18.786 Number Theory II **Spring 2024**
Problem Set #4 **Due: 3/23/2024**

Description

These problems are related to the material covered in Lectures 9-12. Your solutions should be written up in latex and submitted as a pdf-file on Gradescope before midnight on the date due. Collaboration is permitted/encouraged, but you must identify your collaborators or the name of your group on pset partners, and any references you consulted. If there are none write "**Sources consulted: none**" at the top of your solution.

Instructions: Pick any combination of problems that sum to 100 points, then complete the survey problem.

Problem 1. Modular forms on $\mathrm{SL}_2(\mathbb{Z})$ (50 points)

Throughout this problem $\Gamma := \mathrm{SL}_2(\mathbb{Z})$ denotes the full modular group. Let Γ_∞ be the stabilizer of ∞, and let

$$\mathcal{F} := \{z \in \mathbf{H} : |z| \ge 1 \text{ and } |\operatorname{Re}(z)| \le 1/2\}$$

denote the standard fundamental domain for Γ. For even integers $k \ge 4$ we define the Eisenstein series $G_k(z)$ as the Poincaré series (see (2.6.2) in [2]):

$$G_k(z) := F_k(z; \phi_0, \chi_0, \Gamma_\infty, \Gamma) := \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \overline{\chi_0(\gamma)} (\phi_0|_k \gamma)(z),$$

where $\phi_0 = 1$ is the identity function and χ_0 is the trivial character. We also define[1]

$$E_k(z) := -\frac{B_k}{2k} G_k(x),$$

where $B_k := \frac{(-1)^{k/2+1} 2 \cdot k!}{(2\pi)^k} \zeta(k) = 2k(-1)^{k/2+1} \int_0^\infty \frac{t^{k-1}}{e^{2\pi t}-1} dt \in \mathbb{Q}$ is the kth Bernoulli number, with $B_2 = \frac{1}{2}$, $B_4 = -\frac{1}{30}$, $B_6 = \frac{1}{42}$ (see Problem 3 for more on Bernoulli numbers).

(a) Let $k \ge 4$ be even. Prove that $E_k(z)$ has the following q-expansion at ∞:

$$E_k(z) = \frac{-B_k}{2k} + q + \sum_{n=2}^{\infty} \sigma_{k-1}(n) q^n,$$

where $q := e^{2\pi i z}$ and $\sigma_e(n) := \sum_{d|n} d^e$.

(b) Let $\rho = e^{\pi i/3}$. Prove that for any $k \in \mathbb{Z}$ and nonzero $f \in M_k(\Gamma)$ we have

$$\operatorname{ord}_\infty(f) + \frac{1}{2} \operatorname{ord}_i(f) + \frac{1}{3} \operatorname{ord}_\rho(f) + \sum_{\tau \in \mathcal{F} - \{i, \rho\}} \operatorname{ord}_\tau(f) = \frac{k}{12}.$$

Conclude that $\dim M_k = 0$ unless $k \ge 4$ is even.

[1] Note that this is **not** the E_k defined in [2, §4.1].

(c) Let $\Delta := (G_4^3 - G_6^2)/1728$. Prove that for even $k \geq 4$ the map $f \mapsto \Delta f$ defines an isomorphism $M_{k-12} \xrightarrow{\sim} S_k$. Conclude that $\dim M_k = 1$ and $\dim S_k = 0$ for $k = 4, 6, 8, 10, 14$.

(d) Prove that if $4a + 6b = k \equiv 0 \bmod 12$ then $3|a$ and $G_4^a G_6^b / G_6^{k/6} = (G_4^3/G_6^2)^{a/3}$.

(e) Prove that for all even integers $k \geq 2$ we have

$$\dim M_k(\Gamma) = \begin{cases} 0 & \text{if } k \text{ is odd or negative,} \\ \lfloor k/12 \rfloor & \text{if } k \equiv 2 \bmod 12 \text{ is positive and even.} \\ \lfloor k/12 \rfloor + 1 & \text{if } k \not\equiv 2 \bmod 12 \text{ is positive and even.} \end{cases}$$

(this is Corollary 4.1.4 in [2], you are being asked to give an alternative proof).

(f) Prove that $\{G_4^a G_6^b : a, b \in \mathbb{Z}_{\geq 0} \text{ with } 4a + 6b = k\}$ is a basis for $M_k(\Gamma)$ for all $k \in \mathbb{Z}$. (this is Theorem 4.1.8 in [2], you are being asked to give an alternative proof).

(g) Prove that the space $S_k(\Gamma)$ has a unique basis $\{f_1, \ldots, f_d\}$ such that $a_i(f_j) = \delta_{ij}$ for $1 \leq i, j \leq d$, where f_j has q-expansion $f_j = \sum_{i \geq 0} a_i(f_j) q^i$ at ∞, and show that $f_j \in \mathbb{Z}[[q]]$ (hint: use the E_k and Δ). This basis for $S_k(\Gamma)$ is called the Miller basis.

(h) Let $\{f_1, f_2\}$ be the Miller basis for $S_{38}(\Gamma)$. Compute the integers $a_3(f_i)$ for $1 \leq i \leq 2$ and express each f_i in terms of the basis for $M_{38}(\Gamma)$ given by part **(f)**.

(i) Let $\mathbb{T} := \mathbb{Z}[\Gamma \backslash \Delta / \Gamma]$ be the Hecke algebra for $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ over $\mathbb{Z}$, with Δ the set of integer matrices in $\mathrm{GL}_2^+(\mathbb{Q})$. For $n \in \mathbb{Z}_{\geq 1}$ let $T(n) \in \mathbb{T}$ denote the nth Hecke operator $T(n) := \sum_{\det \alpha = n} \Gamma \alpha \Gamma$, where the sum is over double cosets of Γ in Δ. Show that for every even integer $k \geq 4$ and integer $n \geq 1$ we have

$$T(n)(E_k) := E_k | T(n) = \sigma_{k-1}(n) E_k,$$

and compute the matrix of $T(2)$ on the Miller basis for $S_{38}(\Gamma)$.

Problem 2. Hecke operators on $\Gamma_1(N)$ (50 points)

Fix $N \in \mathbb{Z}_{>0}$. In lecture, we considered the Hecke algebra

$$\mathbb{T}(\Gamma_0(N), \Delta_0(N)) := \mathbb{Z}[\Gamma_0(N) \backslash \Delta_0(N) / \Gamma_0(N)],$$

where

$$\Gamma_0(N) := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N, a \perp N \},$$
$$\Delta_0(N) := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2^+(\mathbb{Z}) : c \equiv 0 \bmod N, a \perp N \},$$

see [2, 4.5]. We now want to consider the Hecke algebra $\mathbb{T}(\Gamma_1(N), \Delta_1(N))$, where

$$\Gamma_1(N) := \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N, a \equiv d \equiv 1 \bmod N \},$$
$$\Delta_1(N) := \{ \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2^+(\mathbb{Z}) : c \equiv 0 \bmod N, a \equiv 1 \bmod N \}.$$

We also define the diamond operator $\langle d \rangle$ for each $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, which acts on modular forms of weight k via $f \mapsto f|_k \sigma_d$, where $\sigma_d \in \mathrm{SL}_2(\mathbb{Z})$ satisfies

$$\sigma_d \equiv \begin{pmatrix} 1/d & 0 \\ 0 & d \end{pmatrix} \bmod N.$$

Throughout this problem χ denotes a Dirichlet character of modulus N, and for any integer m we write $m|N^\infty$ to indicate that every prime divisor of m is also a prime divisor of N.

(a) Show that

$$M_k(\Gamma_0(N),\chi) = \{f \in M_k(\Gamma_1(N)) : \langle d\rangle f = \chi(d)f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times\},$$

so $\langle d\rangle$ acts on $M_k(\Gamma_0(N),\chi)$ via $f \mapsto \chi(d)f$. Conclude that $\langle d\rangle$ acts on $M_k(\Gamma_1(N))$ and this action does not depend on the choice of σ_d.

We now define Hecke operators $T(n), T(a,d) \in \mathbb{T}(\Gamma_1(N),\Delta_1(N))$, with $a|d \perp N$, via

$$T(n) := \sum_{\det\alpha = n} \Gamma_1(N)\alpha\Gamma_1(N), \qquad T(a,d) := \Gamma_1(N)\sigma_a\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)\Gamma_1(N),$$

where the sum for $T(n)$ is over double cosets of $\Gamma_1(N)$ in $\Delta_1(N)$.

(b) Show that $\mathbb{T}(\Gamma_1(N),\Delta_1(N))$ is commutative and for any $\alpha \in \Delta_1(N)$ we can choose $\alpha_1,\ldots,\alpha_n \in \Delta_1(N)$ so that $\Gamma_1(N)\alpha\Gamma_1(N) = \sqcup_i\Gamma_1(N)\alpha_i = \sqcup_i\alpha_i\Gamma_1(N)$.

(c) Prove that every Hecke operator $\Gamma_1(N)\alpha\Gamma_1(N)$ with $\alpha \in \Delta_1(N)$ can be uniquely expressed in the form

$$T(m)T(a,d) = T(a,d)T(m),$$

with $m|N^\infty$ and $a|d \perp N$.

(d) Show that $\mathbb{T}(\Gamma_1(N),\Delta_1(N)) = \langle T(p), T(q,q) : p, q \text{ prime}, q \perp N\rangle$ and that we also have $\mathbb{T}_\mathbb{Q}(\Gamma_1(N),\Delta_1(N)) = \langle T(n)\rangle$.

(e) For each $n \in \mathbb{Z}_{>0}$ let $\Delta^n := \{\alpha \in \Delta_1(N) : \det\alpha = n\}$ so that $\Delta_1(N) = \sqcup_{n\geq 0}\Delta^n$. For each positive integer $a \perp N$ fix a choice of $\sigma_a \in \mathrm{SL}_2(\mathbb{Z})$. Show that for each $n \in \mathbb{Z}_{>0}$ we have

$$\Delta^n = \bigsqcup_{\substack{ad=n \\ a\perp N}} \bigsqcup_{0\leq b<d} \Gamma_1(N)\sigma_a\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right).$$

Conclude that for each $f \in M_k(\Gamma_0(N),\chi)$ we have

$$f|_kT(n) = n^{k-1}\sum_{\substack{ad=n \\ a\perp N}}\sum_{0\leq b<d}\chi(a)d^{-k}f\left(\tfrac{az+b}{d}\right),$$

and

$$f|_kT(d,d) = d^{k-2}\chi(d)f.$$

(f) Show that when we restrict the action of $\mathbb{T}(\Gamma_1(N),\Delta_1(N))$ to $M_k(\Gamma_0(N),\chi)$ we have

$$T(m)T(n) = \sum_{d|\gcd(m,n)} d^{k-1}\chi(d)T(mn/d^2),$$

and derive the identity

$$\sum_{n\geq 1} T(n)n^{-s} = \prod_p \left(1 - T(p)p^{-s} + \chi(p)p^{k-1-2s}\right)^{-1}$$

where both of the equalities above are identities of operators on $M_k(\Gamma_0(N),\chi)$.

(g) Prove the following identity of operators on $M_k(\Gamma_1(N))$:

$$p^{k-1}\langle p\rangle = T(p)^2 - T(p^2),$$

valid for all primes p.

Problem 3. Computing Bernoulli numbers (50 points)

For integers $n \geq 0$, the Bernoulli polynomials $B_n(x) \in \mathbb{Q}[x]$ are defined as the coefficients of the exponential generating function

$$E(t,x) := \frac{te^{tx}}{e^t - 1} = \sum_{n\geq 0} \frac{B_n(x)}{n!} t^n.$$

The nth Bernoulli number is then defined as $B_n = B_n(0)$.

(a) Prove that $B_0(x) = 1$, $B_n'(x) = nB_{n-1}(x)$, and $B_n(1) = B_n(0)$ for $n \neq 1$, and that these properties uniquely determine the Bernoulli polynomials.

(b) Prove that $B_n(x+1) - B_n(x) = nx^{n-1}$ and

$$B_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} B_k(x) y^{n-k}.$$

Use this to show that B_n can alternatively be defined by the recurrence $B_0 = 1$ and

$$B_n = -\frac{1}{n+1} \sum_{k=0}^{n-1} \binom{n+1}{k} B_k$$

for all $n > 0$, and show that $B_n = 0$ for all odd $n > 1$.

(optional) This part is not required but you can use the result in your solution to **(c)**. Let $n \geq 2$ be an even integer. Generalize **(b)** to show that for all $y \in \mathbb{Z}_{\geq 1}$ we have

$$\sum_{m=0}^{y-1} (m+x)^{n-1} = \frac{B_n(x+y) - B_n(x)}{n},$$

and use this to deduce a formula for sums of nth powers using Bernoulli numbers

$$\sum_{m=1}^{y-1} m^n = \frac{1}{n+1} \sum_{k=0}^{n} \binom{n+1}{k} B_k y^{n+1-k}.$$

Now derive a formula for B_n in terms of nth powers

$$B_n = \sum_{k=0}^{n} \frac{1}{k+1} \sum_{m=0}^{k} (-1)^m \binom{k}{m} m^n,$$

and also in terms of the Stirling numbers $\left\{ {n \atop k} \right\} := \frac{1}{k!} \sum_{m=0}^{k} (-1)^{k-m} \binom{k}{m} m^n$ that count the number of ways to partition a set of n labelled objects into k nonempty subsets:

$$B_n = \sum_{k=0}^{n} \frac{k!}{k+1} (-1)^k S(n,k).$$

(c) Let $n \geq 2$ be an even integer. Prove that $v_p(B_n) \geq -1$ for all primes p and that $v_p(B_n) = -1$ if and only if $p-1$ divides n. In other words, when written in lowest terms the denominator of the rational number B_n is $\prod_{(p-1)|n} p$.

For a nonzero rational number $r = a/b$ with $a, b \in \mathbb{Z}$ coprime we define its height to be $h(r) := \max(\log|a|, \log|b|) \in \mathbb{R}_{\geq 0}$.

(d) Let $n \geq 2$ be an even integer. Using the identity $\zeta(n) = (-1)^{n/2+1}\frac{(2\pi)^n B_n}{2 \cdot n!}$ and the bounds

$$\sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n} e^{\frac{1}{12n+1}} < n! < \sqrt{2\pi} n^{n+\frac{1}{2}} e^{-n} e^{\frac{1}{12n}}$$

arising from Stirling's approximation, determine an effective upper bound for $h(B_n)$ as a function of n (you are not required to prove the identity but are free to do so!).

(e) Let $\mathsf{M}(b)$ denote the time to multiply two b-bit integers (the bound $M(b) = O(b \log b)$ was recently proved [1], but in practice the Schönhage-Strassen algorithm [3] with complexity $O(b \log b \log\log b)$ is used). Estimate the complexity of computing B_n using the recursive formula above, assuming that it takes $\mathsf{M}(b) \log b$ time to reduce a ratio of b-bit integers to a rational number in lowest terms (this is achieved by the fast Euclidean algorithm). Your answer should be an asymptotic upper bound (in big O-notation) on the number of bit operations required, as a function of n.

(f) Describe an algorithm to compute B_n using Newton iteration to compute $1/f$ modulo x^{n+1}, where $f(x) = (e^x - 1)/x = \sum_{n \geq 0} \frac{x^n}{(n+1)!}$, and estimate its complexity. Note that you can use Kronecker substitution to multiply two polynomials in $\mathbb{Z}[x]$ of degree at most d with coefficients of height b in time $O(\mathsf{M}(bd \log d))$ by replacing x with a suitable power of 2.

(g) Let $n \geq 2$ be an even integer, let $d = \prod_{(p-1)|n} p$ be the denominator of B_n and let A be an approximation to $2 \cdot n!/(2\pi)^n$ to b-bits of precision, such that $2^b > e^{h(B_n)}$. Let $P := \lceil (Ad)^{1/(n-1)} \rceil$ and let $r := \prod_{p \leq P}(1-p^{-n})^{-1}$. Show that if $a = (-1)^{n/2+1}\lceil drA \rceil$ then $B_n = a/d$.

(h) Estimate the complexity of computing B_n using the algorithm suggested by **(e)**.

(i) Illustrate the 3 algorithms to compute B_n considered in this problem for $n = 8$.

Problem 4. Survey

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found it (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			

Please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material to you (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
3/11	Poincare and Eisenstein series				
3/13	Hecke algebras				
3/18	Hecke algebras for modular groups				
3/20	Eigenforms and L-functions				

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.

References

[1] D. Harvey and J. van der Hoeven, *Integer multiplication in time $O(n \log n)$*, Annals of Mathematics **193** (2021), 563–617.

[2] T. Miyake, *Modular forms*, Springer, 2006.

[3] A. Schönhage and V. Strassen, *Schnelle multiplikation großer Zahlen*, Computing **7** (1971), 281–292.