Analysis Junior Seminar: Final Paper

December 20, 2016

Yash Patel

1 Introduction

Throughout the past semester, I have learned a great deal regarding analysis, particularly in its applications to number theory. Prior to the seminar, I had little exposure to the applications of many analysis results but now see their wide reaching scopes. In this paper, I present a thorough breakdown of the two talks I gave in the semester, namely the first regarding Singular Integrals and the second about a key lemma in the two-squares proof.

2 Singular Method/Integral

2.1 Introduction

In this lecture, I will be picking up from where the previous lecture left off, namely after defining the A_q. The end result of this lecture will be demonstrating that $\forall d \geq 5$, for all sufficiently large n, n can be represented as a sum of d squares. To reach that conclusion, however, we need to bound the terms/summations and calculate the specific numerical results, which I hope to do in the next 40 minutes.
So, the basic outline of the lecture is as follows:

1. Discuss the singular series
2. Bound the singular series and its error term
3. Discuss the singular integral as it relates to calculating r_n
4. Conclude by bounding the error term

2.2 Proposition 4.5

Having proven the above result about A_q, we proceed to demonstrate that this series has a convergent tail and is bounded. More specifically, we have the singular series (for $d \geq 5$),

$$\mathfrak{S} = \sum_{q=1}^{\infty} A_q(n)$$

converges absolutely, specifically with

$$\sum_{q>R}^{\infty} A_q(n) = O(R^{2-d/2})$$

$\forall R \geq 1$. Further, $\exists C_1, C_2$ such that:

$$C_1 \leq |\mathfrak{S}| \leq C_2$$

There are three main parts of this proof:

1. We demonstrate that this original summation is bounded, and so is a similarly defined variant $\psi_q(n)$
2. This leads us to formulate the $A_q(n)$ as an infinite product (and prove their equality)
3. We bound this infinite product from above and below non-trivially

2.2.1 Singular series convergence

Namely, by definition, we have that:

$$A_q(n) = \sum_{\substack{1\le p\le q\\(p,q)=1}} q^{-d} S(p/q)^d e^{-2\pi i p/q}$$

Where the $S(p/q)$ are themselves Gauss sums we have already discussed, defined as:

$$S(p/q) = \sum_{1\le n`q} e^{2\pi i n^2 p/q}$$

From Tim's lectures, we have the values for $S(p/q)$, whenever $(p,q)=1$, which were:

$$\begin{cases} \sqrt{q} & q \equiv 1 \mod 4 \\ i\sqrt{q} & q \equiv 3 \mod 4 \\ 0 & q \equiv 2 \mod 4 \\ e^{i\pi/4}\sqrt{2q} & q \equiv 0 \mod 4 \end{cases}$$

Applying this, we have:

$$|A_q(n)| = |\sum_{\substack{1\le p\le q\\(p,q)=1}} q^{-d} S(p/q)^d e^{-2\pi i p/q}| \le \sum_{\substack{1\le p\le q\\(p,q)=1}} |q^{-d} S(p/q)^d e^{-2\pi i p/q}| \tag{1}$$

$$= \sum_{\substack{1\le p\le q\\(p,q)=1}} |q^{-d}||S(p/q)^d||e^{-2\pi i p/q}| = \sum_{\substack{1\le p\le q\\(p,q)=1}} |q^{-d}||S(p/q)^d| \tag{2}$$

Thus, if $q \equiv 1 \mod 4$ or $q \equiv 3 \mod 4$, then $|S(p/q)^d| = |\sqrt{q}^d|$, if $q \equiv 3 \mod 4$ then the term is 0, and if $q \equiv 0 \mod 4$ then $|S(p/q)^d| = |\sqrt{2q}^d|$. Thus,

$$A_q(n) \le \begin{cases} \sum_{1\le p\le q} |q^{-d/2}| & q \equiv 1 \mod 4 or q \equiv 3 \mod 4 \\ 0 & q \equiv 2 \mod 4 \\ 2^{d/2} \sum_{1\le p\le q} |q^{-d/2}| & q \equiv 0 \mod 4 \end{cases}$$

Since $\sum_{1\le p\le q} |q^{-d/2}| = |q^{-d/2}| \sum_{1\le p\le q} 1 = q^{1-d/2}$, we have the desired bounds that:

$$|A_q(n)| \le c_d q^{1-d/2}$$

Where $c_d = 1$ for the odd cases and $2^{d/2-1}$ for the 0 case. Thus, with these bounds, we can bound the sum as:

$$\sum_{q=1}^{\infty} |A_q(n)| = O(\sum_{q=1}^{\infty} q^{1-d/2})$$

Since we can ignore the constants for bounding these error terms. From this, we can see that the series converges whenever we have the exponent ≤ -1, corresponding to a $d \ge 5$.
To now obtain the bound that we wanted to exhibit, we see that the tail of the series satisfies:

$$\sum_{q>R} |A_q(n)| = O(\sum_{q>R} q^{1-d/2}) = O(\sum_{q>R} R^{1-d/2})$$

Since $d \ge 5$, meaning the exponent $1 - d/2 < -1$ and that the function is decreasing in q, allowing us to bound the sum by considering the minimal element in the restricted domain.

With that, we now consider the other series:

$$\psi_q(n) = 1 + \sum_{j=1}^{\infty} A_{q^j}(n)$$

Whenever q is prime. We define this seemingly random series because it will turn out that $\mathfrak{S}$ can be written as an infinite product of these $\psi_q(n)$, which is insane. Before reaching that point, though, let's investigate some of its properties. Let's consider any prime $\neq 2$, that is, any odd prime. In that case:

$$|\psi_q(n) - 1| = |\sum_{j=1}^{\infty} A_{q^j}(n)| \tag{3}$$

$$\leq \sum_{j=1}^{\infty} (q^j)^{1-d/2} = \sum_{j=1}^{\infty} (q^{1-d/2})^j \tag{4}$$

$$= \frac{q^{1-d/2}}{1 - q^{1-d/2}} = \frac{1}{q^{d/2-1} - 1} \tag{5}$$

Which converges whenever $d \geq 5$. For the case of $q = 2$, we have that $A_2(n) = 0$, so:

$$|\psi_2(n) - 1| \leq \frac{1}{2^{d/2-1} - 1}$$

So, putting it all together, we have that the sum:

$$\sum_{\text{q prime}} |\psi_q(n) - 1| \leq \sum_{\text{q prime}} \frac{1}{q^{d/2-1} - 1}$$

By a theorem in complex analysis, the absolute convergence of this sum implies the convergence of the infinite product of the $\psi_q(n)$, meaning that it now makes sense to discuss its value.

2.2.2 Infinite product formulation (Prop 4.13)

Having proven the convergence, we now consider the following proposition about the infinite product of $\psi_q(n)$:

$$\mathfrak{S} = \sum_{q=1}^{\infty} A_q(n) = \prod_{\text{q prime}} \psi_q(n)$$

This follows immediately from another lemma of the multiplicative properties of $A_q(n)$. Specifically:
If $(q_1, q_2) = 1$, $A_{q_1,q_2}(n) = A_{q_1}(n)A_{q_2}(n)$
The desired infinite product is clear by the fact that we can write any $q \in \mathbb{Z}$ as a product of primes (by the fundamental theorem of arithmetic), meaning we can write any $A_q(n) = A_{q_1 q_2 \dots q_j}(n) = \prod_{i=1}^{j} A_{q_i}(n)$, which exactly defines how the infinite product is defined.
Thus, the only thing left to prove is this lemma. If we have $(p_1, q_1) = (p_2, q_2) = (q_1, q_2)$, by a previous proposition:

$$S\left(\frac{p_1 q_2 + p_2 q_1}{q_1 q_2}\right) = S(p_1/q_1)S(p_2/q_2)$$

Thus, we can simplify this as:

$$A_{q_1}(n)A_{q_2}(n) = \sum_{\substack{p_1 \bmod q_1 \\ (p_1,q_1)=1}} \sum_{\substack{p_2 \bmod q_2 \\ (p_2,q_2)=1}} q_1^{-d} q_2^{-d} S(p_1/q_1)^d S(p_2/q_2)^d e^{-\pi i n(p_1/q_1 + p_2/q_2)}$$

$$= \sum_{\substack{p_1 \bmod q_1 \\ (p_1,q_1)=1}} \sum_{\substack{p_2 \bmod q_2 \\ (p_2,q_2)=1}} (q_1q_2)^{-d} S\left(\frac{p_1q_2+p_2q_1}{q_1q_2}\right)^d e^{-\pi i n(p_1/q_1+p_2/q_2)}$$

Which is $= A_{q_1q_2}(n)$ since these values are relatively prime.

2.2.3 Bounding the sum

Finally, we conclude the proof by bounding this infinite product. Since we already showed that:

$$|\psi_q(n)-1| \leq \frac{1}{q^{d/2-1}-1} < 1$$

$|\psi_q(n)| \geq 1$ (if it were $= 0$, then the LHS would be 1), meaning that it is non-trivially bounded below, as desired. Specifically, since this only converges for $d \geq 5$, we consider such values, meaning that (for all relevant d)

$$|\psi_q(n)-1| \leq \frac{1}{q^{3/2}-1} < 1$$

Explicitly, these bounds are:

$$\prod_{\text{q prime}} \left(1-\frac{1}{q^{3/2}-1}\right) \leq |\mathfrak{S}(n)| \leq \prod_{\text{q prime}} \left(1+\frac{1}{q^{3/2}-1}\right)$$

Completing the desired proof.

2.3 Proposition 4.6

From here, we see that, intuitively, the larger the N, the smaller the error in approximating the infinite series by a finite one. We now look separately at bounding the singular integral that was actually used to relate r_d and $A_q(n)$, with the following proposition:
The singular integral $\forall s > 1$:

$$e^{\pi} \int_{-\infty}^{\infty} (1-2ix)^{-s} e^{-2\pi i x} dx = \frac{\pi^s}{\Gamma(s)}$$

Further, $\forall S \geq 1$ and $s \geq 1$:

$$\int_{|x|\geq S} (1-2ix)^{-s} e^{-2\pi i x} = O(S^{1-s})$$

Proof: This follows from section 4.4.4. Specifically, it follows as a standard evaluation of residues on a contour integral. Since this is a fairly standard residue calculation I will prove the tail bound portion but will just discuss the result of the residue calculation. Namely, for the tail, we consider all x sufficiently large, that is $|x| > S$ for:

$$\int_{|x|\geq S} |(1-ix)^{-s} e^{-\pi i x}| dx = \int_{|x|\geq S} |(1-ix)^{-s}| dx = \int_{|x|\geq S} |\sqrt{1+x^2}|^{-s} dx \leq \int_{|x|\geq S} x^{-s} = O(S^{1-s})$$

With these two results in hand, we can trek forward and nearly arrive at the piece de resistance.

2.4 Putting it Together

From this result, we're able to replace the integral that was in the original 4.9 expression. However, the original integral was a finite calculation, namely over the interval: $N^2 I'(p/q)$ of the form:

$$\int_{N^2 I'(p/q)} (1-2ix)^{-d/2} e^{-2\pi i x} dx$$

Thus, in approximating this integral as an infinite integral (as we are from the result of Proposition 4.6), we incur an error term, particularly from the complement of $N^2 I'(p/q)$. From Proposition 4.6, however, we have a bound for this tail estimate. To apply this bound, we just need to show that the $x \in$ the complement of $N^2 I'(p/q)$ are ≥ 1, which we achieve simply by taking $N \leq \sqrt{n}$.
With that, we now proceed through the last stages of bounding. Namely, by definition and now applying the previous calculation we did, with $s = d/2$ and $S = n/Nq$ (for the singular integral):

$$\begin{aligned} r_d(n) &= N^{d-2} e^{\pi n/N^2} \sum_{1 \leq q \leq N} A_q(n) \int_{N^2 I'(p/q)} (1-2ix)^{-d/2} e^{-2\pi i x} dx + O(N^{d/2}) \\ &= n^{d/2-1} \sum_{1 \leq q \leq N} A_q(n) \frac{\pi^{d/2}}{\Gamma(d/2)} + Er \end{aligned}$$

Where Er is our error term. This is where we apply the final bounding result that we demonstrated for the singular series. Specifically (although it's quite ugly):

$$Er = O(n^{d/2-1} \sum_{1 \leq q \leq N} |A_q(n)| \left(\frac{n}{qN}\right)^{1-d/2}) + O(n^{d/4})$$

Since we demonstrated previously

$$|A_q(n)| \leq c_d q^{1-d/2}$$

, this is bounded by:

$$Er \leq O(n^{d/2-1} \sum_{1 \leq q \leq N} c_d q^{1-d/2} \left(\frac{n}{qN}\right)^{1-d/2}) + O(n^{d/4})$$

$$O(n^{d/2-1} \sum_{1 \leq q \leq N} \left(\frac{n}{N}\right)^{1-d/2}) + O(n^{d/4}) = O(\sum_{1 \leq q \leq N} (1/N)^{1-d/2}) + O(n^{d/4}) = O(N^{d/2}) + O(n^{d/4})$$

Since $N \leq \sqrt{n}$, we have $O(N^{d/2})$ is $O(n^{d/4}$, meaning the overall error term too is $O(n^{d/4}$, as desired. The final piece is changing the finite sum in the above definition of $r_d(n)$ to an infinite sum. Namely, if we apply the bound we demonstrated for the tail of the infinite sum of $|A_q(n)|$ to a radius of N, we incur an error term of $O(n^{d/2-1} N^{2-d/2})$, which is once again $O(n^{d/4}$ when considering the restriction of $N \geq \sqrt{n}$. Thus, putting it all together, we have:

$$\begin{aligned} r_d(n) &= n^{d/2-1} \sum_{q=1}^{\infty} A_q(n) \frac{\pi^{d/2}}{\Gamma(d/2)} + O(n^{d/4}) \\ &= \mathfrak{S} \frac{\pi^{d/2}}{\Gamma(d/2)} n^{d/2-1} + O(n^{d/4}) \end{aligned}$$

2.5 Conclusion

To see the final result, simply observe that (as has mentioned in the proof several times), this value has a defined, finite value for any $d \geq 5$, meaning the number of ways a number n can be written as a sum of d squares is well defined. More formally, the full result is:
$\forall d \geq 5$, $\exists N$ such that $\forall n \geq N$, $\exists$ at least one representation of n as a sum of d squares.

3 Two-Squares Lemma Proof

3.1 Introduction

In this section, we explore a largely unrelated topic, that now studies a key lemma used in the proofs of the two-square and four-square theorems. While there are many ways of presenting this proof, the one we consider here involves complex analysis and algebra. Throughout this section, we denote the group of fractional linear transforms by G, which covers all matrices of the form:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Specifically, we only consider those with integer entries, determinant 1, and such that a and d have the same parity, b and c have the same parity, and c and d have opposite parity. We specifically focus on this group, as it acts on upper half-plane by fractional linear transformations. To the group G corresponds the fundamental domain F defined by $|\tau| \geq 1$, $|Re(\tau)| \leq 1$, and $|Im(\tau)| \geq 0$. The overall lemma we wish to prove, therefore, is:

Theorem 1. *Let G denote this group of matrices of fractional linear transformations. A function in $\mathbb{H}$ which is holomorphic, bounded, and invariant under G must be constant.*

The proof requires three main lemmas/results, from which we finally reach our conclusion, which we now turn to.

3.2 Vanishing Function: Upper Half-Plane

We wish to demonstrate the following lemma:

Lemma 1. *Suppose that $f : \mathbb{H} \to \mathbb{C}$ is holomorphic, bounded, and that there exists a sequence of complex numbers $\tau_k = x_k + iy_k$ such that:*

$$f(\tau_k) = 0, \sum_{k=1}^{\infty} y_k = \infty, 0 < y_k \leq 1, |x_k| \leq 1$$

Then $f \equiv 0$.

Proof. We further break this proof into three separate further lemmas, which involves mapping the function to the unit disk ($\mathbb{D}$) and then proving the same result on the transformed function using Jensen's Formula. □

3.2.1 Conformal Map to Unit Disk

To complete this proof, it is much easier to deal with our function f as a transformed function g that maps from $\mathbb{D} \to \mathbb{C}$. Specifically, consider the standard conformal mapping from $\mathbb{D} \to \mathbb{H}$ of:

$$G(w) = i\left(\frac{1-w}{1+w}\right)$$

And further denote $g(z) = F \circ G(z)$. We now demonstrate that the assumption we made regarding f, implies that g satisfies the following properties:

1. g is holomorphic $\in \mathbb{D}$
2. g is bounded
3. g is not identically zero
4. If $z_1, z_2, ..., z_n, ...$, then $\sum_{n=1}^{\infty}(1 - |z_n|) = \infty$

The reason these properties are of importance is for the proof we rely on (in the following subsection). The first three follow quite straightforwardly. Namely, the first is because g is defined as a composition of holomorphic functions. Further, g is bounded as f is bounded (i.e. $|g(w)| = |F(G(w))| \leq M$, for the bound M of f, since $G(w) \in \mathbb{H}$). Similarly, it is not identically zero as we assume $f \not\equiv 0$ (similar argument to bounding).

The final property is similarly straightforward, although not as much as the previous three. Namely, the zeros of g are those w_k for which $G(w_k) = \tau_k$ for some τ_k (a zero of f). Explicitly, we can find these w_k by considering the reverse conformal mapping, namely that which maps $H(z) : \mathbb{D} \to \mathbb{H}$, given by:

$$H(z) = \frac{i - z}{i + z}$$

All that is of importance, however, is the geometric interpretations of both this and the two sums being considered. Namely, this transformation is essentially mapping each point in the upper half plane to the ratio of its distances to the points $-i$ and i respectively. Clearly, as all points $\in \mathbb{H}$ are closer to i than $-i$, this fraction always has magnitude < 1, as desired. As for the two sums, $\sum_{n=1}^{\infty}(1 - |z_n|)$ corresponds to the sum of the distances of the points to the boundary of the unit disk whereas $\sum_{k=1}^{\infty} y_k$ is the sum of the distances of points to the boundary of the upper half plane, i.e. the real axis.

Since we assume the latter diverges, we are assuming that the distances of the y axis to the real axis is consistently large over the sum, i.e. it is sufficiently far away from the real axis to "contribute" to causing the sum to diverge. This implies the point too is closer to i than $-i$ (as we only consider those points in the rectangular region of $Re(z) \in [-1, 1]$ and $Im(z) \in (0, 1]$. As a result, sufficiently many of the points in the former sum are far from the unit disk boundary, causing this sum to similarly diverge, as desired.

3.2.2 Vanishing Function: Unit Disk (Special Case)

Lemma 2. *Prove that if f is holomorphic $\in \mathbb{D}$, bounded and not identically zero, and $z_1, z_2, ..., z_n, ...$ are its zeros ($|z_k| < 1$), then*

$$\sum_{n=1}^{\infty}(1 - |z_n|) < \infty$$

Consider for some $R < 1$ the disk $\overline{D_R(0)}$. Since this region is closed (by definition of the closure) and also bounded ($|z| \leq R$), this forms a compact region. Thus, any infinite sequence of $\{z_k\}_{k=1}^{\infty}$ must have a convergent subsequence. As a result, if it were the case that there were infinitely many zeros $\in \overline{D_R(0)}$, there would be a limit point of f in this closed region, which would imply that $f \equiv 0$, contradicting our assumption. Thus, we must have that there are only finitely many zeros $\in \overline{D_R(0)}$. In turn, we may number these zeros in an arbitrary order, with denotation $z_1, z_2, ..., z_{n_R}$, where n_R clearly corresponds to the number of zeros that occurs in the region $\overline{D_R(0)}$. Since this region clearly converges to $\mathbb{D}$ in the limit of $R \to 1$, $n_R \to \infty$ as $R \to 1$.

Thus, the main takeaway from the above was that the number of zeros is finite in the interior of a closed subset of $\mathbb{D}$, thus allowing us to apply Jensen's Formula. For simplicity, we assume that $f(0) \neq 0$. If it were the case that $f(0) = 0$, that would imply we could factor f as $z^n g(z)$, where $g(0) \neq 0$ and similarly proceed through the proof, now considering g. Further, we denote the bound for f as M, namely that $|f(z)| \leq M \forall z \in \mathbb{D}$ (as we assumed f is bounded). Specifically, in this closed subset, we can consider:

$$\sum_{k=1}^{N} \log(\frac{R}{|z_k|}) = \qquad \frac{1}{2\pi}\int_0^{2\pi} \log|f(Re^{i\theta})|d\theta - \log|f(0)| \tag{6}$$

Since log is monotonically increasing, it is bounded above by the log of the maximum argument. Namely:

$$\frac{1}{2\pi}\int_0^{2\pi}\log|f(Re^{i\theta})|d\theta - \log|f(0)| \leq \qquad \frac{1}{2\pi}\int_0^{2\pi}\log|M|d\theta - \log|f(0)| \tag{7}$$

$$= \qquad \log|M|\frac{1}{2\pi}\int_0^{2\pi}d\theta - \log|f(0)| = \qquad \log\left|\frac{M}{|f(0)|}\right| \tag{8}$$

We now apply the bound that $1 - x \leq -\log(x)$ for $x \in (0,1)$. Specifically, since $|z_k| < R$, we have that $\frac{|z_k|}{R} \in (0,1)$, which we use to conclude:

$$\sum_{n=1}^{n_R}\left(1 - \frac{|z_k|}{R}\right) \leq \qquad \sum_{n=1}^{n_R} -\log\left(\frac{|z_k|}{R}\right) = \qquad \sum_{n=1}^{n_R}\log\left(\frac{R}{|z_k|}\right) \leq \qquad \left|\frac{M}{|f(0)|}\right| < \infty \tag{9}$$

3.2.3 Vanishing Function: Generalization

To apply the above result to our desired lemma, assume for sake of contradiction, that the function $f : \mathbb{H} \to \mathbb{C} \not\equiv 0$. This would imply that g (as defined previously) is also not identically zero and thus (for its zeros $\{z_k\}_{k=1}^{\infty}$) $\sum_{n=1}^{\infty}(1 - |z_n|) < \infty$. However, we proved that our assumptions on f implies that g has $\sum_{n=1}^{\infty}(1 - |z_n|) = \infty$, arriving at a contradiction. Thus, $f \equiv 0$, as desired.

3.3 Fractional Linear Transformations

We now revisit the group G of fractional linear transforms that were initially discussed in the statement of the lemma. Namely, matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

with integer entries, determinant 1, and same parity along diagonals but with each diagonal having a different parity. The group creates a correspondence to transforms by defining (for each $g \in G$) the transformation:

$$g(\tau) = \frac{a\tau + b}{c\tau + d}$$

This group is of particular importance as every fractional linear transformation corresponding to $g \in G$ is a composition of finitely many S, T_2 and their inverses, where S and T_2 are the following transforms:

$$S(\tau) = -1/\tau \leftrightarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$T_2(\tau) = \tau + 2 \leftrightarrow \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

3.3.1 Existence for Arbitrary Pair

Lemma 3. *Given two relatively prime integers c and d with different parity, show that there exist integers a and b such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.*

Proof. Since we assume that $(c,d) = 1$, it follows that these two integers span the ring of integers over linear combinations. That is, we can find constants c_1, c_2 such that $c_1 c + c_2 d = n$ for any choice of n. Thus, we can find constants a_0, b_0 such that:

$$det(g) = a_0 d - b_0 c = 1 \tag{10}$$

If WLOG we assume c to be even and d odd, we would wish for a to be odd and b even. This choice of a_0, b_0 may, however, not abide by the desired properties of parity. However, since infinitely many pairs of a_0, b_0 exist that satisfy the above linear combination, we can find a pair for which a_0 has the desired parity (i.e. odd). However, b_0 may be odd too in this pair found. To arrive at our final version, we observe that $\forall t \in \mathbb{Z}$, the values $a = a_0 - ct$ and $b = b_0 - dt$ also satisfy the equation, as:

$$(a_0 - ct)d - (b_0 - dt)c = a_0 d - dct - b_0 c + dct = a_0 d - b_0 c = 1 \tag{11}$$

Since c is even, adding/subtracting ct to a_0 will not affect its parity. However, adding/subtracting dt to b_0 (for any odd t) will switch its parity, as desired. Thus, setting $t = 1$ will complete the proof, finding out desired integers a, b.

□

3.3.2 Unbounded Sum

We finally prove the result of a sum that will be critical in the final conclusive step of the proof:

Lemma 4. $\sum \frac{1}{c^2+d^2} = \infty$, *where the sum is taken over all c and d that are relatively prime and of opposite parity.*

We proceed through contradiction. Namely assume instead that this sum were bounded, namely that:

$$\sum_{\substack{(c,d)=1 \\ c,d \text{ opp par}}} \frac{1}{c^2 + d^2} < \infty$$

We demonstrate that this would imply that the sum over *all* (i.e. not just those with opposite parity and relatively prime) pairs of integers is bounded, which is a contradiction. In particular, we first demonstrate that the above assumption implies the sum over all relatively prime numbers (not just those of opposite parity) is bounded. Clearly:

$$\sum_{(c,d)=1} \frac{1}{c^2 + d^2} = \sum_{\substack{(a,b)=1 \\ a,b \text{ opp par}}} \frac{1}{a^2 + b^2} + \sum_{\substack{(a,b)=1 \\ a,b \text{both even}}} \frac{1}{a^2 + b^2} + \sum_{\substack{(a,b)=1 \\ a,b \text{both odd}}} \frac{1}{a^2 + b^2}$$

Since we took the first term on the RHS to be bounded by assumption, it suffices to demonstrate the latter two terms are similarly bounded. Clearly, the cases of both being odd and even are parallel, meaning it suffices to demonstrate one of the two cases. In particular, we demonstrate the case where both a, b are odd. In this case, we have for some n, m $a = 2n + 1$ and $b = 2m + 1$, meaning (assuming $a > b$):

$$c = \frac{a+b}{2}, d = \frac{a-b}{2}$$

Are relatively prime and opposite parity. To see that these are relatively prime, simply observe that, if they were *not* relatively prime, there must be some $x \in \mathbb{Z}$ that evenly divides both c, d, meaning there exists some x for which $\frac{a+b}{2x}, \frac{a-b}{2x}$ are both integers. This is only possible if, for such an x, $a + b \equiv a - b(\mod x)$. This could only be the case if b and $-b$ were symmetric about $\mod x$, which could only occur when $b = x/2$, implying that x is even. This, however, implies that a, b must have the same parity, which is opposite the assumption. Thus, c, d are relatively prime.
To see that these are of opposite parity, simply observe:

$$a + b = (2n + 1) + (2m + 1) = 2(n + m + 1) \implies c = n + m + 1$$
$$a - b = (2n + 1) - (2m + 1) = 2(n - m) \implies d = n - m$$

Since adding an even number does not change the parity of a number, d has the same parity as $d+2m = n+m$, clearly demonstrating that c, d have opposite parities ($n+m$ vs. $n+m+1$). As a result, we have that:

$$c^2 + d^2 = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 = 1/4(a^2 + 2ab + b^2 + a^2 - 2ab + b^2) = 1/2(a^2 + b^2) \leq a^2 + b^2 \tag{12}$$

$$\implies \sum_{\substack{(a,b)=1 \\ a,b \text{both odd}}} \frac{1}{a^2+b^2} \leq \sum_{\substack{(c,d)=1 \\ c,d \text{ opp par}}} \frac{1}{c^2+d^2} < \infty$$

This demonstrate that each of the sum over all relatively prime integers is bounded (as the above process can be repeated for relatively prime even pairs). Further, it also shows that $\forall n \in \mathbb{Z}$, $c^2 + d^2 \leq n^2(a^2 + b^2)$, implying that:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} \sum_{(a,b)=1} \frac{1}{a^2+b^2} = \sum_{n=1}^{\infty} \sum_{(a,b)=1} \frac{1}{(na)^2+(nb)^2} \leq \sum_{\substack{(c,d)=1 \\ c,d \text{ opp par}}} \frac{1}{c^2+d^2} < \infty$$

Since $(a, b) = 1$, when multiplied over all integers n, we span over all integers (by a similar argument as how relatively prime integers span the ring of integers used in the singular integrals proof). Thus, this implies:

$$\sum_{\ell,k\neq 0} \frac{1}{\ell^2+k^2} < \infty$$

Reaching a contradiction, as this last sum is known to diverge.

3.3.3 Conclusion

Finally, we wish to show the original result. Namely, consider any function $F(\tau)$ that satisfies the original properties of the lemma. We now linearly shift the function and define $f(\tau) = F(\tau) - F(i)$, which clearly vanishes at $\tau = i$ by definition. We now consider any pair of relatively prime integers c, d with different parity. By Lemma 3, we have a corresponding $\exists g_{c,d} \in G$. By definition:

$$g_{c,d}(i) = \frac{b+ai}{d+ci} \cdot \frac{d-ci}{d-ci} = \frac{bd - bci + adi + ac}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\frac{ad-bc}{c^2+d^2}$$

Since the determinant of these matrices is 1 by assumption, the imaginary part is simply $1/(c^2+d^2)$. Similarly, we can simply shift the real part over such that it has a magnitude ≤ 1. Thus, if we denote the real part as $x_{c,d}$ and imaginary as $y_{c,d}$, we clearly have that $|x_{c,d}| \leq 1$ and $|y_{c,d}| \in (0, 1]$. Further, by Lemma 4, we have the $\sum_{\substack{(c,d)=1 \\ c,d \text{ opp par}}} y_{c,d} = \infty$. Finally, since F was assumed to be invariant under transformations in G, so too must f be invariant, meaning that $f(g_{c,d}(i)) = f(i)$, meaning that f vanishes at all these $g_{c,d}(i)$. As it too is holomorphic and bounded, this implies that $f \equiv 0$ by Lemma 1, which further implies that $F(\tau) \equiv F(i)$, a constant, completing the proof.