^2-4mn)}{c} \cdot \frac{1}{4n} \cdot \frac{1}{d}\right) \qquad \text{by Lemma 3.1} \\
&= g(n,c) \sum_{d \,(\mathrm{mod}^{\times} c)} e\left(\frac{\gcd(4mn - y^2, c)d}{c}\right) \qquad (6) \\
&= g(n,c) \sum_{d \mid \gcd(4mn-y^2, c)} d\mu\left(\frac{c}{d}\right).
\end{aligned}
$$

In (6) we replaced $\frac{1}{d}$ by $4nd \cdot \frac{\gcd(4mn-y^2,c)}{c}$, which is legit since $4n \cdot \frac{\gcd(4mn-y^2,c)}{c}$ is a unit modulo $c$. We used $g(nd^2, c) = \sum_{t \,(\mathrm{mod}\, c)} e\left(\frac{n(dt)^2}{c}\right) = \sum_{t \,(\mathrm{mod}\, c)} e\left(\frac{nt^2}{c}\right) = g(n,c)$, since as $t$ ranges over units modulo $c$ so does $dt$.

**(B)**

Taking the inverse Fourier Transform of (A) gives

$$
\begin{aligned}
F(x) &= \frac{1}{c} \sum_{y \,(\mathrm{mod}\, c)} \left( e\left(\frac{xy}{c}\right) g(n,c) \sum_{d \mid \gcd(4mn-y^2, c)} d\mu\left(\frac{c}{d}\right) \right) \\
&= g(n,c) \frac{1}{c} \sum_{d \mid c} \left[ d\mu\left(\frac{c}{d}\right) \sum_{y \,(\mathrm{mod}\, c), d \mid 4mn - y^2} e\left(\frac{xy}{c}\right) \right] \qquad (7) \\
&= g(n,c) \frac{1}{c} \sum_{y^2 \equiv 4mn \,(\mathrm{mod}\, c)} ce\left(\frac{xy}{c}\right) \\
&= g(n,c) \sum_{y^2 \equiv mn \,(\mathrm{mod}\, c)} e\left(\frac{2xy}{c}\right)
\end{aligned}
$$

Note that in (7) the inner sum for $d \neq c$ is 0, because a solution $y$ to $d | 4mn - y^2$ can be grouped with the solutions $y + dk$ for $0 \leq k < \frac{c}{d}$, and the resulting $e\left(\frac{xy}{c}\right)$ are evenly spaced around the unit circle (for $x$ invertible modulo $c$) and sum to 0.

In particular, putting in $x = 1$ gives

$$T(m, n; c) = g(n, c) \sum_{y^2 \equiv mn \pmod{c}} e\left(\frac{2y}{c}\right).$$

## Problem 4 *(Line bundles)*

**(A)**
Let $K = \mathbb{R}$ or $\mathbb{C}$.

The trivial line bundle $\pi' : M \times K \to M$ has the nonvanishing section $g$ defined by

$$g(m) = (m, 1).$$

Conversely suppose there is a nonvanishing section $f : M \to L$. Let $\pi : L \to M$ be the projection map. We find a way to identify $L$ with $M \times K$ so that $f$ is identified with the map $m \mapsto (m, 1)$ given above. Define $h : L \to M \times K$ as follows:

$$h(l) = \left(\pi(l), \frac{l}{f(\pi(l))}\right).$$

Since the fiber above $\pi(l)$ is a one-dimensional vector space and $f(\pi(l))$ does not correspond to the zero vector (as $f$ is nonvanishing), the division is well-defined. We claim that the following commutes:

$$\begin{tikzcd} L \arrow[r, "h"] & M \times K \\ M \arrow[u, "f"] \arrow[ur, "g"'] & \end{tikzcd}$$

Indeed, $h(f(m)) = \left(m, \frac{f(m)}{f(m)}\right) = (m, 1) = g(m)$. Note $h$ is a diffeomorphism: given $l \in L$, we can choose an open neighborhood $U$ around $\pi(l)$ so that $\pi^{-1}(U) = U \times K$; then the map from $U \times K \to M \times K$ induced by $h : L \to M \times K$ is clearly a diffeomorphism. It remains to note that $h$ carries $\pi^{-1}(l)$ bijectively to $\pi'^{-1}(l)$, and it is a linear transformation here, for each $l$.

**(B)**
The Möbius strip is not isomorphic to $S^1 \times \mathbb{R}$.

We identify $S^1$ with the reals modulo 1. Let $U_1 = (0, 1)$ and $U_2 = (.9, 1) \cup [0, .1)$. As a set, let $L$ be a copy of $S^1 \times \mathbb{R}$. Let $\pi : L \to S^1$ be the projection map. Give $\pi^{-1}(U_1)$ the same topology as the usual topology $U_1 \times \mathbb{R} \subseteq L$. However, define the topology on $U_2$ as follows: Let $h : \pi^{-1}(U_2) \to U_2 \times \mathbb{R}$ be the map defined by

$$h((x, y)) = \begin{cases} (x, y), & x \in (.9, 1) \\ (x, -y), & x \in [0, .1) \end{cases}$$

and topologize $\pi^{-1}(U_2)$ so that $h$ is a homeomorphism. Note the topology on $U_1 \cap U_2$ is consistent in both cases: on the component $(.9, 1)$ $h$ is simply the identity map on sets, while on the component $(0, .1)$ $h$ is the map $(a, b) \to (a, -b)$ which is a automorphism of $(0, .1) \times \mathbb{R}$. $L$ is known as the Möbius strip.

Now let $f$ be any section $S^1 \to L$. Write $f$ as $f(x) = (x, f_1(x))$. Then from the topology on $L$, in order for $f$ to be continuous,

$$f(0) = -\lim_{x \to 1^-} f(x).$$

If $f_1(0) = 0$ then $f$ vanishes, else, $f_1(0)$ and $f_1(1 - \varepsilon)$ are of different sign for small $\varepsilon$, so $f_1$ vanishes somewhere on $(0, 1)$ and again $f$ vanishes. Thus by (A), $L \not\cong S^1 \times \mathbb{R}$.

# References

[1] Iwaniec, H.: "Topics in Classical Automorphic Forms," AMS, 1997.

[2] Rankin, R.: "The Vanishing of Poincaré Series," *Proceedings of the Edinburgh Mathematical Society* (1980), 23, 151-161.