Modular Forms: Problem Sheet 4

Sarah Zerbes

22nd March 2022

---

1. If f is a modular form (of any weight), write $a_i(f)$ for the coefficient of q^i in its q-expansion.

   (a) Find constants c_1 and c_2 such that $f = c_1 E_4^3 + c_2 E_6^2$ has $a_1(f) = 1$ and $a_2(f) = \sigma_{11}(2)$. Hence show that the constant γ_{12} such that

$$E_{12} = 1 + \gamma_{12} \sum_{n \geq 1} \sigma_{11}(n) q^n$$

is equal to $\frac{65520}{691}$.

Solution: This exercise is way less painful to solve using a computer. You can find a sage script in the appendix. Instructions on how to access sage and carry out basic operations can be found on this exercise sheet written by Professor David Loeffler and Tim Gehrunger. We recall that

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

Hence we have

$$\begin{aligned} E_4^3 &= 1 + \binom{3}{1} \left(\frac{-8}{B_4}\right) \left[\sigma_3(1) q + \left(\sigma_3(2) - \frac{8}{B_4} \sigma_3(1)^2\right) q^2\right] + \mathcal{O}(q^3) \\ E_6^2 &= 1 - \binom{2}{1} \frac{12}{B_6} \sigma_5(1) q - \left[\binom{2}{1} \frac{12}{B_6} \sigma_5(2) - \left(\frac{12}{B_6} \sigma_5(1)\right)^2\right] q^2 + \mathcal{O}(q^3). \end{aligned}$$

In order to find c_1 and c_2, all we need to do is to solve the linear system $AX = Y$, where

$$A = \begin{pmatrix} a_1(E_4^3) & a_1(E_6^2) \\ a_2(E_4^3) & a_2(E_6^2) \end{pmatrix}, \; X = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}, \text{ and } Y = \begin{pmatrix} 1 \\ \sigma_{11}(2) \end{pmatrix}.$$

We obtain

$$c_1 = \frac{7}{1040}, \; c_2 = \frac{25}{6552}.$$

From the lectures we know that

$$M_{12} = S_{12} \oplus (\mathbb{C} \cdot E_{12})$$

but also that $S_{12} = \mathbb{C} \cdot \Delta$. Hence,

$$f = \lambda_1 \Delta + \lambda_2 E_{12}, \text{ for some } \lambda_1, \lambda_2 \in \mathbb{C}.$$

From looking at the constant coefficient in the q-expansions of both sides of the above equation, we deduce that $\lambda_2 = c_1 + c_2$. Moreover,

$$\begin{aligned} 1 = a_1(f) &= \lambda_1 a_1(\Delta) + (c_1 + c_2) a_1(E_{12}) = \lambda_1 + (c_1 + c_2)\gamma_{12} \\ \sigma_{11}(2) = a_2(f) &= \lambda_1 a_2(\Delta) + (c_1 + c_2) a_2(E_{12}) = -24\lambda_1 + (c_1 + c_2)\gamma_{12}\sigma_{11}(2). \end{aligned}$$

We then solve the linear system $B\tilde{X} = Y$, for

$$B = \begin{pmatrix} 1 & c_1 + c_2 \\ -24 & \sigma_{11}(2)(c_1 + c_2) \end{pmatrix}, \ \tilde{X} = \begin{pmatrix} \lambda_1 \\ \gamma_{12} \end{pmatrix}$$

and obtain that

$$\lambda_1 = 0$$
$$\gamma_{12} = \frac{1}{c_1 + c_2} = \frac{65520}{691}.$$

(b) Deduce that

$$\zeta(12) = \frac{691}{638512875}\,\pi^{12}.$$

Solution: Recall that we proved

$$\zeta(k) = -\frac{(2\pi i)^k B_k}{2 \cdot k!}, \tag{1}$$

for all even integers $k \geq 2$. From the formula for the q-expansion of E_{12}, we deduce that

$$B_{12} = -\frac{24}{\gamma_{12}}.$$

We obtain the result by plugging this into (1).

(c) Find constants d_1, d_2 such that

$$\Delta = d_1 E_{12} + d_2 E_4^3.$$

Hence prove Ramanujan's congruence for the coefficients of Δ modulo 691, namely that

$$\tau(n) = \sigma_{11}(n) \pmod{691}.$$

Solution: Proceeding similarly as for (a), we obtain

$$d_1 = -\frac{691}{432000} = -d_2.$$

By the identity theorem for power series, we then have

$$\tau(n) = -d_1 \left(\frac{24}{B_{12}} \sigma_{11}(n) + a_n(E_4^3) \right)$$
$$\iff 43200\tau(n) = 691 \left(\frac{24}{B_{12}} \sigma_{11}(n) + a_n(E_4^3) \right).$$

This implies

$$125\tau(n) \equiv 125\sigma_{11}(n) \mod 691$$

(recall that we showed that $E_4^n \in M_{4n}(\mathbb{Z})$ for all $n \geq 0$). Finally, since $\gcd(125, 691) = 1$, we can multiply by the inverse of 125 in $\mathbb{Z}/691\mathbb{Z}$ on both sides and obtain the desired result.

2. Let $N \geq 2$ and let $c, d \in \mathbb{Z}/N\mathbb{Z}$. We say that c and d are **coprime modulo** N if there is no $f \neq 0$ in $\mathbb{Z}/N\mathbb{Z}$ such that $fc = fd = 0$.

   (a) Show that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then c and d are coprime modulo N.

Solution: Assume that for some $f \in \mathbb{Z}/N\mathbb{Z}$ we have $fc = fd = 0 \mod N$. Then,

$$f = f \cdot 1 = f \cdot (ad - bc) = afd - bfc = 0 \mod N.$$

(b) Show that for any pair (c, d) that are coprime modulo N, there exist $c', d' \in \mathbb{Z}$ such that $c' = c$ and $d' = d \pmod N$ and $\mathrm{HCF}(c', d') = 1$.

Solution: Let us also write c and d for representatives of the classes c, d mod N chosen in $\{0, \ldots, N-1\}$. First note that (c, d) are coprime mod N implies $\gcd(c, d, N) = 1$. Indeed, if $a = \gcd(c, d, N) > 1$, then $N/a \neq 0$ mod N and $\frac{N}{a}c = 0 = \frac{N}{a}d \mod N$. This implies that if $g = \gcd(c, d)$, then $\gcd(g, N) = 1$.

We are now looking for

$$c' = c + sN,\ d' = d + tN,\ s, t \in \mathbb{Z} \text{ such that } \gcd(c', d') = 1.$$

Assume that $c \neq 0$ and let p be a prime factor of c dividing g. We then know that $p \nmid N$ and we do not want p to divide t since if it doesn't then it won't divide $d + tN$. If now p is a prime factor of c that doesn't divide g, we know that $g \nmid d$. Hence, we want p to divide t since we'll then be sure that $p \nmid d + tN$.

We use the Chinese Remainder Theorem to find some $t \in \mathbb{Z}$ that is congruent to 1 mod every prime factor of c that divides g and congruent to 0 mod every other prime factor of c. Letting $s = 0$ we then have found a pair of integers with the required properties when $c \neq 0$.

Otherwise, if $c = 0$, we must then have $d \neq 0$ (since otherwise they are not coprime and since the case $N = 1$ is vacuous). We then proceed similarly as in the first case, inverting the roles of c and d and those of s and t.

(c) Hence (or otherwise) show that the natural reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective for any $n \geq 2$.

Solution: We are looking for $k, l \in \mathbb{Z}$ such that

$$A_{k,l} := \begin{pmatrix} a + kN & b + lN \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Let $m \in \mathbb{Z}$ such that $ad' - bc' = 1 + mN$. Since $\gcd(c', d') = 1$ there exist some $u, v \in \mathbb{Z}$ such that $uc' + vd' = 1$. Let $k = -vm$, $l = um$. Then

$$\det A_{k,l} = (a - vmN)d' - (b + umN)c' = ad' - bc' - mN(vd' + uc') = 1.$$

(d) Give an example of an integer N and an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which is not the reduction of any element of $\mathrm{GL}_2(\mathbb{Z})$.

Solution: We recall that for a commutative unital ring R, the general linear group of degree 2, denoted $\mathrm{GL}_2(R)$ and defined to be the group of invertible matrices with entries in R, is equal to

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in R \text{ and } (ad - bc)^{-1} \in R \right\},$$

where by $(ad - bc)^{-1}$ we mean the multiplicative inverse of $ad - bc$ in the field of fractions of R.

Let $N = 5$ and consider the matrix

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 3 \end{pmatrix}.$$

We compute $\det(A) = 3 \bmod 5$, so since $\gcd(3,5) = 1$, A is an element of $\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$. Note however that the determinant of any lift $\tilde{A}$ of A with integral entries is of the form

$$\det(\tilde{A}) = 3 + 5 \cdot \alpha, \text{ for some } \alpha \in \mathbb{Z}.$$

But there is then no way that $\det(\tilde{A}) \in \{\pm 1\}$. Hence there is no lift of A in $\mathrm{GL}_2(\mathbb{Z})$.

3. (a) Let D and N be positive integers, and let β be a (2x2) matrix with integral entries and determinant D. Prove that $\Gamma(DN) \subseteq \Gamma(N) \cap \beta^{-1}\Gamma(N)\beta$

Solution: It is not hard to see from the definition that $\Gamma(DN) \subset \Gamma(N)$. We are left to show that $\Gamma(DN) \subset \beta^{-1}\Gamma(N)\beta$ or equivalently that for any $\gamma \in \Gamma(DN)$, $\beta\gamma\beta^{-1} \in \Gamma(N)$. Let

$$\beta = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, \text{ then } \beta^{-1} = \frac{1}{D}\begin{pmatrix} h & -f \\ -g & e \end{pmatrix},$$

and let

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(DN).$$

We compute the coefficients of $\beta\gamma\beta^{-1}$. For example, D times the upper left coefficient equals

$$hea + hfc - geb - gfd = he - gf = D \mod DN.$$

Hence, the upper left coefficient is congruent to 1 mod N.
As another example, D times the lower left coefficient equals

$$hga + h^2c - g^2b - ghd \equiv hg - gh = 0 \mod DN,$$

which implies that is also vanishes mod N. We let the reader compute the two remaining coefficients and deduce that $\beta\gamma\beta^{-1} = \mathrm{id} \bmod N$. Since this holds for any $\gamma \in \Gamma(DN)$, we conclude that $\Gamma(DN) \subset \beta^{-1}\Gamma(N)\beta$.

(b) Let Γ be any congruence subgroup, and let $\alpha \in \{A \in \mathrm{GL}_2(\mathbb{Q}) : \det(A) > 0\}$. Prove that the group $\Gamma' = \Gamma \cap \alpha^{-1}\Gamma\alpha$ is again a congruence subgroup.

Solution: Write

$$\alpha = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q})$$

and let $m \in \mathbb{Z}$ be the lowest common multiple of the denominators of e, f, g and h. We clear the denominators in α by multiplying by m and denote the resulting matrix $\beta \in \mathrm{GL}_2(\mathbb{Z})$. Then, $D := \det(\beta) = m^2 \det(\alpha) \in \mathbb{Z}$.
Now let $N \in \mathbb{Z} \setminus \{0\}$ such that $\Gamma(N) \subset \Gamma$. Then,

$$\Gamma(N) \cap \alpha^{-1}\Gamma(N)\alpha \subset \Gamma \cap \alpha^{-1}\Gamma\alpha.$$

Note additionally that

$$\beta^{-1}\Gamma(N)\beta = (m\alpha)^{-1}\Gamma(N)(m\alpha) = \frac{m}{m}\alpha^{-1}\Gamma(N)\alpha,$$

since $\mathrm{GL}_2(\mathbb{Q})$ is a left and right $\mathbb{Q}$-module. Hence

$$\Gamma(N) \cap \beta^{-1}\Gamma(N)\beta \subset \Gamma \cap \alpha^{-1}\Gamma\alpha.$$

Finally, by part (a), we have that $\Gamma(DN)$ is a subgroup of the left-hand of side the above inclusion. We conclude that $\Gamma \cap \alpha^{-1}\Gamma\alpha$ contains a principal congruence subgroup and is therefore a congruence subgroup.

A Sage code

```
#Exercise 1.a)

a = -24*sigma(1,3)/bernoulli(4)
b = -24*sigma(1,5)/bernoulli(6)
c = -(24/bernoulli(4))*(sigma(2,3)-(8/bernoulli(4))*sigma(1,3)^2)
d = -(24*sigma(2,5)/bernoulli(6))+(12*sigma(1,5)/bernoulli(6))^2

A = Matrix(QQ, [[a,b],[c,d]])
Y = vector([1, sigma(2,11)])

(c1,c2) = A.solve_right(Y)

B = matrix(QQ, [[1, c1+c2], [-24, (c1+c2)*sigma(2,11)]])
Z = vector([1, sigma(2,11)])

(lambda1, gamma12) = B.solve_right(Z)


#Other option

R.<q> = QQ[] #defines the ring of polynomials with variable q

E4 = 1 - (8/bernoulli(4))*(sigma(1,3)*q + sigma(2,3)*q^2)
E43=E4^3
E6 = 1 - (12/bernoulli(6))*(sigma(1,5)*q + sigma(2,5)*q^2)
E62 = E6^2

A = matrix(QQ, [[E43[1], E62[1]], [E43[2], E62[2]]])
Y = vector([1, sigma(2,11)])

(c1,c2) = A.solve_right(Y) #after this proceed as above


#Exercise 1.c)

E12 = 1 - (24/bernoulli(12))*(sigma(1,11)*q
B = matrix(QQ, [[1,1], [E12[1], E43[1]]])
Y = vector([0, 1])
(d1,d2) = B.solve_right(Y)
```