Diamond & Shurman – najciekawsze zadania

Rozdział I

Podrozdział 1.1

1.1.1 Chcemy wykazać, że $\mathrm{Sl}_2(\mathbb{Z}) = \Gamma$, gdzie $\Gamma = \langle A, B\rangle$, zaś $A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Niech $C = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$. Za pomocą algorytmu dzielenia z resztą zapiszmy $d = nc + r$, gdzie $|r| < c/2$. Wtedy:

$$CA^{-n} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} 1 & -n \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} a & b' \\ c & d_1 \end{bmatrix}$$

dla pewnego $b' \in \mathbb{Z}$. Niech $C_1 = CA^{-n}B = \begin{bmatrix} b & -a \\ d & -c \end{bmatrix} =: \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$. Powtarzając ten proces dostaniemy ciąg macierzy $C_n = \begin{bmatrix} a_n & b_n \\ c_n & d_n \end{bmatrix}$, przy czym $|c_{n+1}| = |d_n| < |c_n|/2$. W końcu dostaniemy więc $C_n = \begin{bmatrix} a_n & b_n \\ 0 & d_n \end{bmatrix}$. Ale $C_n \in \mathrm{Sl}_2(\mathbb{Z})$, więc $\pm 1 = \det C_n = a_n d_n$, więc $a_n, d_n = \pm 1$. Przemnażając ewentualnie przez macierz $\begin{bmatrix} 0 & -1 \\ 0 & 1 \end{bmatrix}^2 = -I$, dostajemy macierz $\begin{bmatrix} 1 & b_n \\ 0 & 1 \end{bmatrix} = A^{b_n} \in \Gamma$. Ostatecznie $C \in \Gamma$.

1.1.4 (a)

(b) Niech $C < \min(\frac{B}{2A}, \frac{1}{2}, B)$. Niech $\tau = x + iy \in \Omega$. Wtedy:

1^o dla $|\delta| < 2A$ mamy: $|\tau + \delta| \geqslant |\Im(\tau + \delta)| = |y| \geqslant B \geqslant \frac{B}{2A}|\delta| > C|\delta|$,

2^o dla $|\delta| \geqslant 2A$ mamy: $|\tau + \delta| \geqslant \Re(\tau + \delta) = |x + \delta| \geqslant |\delta| - |x| \geqslant |\delta| - A \geqslant \frac{1}{2}|\delta| > C|\delta|$.

a ponadto $|\tau + \delta| \geqslant |\Im(\tau + \delta)| = |y| \geqslant B > C$ dla dowolnego $\tau \in \Omega$

(a) 1.1.6

Ustalmy $y > 0$ i niech $F(q) = f(\tau + iy) = \sum_n b_n q^n$, wtedy $a_m = b_m e^{-2\pi y}$ Mamy:

$$\begin{aligned} a_m &= e^{-2\pi y}\frac{1}{2\pi i}\int \gamma \frac{F(q)}{q^{m+1}} q = \begin{pmatrix} q & = & e^{2\pi i \tau}, \\ dq & = & 2\pi i q d\tau \end{pmatrix} = \\ &= e^{-2\pi y}\frac{1}{2\pi i}\int_0^1 f(\tau + iy) e^{-2\pi i m(\tau + iy)}\, d\tau = \\ &= \int_{\tau=0+iy}^{1+iy} f(\tau) e^{-2\pi i m \tau} d\tau \end{aligned} \tag{1}$$

co dowodzi pierwszej równości. Z definicji funkcji f:

$$\begin{aligned} \int_{\tau=0+iy}^{1+iy} f(\tau) e^{-2\pi i m\tau}\, d\tau &= \int_{\tau=0+iy}^{1+iy} \left(\sum_{d\in\mathbb{Z}} \frac{1}{(\tau + d)^k} \right) e^{-2\pi i m \tau}\, d\tau = \\ &\overset{(*)}{=} \sum_{d\in\mathbb{Z}} \int_{\tau=0+iy}^{1+iy} \frac{1}{(\tau+d)^k} e^{-2\pi i m\tau}\, d\tau = \end{aligned} \tag{2}$$

(dokonując podstawienia $t \mapsto t-d$ oraz korzystając z 1-okresowosci $e^{-2\pi i m\tau}$)

$$= \sum_{d\in\mathbb{Z}} \int_{\tau=d+iy}^{d+1+iy} \frac{1}{\tau^k} e^{-2\pi i m\tau}\, d\tau = \int_{-\infty+iy}^{\infty+iy} \tau^{-k} e^{-2\pi i m\tau}\, d\tau$$

(b) mamy: $g_m(\tau) = \tau^{-k}e^{-2\pi i m\tau} = \sum_{l\in\mathbb{Z}} \frac{(-2\pi i m)^l}{l!}\tau^{l-k}$ – residuum to współczynnik przy τ^{-1}, czyli $(\frac{(-2\pi i m)^{k-1}}{(k-1)!})$

(c) całkując g_m wzdłuż prostokąta o wierzchołkach $P_1 = n+iy$, $P_2 = -n+iy$, $P_3 = -n-in$, $P_4 = n-in$ i korzystając z tw. o residuach:

$$2\pi i \cdot Res_{\tau=0} g_m(\tau) = \int_{P_1P_2P_3P_4} g_m(\tau)d\tau = (\int_{P_1P_2} + \int_{P_2P_3} + \int_{P_3P_4} + \int_{P_4P_1})g_m(\tau)d\tau$$

Ponadto:

– dla $\Im\tau = -n$ mamy: $|g_m(\tau)| = |\tau^{-k}e^{-2\pi i m\tau}| \leqslant n^{-k}e^{\Re(-2\pi i m\tau)} = n^{-k}e^{-2\pi mn)}$, więc $|\int_{-n+in}^{n-in} g_m(\tau)| \leqslant |P_3P_4| \cdot \sup_{\tau\in P_3P_4}|g_m(\tau)| \leqslant 2n\cdot n^{-k}e^{-2\pi mn} \to 0$ przy $n\to\infty$,

– dla $\Re\tau = \pm n$, $\Im\tau \leqslant y$, $y < n$ mamy: $|g_m(\tau)| = |\tau^{-k}e^{-2\pi i m\tau}| \leqslant n^{-k}e^{\Re(-2\pi i m\tau)} = n^{-k}e^{2\pi my)}$, więc $|\int_{n-in}^{n+iy} g_m(\tau)| \leqslant 2n\cdot n^{-k}e^{2\pi my} \to 0$ przy $n\to\infty$,

(d) Ustalmy $y>0$. Ze wzoru sumacyjnego Poissona dla funkcji $h(x) = (x+iy)^{-k} = \tau^{-k}$ mamy:

$$\sum_{d\in\mathbb{Z}} \frac{1}{(\tau+d)^k} = \sum_{d\in\mathbb{Z}} h(x+d) = \sum_{m\in\mathbb{Z}} e^{2\pi i m x}\widehat{h}(m)$$

gdzie

$$\widehat{h}(m) = \int_{-\infty}^{\infty} h(t)\, e^{-2\pi i m t}\, dt = e^{-2\pi m y}\int_{-\infty+iy}^{\infty+iy} \tau^{-k}e^{-2\pi i m\tau}\, d\tau = e^{-2\pi m y}a_m$$

1.1.9 Załóżmy nie wprost, że $c \notin Im(j)$. Wtedy z zasady argumentu:

$$0 = \frac{1}{2\pi i}\int_\gamma \frac{(j(t)-c)'}{j(t)-c}dt = \frac{1}{2\pi i}\int_\gamma \frac{j(t)'}{j(t)-c}dt$$

gdzie γ jest sumą łuku L okręgu jednostkowego od $P_1 = \frac{-1+i\sqrt{3}}{2}$ do $P_2 = \frac{1+i\sqrt{3}}{2}$ oraz odcinków P_2P_3, P_3P_4, P_4P_1, gdzie $P_3 = \frac{1}{2}+iy$, $P_4 = -\frac{1}{2}+iy$ dla pewnego $y>0$. Równości $j(\tau) = j(\tau+1)$ oraz $j(\tau) = j(-1/\tau)$ pokazują, że

$$\int_\gamma \frac{j(t)'}{j(t)-c}dt = \int_{P_3P_4} \frac{j(t)'}{j(t)-c}dt$$

(odcinki P_2P_3, P_4P_1 kasują się; łuki od P_1 do i oraz od Q do P_2 też).
Zauważmy, że $j(t) = J(q) = \frac{1}{q}+\ldots$, więc zamieniając zmienne:

$$\int_{P_3P_4} \frac{j(t)'}{j(t)-c}dt = \begin{pmatrix} q & = & e^{2\pi i t}, \\ dq & = & 2\pi i q dt, \\ j'(t) & = & 2\pi i q J'(q) \end{pmatrix} = 2\pi i\int_\omega \frac{J'(q)dq}{J(q)-c} = 2\pi i \int_\omega \frac{\frac{-1}{q^2}+\ldots}{J(q)-c}dq = 2\pi i\int_\omega \frac{-1+\ldots}{q^2\cdot(J(q)-c)}dq$$

gdzie ω jest okręgiem o środku w 0 i promieniu $e^{-2\pi y}$. Zauważmy, że $q(J(q)-c) = 1+q\cdot(\ldots)\to 1$ dla $q\to 0$, więc biorąc dostatecznie duże y, funkcja $\frac{J'(q)}{J(q)-c} = \frac{-1+\ldots}{q^2\cdot(J(q)-c)}$ będzie miała tylko jeden biegun, tzn. 0 z residuum 1. Stąd z tw. o residuach:

$$\int_{P_3P_4} \frac{j(t)'}{j(t)-c}dt = 1$$

– sprzeczność kończy dowód.

Podrozdział 1.2

1.2.1

1.2.2

1.2.3 (a) ??????

(b) z Chińskiego Tw. o Resztach $\mathbb{Z}/n \cong \bigoplus_{p^\alpha || n} \mathbb{Z}/p^\alpha$, więc $\mathrm{Sl}_2(\mathbb{Z}/n) \cong \bigoplus_{p^\alpha || n} \mathrm{Sl}_2(\mathbb{Z}/p^\alpha)$ oraz

$$|\mathrm{Sl}_2(\mathbb{Z}/n)| = \prod_{p^\alpha || n} |\mathrm{Sl}_2(\mathbb{Z}/p^\alpha)| = \prod_{p^\alpha || n} p^{3\alpha}(1 - 1/p^2) = n^3 \prod_{p|n}(1 - 1/p^2)$$

Ponadto $\mathrm{Sl}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{Sl}_2(\mathbb{Z}/N)$, więc $[\mathrm{Sl}_2(\mathbb{Z}) : \Gamma(N)] = |\mathrm{Sl}_2(\mathbb{Z}/N)|$.

(c) ad. surjektywność: $\Gamma_1(N) \ni \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^b \mapsto b \in \mathbb{Z}/N$.

ad. jądro: oczywiste.

(d) ad. surjektywność: niech $d \in (\mathbb{Z}/N)^*$ oraz $ad \equiv 1 \pmod N$, $ad = kN + 1$. Wtedy:

$$\Gamma_0(N) \ni \begin{bmatrix} a & k \\ N & d \end{bmatrix} \mapsto d \in (\mathbb{Z}/N)^*$$

ad. jądro: oczywiste.

(e)

$$[\mathrm{Sl}_2(\mathbb{Z}) : \Gamma_0(N)] = \frac{[\mathrm{Sl}_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma_0(N) : \Gamma_1(N)] \cdot [\Gamma_1(N) : \Gamma(N)]} = \frac{n^3 \prod_{p|n}(1 - 1/p^2)}{|\mathbb{Z}/N| \cdot |(\mathbb{Z}/N)^*|} = \frac{n^3 \prod_{p|n}(1 - 1/p^2)}{n \cdot n \cdot \prod_{p|n}(1 - 1/p)} = n \cdot \prod_{p|n}(1+1/p)$$

1.2.4

1.2.6 Załóżmy, że $f(\tau) = \sum_n a_n q_N^n$, $q_N = \exp(2\pi i\tau/N)$, $|a_n| \leqslant Cn^r$. Oznaczmy: $\tau = x + iy$, $y > 0$.

(a) Funkcja $g(t) = t^r e^{-2\pi yt/N}$ jest rosnąca w przedziale $[0, \frac{rN}{2\pi y}]$ i malejąca w $[\frac{rN}{2\pi y}, \infty)$, więc:

$$|f(\tau)| = |\sum_n a_n q_N^n| \leqslant \sum_n |a_n||q_N|^n \leqslant a_0 + C\sum_n n^r e^{-2\pi ny/N} \leqslant$$

$$\leqslant a_0 + C \sum_{0 \leqslant n \leqslant \frac{rN}{2\pi y} - 1} \int_n^{n+1} g(n+1)\, dt + C \sum_{n > \frac{rN}{2\pi y}} \int_n^{n+1} g(n)\, dt + \underbrace{g(\frac{rN}{2\pi y})}_{\leqslant C/y^r} \leqslant$$

$$\leqslant C + C \cdot (\int_0^\infty g(t)\, dt + 1/y^r) = (\text{podstawienie } u = 2\pi ty/N) = C_0 + C \cdot (\frac{C_1}{y^{r+1}} \underbrace{\int_0^\infty u^r e^{-u}\, du}_{=\Gamma(1)=\text{stała}} + 1/y^r) =$$

$$= C_0 + C/y^r$$

(b) aby pokazać, że $f[\alpha]_k$ jest holomorficzna w ∞, wystarczy pokazać, że $\lim_{y\to\infty} q_N \cdot f[\alpha]_k(\tau) = 0$. Zauważmy, że $f(\tau) = f(\tau + N)$, więc bez straty ogólności możemy założyć, że $0 \leqslant x \leqslant N$ – wtedy $c_1 y \leqslant |c\tau + d| \leqslant c_2 y$. Z podpunktu (a) mamy:

$$|f[\alpha]_k(\tau)| = |(c\tau + d)^{-k} f(\alpha(\tau))| \leqslant C \cdot \left|(c\tau + d)^{-k}(1 + (Im(\alpha(\tau))^{-r}))\right| =$$

$$= C \cdot \left|(c\tau + d)^{-k}(1 + \left(\frac{|c\tau + d|^2}{y}\right)^r)\right| \leqslant Cy^{r-k}$$

Ale $|q_N| = e^{-2\pi y/N}$, więc:

$$|q_N f[\alpha]_k(\tau)| \leqslant Ce^{-2\pi y/N} y^{r-k} \xrightarrow[y\to\infty]{} 0$$

1.2.8 (a) Z tożsamości (1.2):

$$\sum_{d\in\mathbb{Z}} \frac{1}{(\tau + d)^2} = -(2\pi)^2 \sum_{m=1}^{\infty} mq^m$$

– podstawiając $\tau := c\tau$ i sumując po $c \neq 0$:

$$G_2(\tau) = \sum_{d\in\mathbb{Z}\setminus\{0\}} \frac{1}{d^2} + \sum_{c\neq 0}\sum_{d\in\mathbb{Z}} \frac{1}{(c\tau+d)^2} = 2\zeta(2) - (2\pi)^2 \sum_{c\neq 0}\sum_{m=1}^{\infty} m\exp(2\pi i c m\tau) =$$

$$= 2\zeta(2) - (2\pi)^2 \sum_{c\neq 0}\sum_{m=1}^{\infty} m q^{cm}$$

– zauważmy przy tym, że prawa strona jest absolutnie zbieżna (jako szereg potęgowy w obszarze zbieżności), więc możemy przestawić wyrazy, by dostać:

$$G_2(\tau) = 2\zeta(2) - (2\pi)^2 \sum_n \left(\sum_{d|n, d\in\mathbb{Z}} d \right) q^n = 2\zeta(2) - 8\pi^2 \sum_n \sigma(n) q^n$$

(b)

(e) oznaczmy $\widetilde{G}_2(\tau) = G_2(\tau) - \frac{\pi}{\Im(\tau)}$ (jest to wtedy funkcja $\mathrm{Sl}_2(\mathbb{Z})$–niezmiennicza wagi 2) – wtedy: $G_{2,N}(\tau) = G_2(\tau) - NG_2(N\tau) = \widetilde{G}_2(\tau) - N\widetilde{G}_2(N\tau)$. Niech $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$, wtedy $\gamma' := \begin{bmatrix} a & Nb \\ c/N & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$ oraz $N\gamma(\tau) = \gamma'(N\tau)$, więc:

$$G_{2,N}(\gamma\tau) = \widetilde{G}_2(\gamma\tau) - N\widetilde{G}_2(N\gamma(\tau)) = \frac{1}{(c\tau+d)^2}\widetilde{G}_2(\tau) - N\widetilde{G}_2(\gamma'(N\tau)) =$$

$$= \frac{1}{(c\tau+d)^2}\widetilde{G}_2(\tau) - \frac{1}{(\frac{c}{N}N\tau+d)^2} N\widetilde{G}_2(N\tau) = \frac{1}{(c\tau+d)^2} G_{2,N}(\tau)$$

Podrozdział 1.5

W zadaniach będziemy często korzystali z następującego oczywistego faktu:

Fakt Niech $\tau' = \gamma\tau$, $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$. Wtedy

$$F_\gamma : E_\tau \to E_{\tau'}, F_\gamma(x) = j(\gamma,\tau)^{-1}x = \frac{1}{c\tau+d}x$$

jest izomorfizmem. W szczególności: $F_\gamma(a\tau+b) = \tau'$, $F_\gamma(c\tau+d) = 1$, $F_\gamma(\tau) = d\tau' - b$, $F_\gamma(1) = -c\tau' + a$.

1.5.3

1.5.4 Mamy:

$$w_N \begin{bmatrix} a & b \\ c & d \end{bmatrix} w_N^{-1} = \begin{bmatrix} d & -Nb \\ -c/N & a \end{bmatrix} \in \Gamma_0(N)$$

więc $w_n\Gamma_0(N)w_n^{-1} = \Gamma_0(N)$, więc funkcja: $G(\Gamma_0(N)\tau) = \Gamma_0(N)w_n(\tau)$ jest dobrze określona (nie zależy od wyboru reprezentanta τ).
Wykażemy, że $G([E,C]) = [E/C, E[n]/C]$. Istotnie,

$$G([E_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle]) = [E_{w_n(\tau)}, \langle \frac{1}{N} + \Lambda_{w_n(\tau)} \rangle] = [E_{-1/(N\tau)}, \langle \frac{1}{N} + \Lambda_{-1/(N\tau)} \rangle]$$

(korzystając z tego, że $\frac{-1}{N\tau} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} N\tau$ oraz z izomorfizmu z **Faktu:** $F : E_{-1/(N\tau)} \to E_{N\tau}$, $F(1) = N\tau$, $F(\frac{-1}{N\tau}) = 1$ – w szczególności $F(\frac{1}{N} + \Lambda_{-1/(N\tau)}) = \tau + \Lambda_{N\tau}$)

$$= [E_{N\tau}, \langle \tau + \Lambda_{N\tau} \rangle]$$

Ponadto:

$$[E_\tau/\langle\frac{1}{N}+\Lambda_\tau\rangle, E_\tau[N]/\langle\frac{1}{N}+\Lambda_\tau\rangle] = \left[\frac{\mathbb{C}/(\mathbb{Z}+\tau\mathbb{Z})}{(\frac{1}{N}\mathbb{Z}+\tau\mathbb{Z})/(\mathbb{Z}+\tau\mathbb{Z})}, \frac{(\frac{1}{N}\mathbb{Z}+\frac{\tau}{N}\mathbb{Z})/(\mathbb{Z}+\tau\mathbb{Z})}{(\frac{1}{N}\mathbb{Z}+\tau\mathbb{Z})/(\mathbb{Z}+\tau\mathbb{Z})}\right] =$$

(III tw. o izomorfizmie)

$$= \left[\frac{\mathbb{C}}{\frac{1}{N}\mathbb{Z}+\tau\mathbb{Z}}, \frac{\frac{1}{N}\mathbb{Z}+\frac{\tau}{N}\mathbb{Z}}{\frac{1}{N}\mathbb{Z}+\tau\mathbb{Z}}\right] =$$

(jednokładność o skali N jest izomorfizmem)

$$= \left[\frac{\mathbb{C}}{\mathbb{Z}+N\tau\mathbb{Z}}, \frac{\mathbb{Z}+\tau\mathbb{Z}}{\mathbb{Z}+N\tau\mathbb{Z}}\right] = [E_{N\tau}, \langle\tau+\Lambda_{N\tau}\rangle] = G([E_\tau, \langle\frac{1}{N}+\Lambda_\tau\rangle])$$

1.5.5

(a) 1.5.6 Zgodnie z Twierdzeniem 1.5.1(b) możemy bez straty ogólności przyjąć, że $[E, C, Q] = [E_\tau, C, \frac{1}{N}+\Lambda_\tau]$. Niech $C = \langle a\frac{\tau}{p} + b\frac{1}{p} + \Lambda_\tau\rangle$. Ponadto $C \cap \langle Q\rangle \neq \{0\}$ zachodzi wtw. gdy $a \equiv 0 \pmod p$ oraz $p|N$. Stąd mamy 2 możliwości:

1^o $a \in (\mathbb{Z}/p)^*$ – wtedy $C = \langle a\frac{\tau}{p} + b\frac{1}{p} + \Lambda_\tau\rangle = \langle\frac{\tau}{p} + \underbrace{ba^{-1}}_{=j}\frac{1}{p} + \Lambda_\tau\rangle$. Stąd, biorąc $\tau' = \gamma\tau$, $\gamma = \begin{bmatrix} 1 & j \\ 0 & 1 \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$ dostajemy:

$$[E_\tau, C, \frac{1}{N}+\Lambda_\tau] = [E_{\tau'}, \langle\tau'/p+\Lambda_{\tau'}\rangle, \frac{1}{N}+\Lambda_{\tau'}]$$

2^o $a \equiv 0 \pmod p$ oraz $p \nmid N$ – wtedy $b \in (\mathbb{Z}/p)^*$ oraz $C = \langle b\frac{1}{p}+\Lambda_\tau\rangle = \langle\frac{1}{p}+\Lambda_\tau\rangle$. Ponadto $(p, N) = 1$ $\Rightarrow$ $Ap - BN = 1$ dla pewnych $A, B \in \mathbb{Z}$. Oczywiście $\frac{1}{p}+\Lambda_\tau = \frac{Ap\tau+1}{p}+\Lambda_\tau$, $\frac{1}{N}+\Lambda_\tau = \frac{BN\tau+1}{N}+\Lambda_\tau$. Stąd, biorąc $\tau' = \gamma\tau$, $\gamma = \begin{bmatrix} Ap & 1 \\ BN & 1 \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$ mamy:

$$[E_\tau, C, \frac{1}{N}+\Lambda_\tau] = [E_{\tau'}, \langle\tau'/p+\Lambda_{\tau'}\rangle, \frac{1}{N}+\Lambda_{\tau'}]$$

(b) Wykażemy teraz, że $[E_\tau, \langle\tau/p+\Lambda_\tau\rangle, \frac{1}{N}+\Lambda_\tau] = [E_{\tau'}, \langle\tau'/p+\Lambda_{\tau'}\rangle, \frac{1}{N}+\Lambda_{\tau'}]$ wtw. gdy $\tau = \gamma\tau'$ dla pewnego $\gamma \in \Gamma_1^0(N, p)$. Istotnie, jeżeli $[E_\tau, \langle\tau/p+\Lambda_\tau\rangle, \frac{1}{N}+\Lambda_\tau] = [E_{\tau'}, \langle\tau'/p+\Lambda_{\tau'}\rangle, \frac{1}{N}+\Lambda_{\tau'}]$, to z Tw. 1.5.1 (b) mamy: $\tau = \gamma\tau'$ dla pewnego $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_1(N)$ oraz izomorfizm rozszerzonych krzywych eliptycznych zadany jest przez F_γ jak w fakcie. Ale $F_\gamma(\langle\tau/p+\Lambda_\tau\rangle) = \langle\tau'/p+\Lambda_\tau\rangle$ wtw. gdy $\langle d\tau - b/p + \Lambda_\tau\rangle = \langle\tau'/p+\Lambda_\tau\rangle$, więc musi być $b \equiv 0 \pmod p$ oraz $\gamma \in \Gamma_1^0(N, p)$.
Odwrotne twierdzenie również wynika od razu z Faktu.

(c) Odwzorowanie $\Gamma_1^0(N, p) \ni [\tau] \mapsto [\tau/p] \in \Gamma_1(N)$ odpowiada odwzorowaniu: $[E, C, Q] = [E_\tau, \langle\tau/p + \Lambda_\tau\rangle, \frac{1}{N}+\Lambda_\tau] \mapsto [E_{\tau/p}, \frac{1}{N}+\Lambda_{\tau/p}]$. Ale $E/C = (\mathbb{C}/\Lambda_\tau)/((\tau/p+\Lambda_\tau)/\Lambda) \cong \mathbb{C}/(\tau/p+\Lambda_\tau) = \mathbb{C}/(\tau/p\mathbb{Z} + \mathbb{Z}) = E_{\tau/p}$ oraz przy tym izomorfizmie $\frac{1}{N}+\Lambda_{\tau/p} = (Q+\Lambda_\tau)+C$ przechodzi na $Q+C$. Stąd $[E, Q, C] \mapsto [E/C, Q+C]$.

Rozdział II

2.1.3 (a) U_1', U_2' są zwartymi zbiorami zawartymi w $\mathcal{H}$, więc są zawarte w pewnych zbiorach $A_i = \{x+iy \in \mathbb{C} : |x| \leqslant M_i, c_i \leqslant y \leqslant M_i\}$, gdzie $c_i, M_i > 0$. Wtedy dla $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\tau = x+iy \in U_1'$:

1^o jeżeli $|c| > \sqrt{M_1/(c_2c_1^2)}$ to

$$\Im(\gamma(\tau)) = \frac{\Im(\tau)}{|c\tau+d|^2} \leqslant \frac{M_1}{|c\tau+d|^2} \leqslant \frac{M_1}{|\Im(c\tau+d)|^2} = \frac{M_1}{|cy|^2} \leqslant \frac{M_1}{|cc_1|^2} < c_2 \leqslant \inf\{\Im(\tau) : \tau \in U_2'\}$$

2^o jeżeli $|c| \leqslant \sqrt{M_1/(c_2c_1^2)}$, $|d| > \sqrt{M_1/(c_2c_1^2)}M_1 + \frac{M_1}{c_2}$, to:

$$\Im(\gamma(\tau)) = \frac{\Im(\tau)}{|c\tau+d|^2} \leqslant \frac{M_1}{|c\tau+d|^2} \leqslant \frac{M_1}{|\Re(c\tau+d)|^2} = \frac{M_1}{|cx+d|^2} \leqslant \frac{M_1}{(|d|-|c|\cdot|x|)^2} < c_2 \leqslant \inf\{\Im(\tau) : \tau \in U_2'\}$$

(b) wystarczy zauważyć, że dla $A = \begin{bmatrix} a' & b' \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$ mamy:

$$AB^{-1} = \begin{bmatrix} a' & b' \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = \begin{bmatrix} a'd-b'c & * \\ 0 & ad-bc \end{bmatrix} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix}$$

(c) zauważmy, że dla $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{R})$:

$$\gamma i = i \Leftrightarrow ai+b = -c+di \Leftrightarrow \gamma = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}, a^2+b^2=1 \Leftrightarrow \gamma \in SO_2(\mathbb{R})$$

Ponadto dla $\tau = x+iy$, $s(\tau) = \frac{1}{\sqrt{y}}\begin{bmatrix} y & x \\ 0 & 1 \end{bmatrix}$ mamy: $s(\tau)i = \tau$, więc odwzorowanie $\gamma \mapsto \gamma i$ wyznacza izomorfizm $SL_2(\mathbb{R})/SO_2(\mathbb{R}) \cong \mathcal{H}$.

Załóżmy, że U_1', U_2' są otoczeniami τ_1, τ_2 o zwartych domknięciach w $\mathcal{H}$. Jeżeli $\gamma(e_1) = e_2$, to $\gamma \circ s(e_1)i = s(e_2)i$, czyli $s(e_2)^{-1} \circ \gamma \circ s(e_1)i = i$ oraz $s(e_2)^{-1} \circ \gamma \circ s(e_1) \in SO_2(\mathbb{R})$, bądź równoważnie: $\gamma \in S(e_1,e_2) := s(e_2)\cdot SO_2(\mathbb{R})\cdot s(e_1)^{-1}$. Stąd:

$$\{\gamma \in \mathrm{Sl}_2(\mathbb{Z}) : U_1' \cap \gamma(U_2') \neq \varnothing\} \subset \left(\bigcup_{e_1 \in \overline{U_1'}, e_2 \in \overline{U_2'}} S(e_1,e_2)\right) \cap \mathrm{Sl}_2(\mathbb{Z})$$

Wystarczy teraz zauważyć, że:

- dla $\tau \in \overline{U_i'}$ norma $\|s(\tau)\|$, jest ograniczona (bo $\|s(\tau)\|$ jest ciągłą funkcją, zaś $\overline{U_i'}$ jest zwarte)
- $SO_2(\mathbb{R})$ jest ograniczone (jeżeli $\gamma \in SO_2(\mathbb{R})$, to $\gamma = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$, $a^2+b^2=1$, więc $\|\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\| = 2(a^2+b^2) = 2)$,
- $\mathrm{Sl}_2(\mathbb{Z})$ jest podzbiorem dyskretnym $SL_2(\mathbb{R})$ (jeżeli $A \in SL_2(\mathbb{Z})$ oraz $\|A\| < 1$, to A) [??????????coś z normami...]

więc ostatecznie $\left(\bigcup_{e_1 \in \overline{U_1'}, e_2 \in \overline{U_2'}} S(e_1,e_2)\right) \cap \mathrm{Sl}_2(\mathbb{Z})$ jest zbiorem skończonym.

2.2.1 Załóżmy, że $\Gamma_\tau = I$. Biorąc w Proposition 2.2.1 $\tau_1 = \tau_2 = \tau$ oraz $U = U_1 \cap U_2$ dostajemy:

jeżeli dla pewnego $\gamma \in \mathrm{Sl}_2(\mathbb{Z})$ mamy: $\gamma(U) \cap U \neq \varnothing$, to $\gamma(\tau) = \tau$, czyli $\gamma = I$.

Stąd rzutowanie $\pi : U \to \pi(U)$ jest różnowartościowe – jeżeli $\eta_1, \eta_2 \in U$, $\pi(\eta_1) = \pi(\eta_2)$, to $\exists_{\gamma\in\Gamma} \quad \eta_1 = \gamma\eta_2$ oraz $\gamma(U) \cap U \neq \varnothing$, więc $\gamma = I$, $\eta_1 = \eta_2$. Wystarczy zauważyć, że π jest odwzorowaniem otwartym, jest więc homeomorfizmem.

2.2.2 Mamy:

$$\begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}^{-1} = \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix}$$

więc dla małych τ:

$$\gamma(\tau) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\tau \approx \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}^{-1} = -\tau$$

2.2.4 Biorąc w Proposition 2.2.1 $\tau_1 = \tau_2 = \tau$ oraz $U = U_1 \cap U_2$ dostajemy:

jeżeli dla pewnego $\gamma \in \mathrm{Sl}_2(\mathbb{Z})$ mamy: $\gamma(U) \cap U \neq \varnothing$, to $\gamma(\tau) = \tau$.

Załóżmy, że $\tau' \in U$ jest punktem eliptycznym, $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})_{\tau'} \setminus \{\pm I\}$. Wtedy $\tau' \in \gamma(U) \cap U \neq \varnothing$, więc $\gamma(\tau) = \tau$ oraz $\gamma \in \mathrm{Sl}_2(\mathbb{Z})_\tau$. Ale γ może mieć co najwyżej jeden punkt stały na górnej półpłaszczyźnie: rozwiązania równania kwadratowego $\frac{az+b}{cz+d} = z$ dla $c \neq 0$ są rzeczywiste lub wzajmenie sprzężone. Stąd $\tau' = \tau$.

2.3.2 Jeżeli $\gamma \in \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z}) \setminus \{I_2\}$ spełnia $\gamma\tau = \tau$ dla pewnego $\tau \in \mathcal{H}$, to $c \neq 0$ (w przeciwnym wypadku $\gamma = \pm I_2$) – dostajemy więc równanie kwadratowe $\frac{a\tau+b}{c\tau+d} = \tau$, czyli $c\tau^2 + (d-a)\tau - b = 0$. Równanie to ma rozwiązania $z = \frac{(a-d)\pm\sqrt{\Delta}}{2c}$ – jedno z tych rozwiązań należy do górnej półpłaszczyzny wtw. gdy $\sqrt{\Delta} \in i\mathbb{R}$, tzn. gdy $\Delta < 0$, czyli:

$$0 > \Delta = (a-d)^2 + 4bc = (a-d)^2 + 4(ad-1) = (a+d)^2 - 4 \Leftrightarrow |a+d| < 2$$

2.3.4 (b) Niech $n \in \{3, 4, 6\}$, $\gamma \in \mathrm{Sl}_2(\mathbb{Z})$ będzie rzędu n, zaś ω będzie n–tym pierwiastkiem z jedności. Wtedy $\mathbb{Z}[\omega] = \mathbb{Z} + \omega\mathbb{Z}$ jest dziedziną ideałów głównych (pierścień liczb całkowitych ciała kwadratowego $\mathbb{Q}(\omega)$), zaś $L = \mathbb{Z}^2$ ma strukturę skończenie gen. $\mathbb{Z}[\omega]$–modułu ($(a + b\omega) \cdot v := (aI + b\gamma)v$). Z twierdzenia klasyfikacyjnego dla skończenie gen. modułów nad PIDami: $L \cong \oplus_{i=1}^k \mathbb{Z}[\omega]/I_k$ jako $\mathbb{Z}[\omega]$–moduły dla pewnych ideałów $I_k \trianglelefteq \mathbb{Z}[\omega]$. Zauważmy, że L nie ma torsji, więc jest wolnym $\mathbb{Z}[\omega]$–modułem, a porównując rangi jako $\mathbb{Z}$–modułów, stwierdzamy, że $L \cong \mathbb{Z}[\omega]$. Niech $\phi : \mathbb{Z}[\omega] \to L$ będzie izomorfizmem. Niech $u = \phi(1)$, $v = \phi(\omega)$ – wtedy $\gamma u = \phi(\omega \cdot 1) = v$ oraz

$$\gamma v = \phi(\omega \cdot \omega) = \begin{cases} \phi(-\omega - 1) = -u - v, & \text{dla } n = 3 \\ \phi(-1) = -u, & \text{dla } n = 4 \\ \phi(\omega - 1) = -u + v, & \text{dla } n = 6 \end{cases}$$

oraz w bazie u, v macierz γ ma postać:

$$A\gamma A^{-1} = \begin{cases} \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}, & \text{dla } n = 3 \\[2ex] \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, & \text{dla } n = 4 \\[2ex] \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}, & \text{dla } n = 6 \end{cases}$$

(gdzie $A \in GL_2(\mathbb{Z})$ – macierz przejścia między bazami $[u, v]$, $[(1, 0), (0, 1)]$). Zamieniając w razie potrzeby bazę $[u, v]$ na $[v, u]$ (odpowiada to zamianie kolumn) tak, by wyznacznik był równy 1, dostajemy tezę.

2.3.5

2.3.7 Zauważmy, że Γ ma punkty eliptyczne wtw. gdy do Γ należy pewne macierz $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ spełniająca $|a+d| < 2$ (por. zadanie 2.3.2).

(a) Jeżeli $\Gamma(N)$ ma punkty eliptyczne, to istnieją $a, b, c, d \in \mathbb{Z}$, $a, d \equiv 1 \pmod N$, $b, c \equiv 0 \pmod N$, $ad - bc = 1$, $a + d \in \{0, \pm 1\}$.

1^o jeżeli $a = -d$, to $1 \equiv a \equiv -d \equiv -1 \pmod N$, więc $N = 2$. Ale wtedy $bc \equiv 0 \pmod 4$, więc:

$$1 = ad - bc = -a^2 - bc \equiv -a^2 \pmod 4$$

co jest niemożliwe, bo -1 jest nieresztą $\pmod 4$.

2^o jeżeli $a+d=\pm 1$, to $2 \equiv a+d \equiv \pm 1 \pmod N$, więc $N=3$, $a+d=-1$. Stąd $bc \equiv 0 \pmod 9$ oraz:

$$1 = ad - bc \equiv -a(a+1) \pmod 9 \Rightarrow (2a+1)^2 \equiv 5 \pmod 9$$

co jest niemożliwe, bo 5 jest nieresztą $\pmod 9$.

(b) wynika z dowodu (a).

(c) załóżmy, że $ad-bc=1$, $a+d \in \{0, \pm 1\}$, $c \equiv 0 \pmod p$ dla $p \equiv -1 \pmod{12}$.

1^o jeżeli $a=-d$, to $1 = ad - bc \equiv -a^2 \pmod p$, co jest niemożliwe, bo $(\frac{-1}{p}) = -1$.

2^o jeżeli $a+d=\pm 1$, to $1 = ad - bc \equiv a(\pm 1 - a) \pmod p$, czyli $a^2 \pm a + 1 \equiv 0 \pmod p$. Równanie to ma rozwiązania $\pmod p$ wtw. gdy wyróżnik $\Delta = -3$ jest kwadratem – to jednak nie jest prawdą z własności symbolu Legendre'a:

$$(\frac{-3}{p}) = (\frac{-1}{p})(\frac{3}{p}) = (-1)^{(p-1)/2} \cdot (-1)^{(p-1)\cdot(3-1)/4} \cdot (\frac{p}{3}) = (-1)\cdot(-1)\cdot(-1) = -1$$

(d) jeżeli $-I \notin \Gamma$, to mielibyśmy $2 = h_\tau = |\Gamma_\tau|$. Stąd Γ_τ musi być dwuelementową podgrupą $\mathrm{Sl}_2(\mathbb{Z})$, co (z zadania 2.3.3) oznacza że $\Gamma_\tau = \{\pm I\}$– sprzeczność kończy dowód.

2.4.3 Niech $\{U_\alpha\}$ będzie dowolnym pokryciem zbiorami otwartymi. Wtedy $\infty \in U_\beta$ dla pewnego β. Z definicji topologii na $\mathcal{H}^*$ istnieje $M > 0$ tże $\mathcal{N}_M := \{\tau : \Im(\tau) > M\} \subset U_\beta$. Ale $\mathcal{D} \cap \{\tau : \Im(\tau) \leqslant M\}$ jest zwarty jako domknięty i ograniczony podzbiór $\mathbb{C}$, więc ma skończone podpokrycie $\{U_i\}_{i=1}^n$. Stąd $\{U_i\}_{i=1}^n \cup \{U_\beta\}$ jest skończonym podpokryciem $\{U_\alpha\}$ dla $\mathcal{D}^*$.

2.4.4 (a) niech $\Gamma(N) \subset \Gamma$, $\gamma = \begin{bmatrix} 1 & N \\ 0 & 1 \end{bmatrix}$– wtedy $\langle\gamma\rangle \subset \Gamma(N) \subset \delta\{\pm I\}\Gamma\delta^{-1}$, więc (ponieważ $\gamma\infty = \infty$):

$$|\,\mathrm{Sl}_2(\mathbb{Z})_\infty/(\delta\{\pm I\}\Gamma\delta^{-1})_\infty| \leqslant |\,\mathrm{Sl}_2(\mathbb{Z})_\infty/\langle\gamma\rangle| =$$

$$|\{\pm \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} : m \in \mathbb{Z}\}/\langle\gamma\rangle| = |(\mathbb{Z}/2 \oplus \mathbb{Z})/(1 \oplus N\mathbb{Z})| = 2N$$

(b)

2.4.7 Wybierzmy $\tau \in X(\Gamma_1)$ i niech $(U_\tau, \Psi_\tau : U_\tau \to V_\tau)$ będzie jego mapą z atlasu, $(U_{\gamma(\tau)}, \Psi_{\gamma(\tau)} : U_\tau \to V_\tau)$ mapą w atlasie $X(\Gamma_2)$. Chcemy pokazać, że $\Psi_{\gamma(\tau)} \circ F \circ \Psi_\tau^{-1} : V_\tau \to V_{\gamma(\tau)}$ jest holomorficzne, gdzie $F : X(\Gamma_1) \to X(\Gamma_2)$, $F(\tau\Gamma) = \gamma(\tau)\Gamma$. Rozważmy dwa przypadki:

1^o **τ nie jest cuspem. Wtedy $\gamma\tau$ też nie jest cuspem.**

Niech h będzie periodem τ w Γ, zaś H – periodem $\gamma(\tau)$ w Γ_2. Niech też δ_τ przeprowadza τ na 0 oraz $\overline{\tau}$ na ∞. Wtedy $\gamma(\Gamma_1)_\tau\gamma^{-1} = (\gamma\Gamma_1\gamma^{-1})_{\gamma\tau} \leqslant (\Gamma_2)_{\gamma\tau}$, więc z tw. Lagrange'a: $h|H$. Mamy:

$$\Psi_{\gamma(\tau)} \circ F \circ \Psi_\tau^{-1}(z) = \Psi_{\gamma(\tau)}(\gamma\delta_\tau^{-1}z^{1/h}) = \left((\delta_{\gamma(\tau)}\gamma\delta_\tau^{-1})(z^{1/h})\right)^H$$

Zauważmy jednak, że $\delta_{\gamma(\tau)}\gamma\delta_\tau^{-1}$ przenosi 0 na 0 oraz ∞ na ∞, jest więc postaci $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, czyli działa jak mnożenie przez $\alpha := \frac{a}{b}$:

$$\Psi_{\gamma(\tau)} \circ F \circ \Psi_\tau^{-1}(z) = \alpha^H z^{H/h}$$

–jest to funkcja holomorficzna.

2^o **τ jest cuspem. Wtedy $\gamma\tau$ też jest cuspem.**

Niech H będzie szerokością τ w Γ, zaś h – szerokością $\gamma(\tau)$ w Γ_2. Niech też $\delta_\tau \in \mathrm{Sl}_2(\mathbb{Z})$ przeprowadza τ na ∞. Wtedy $\gamma(\Gamma_1)_\tau\gamma^{-1} \leqslant (\Gamma_2)_{\gamma\tau}$, więc $h|H$. Stąd

$$\Psi_{\gamma(\tau)} \circ F \circ \Psi_\tau^{-1}(z) = \Psi_{\gamma(\tau)}\left(\gamma\delta_\tau^{-1}\left(H\frac{\log z}{2\pi i}\right)\right) = \exp\left(2\pi i \cdot h \cdot \left(\delta_{\gamma(\tau)} \circ \gamma \circ \delta_\tau\right)^{-1}\left(\frac{H\log z}{2\pi i}\right)\right)$$

Tak jak poprzednio, $\delta_{\gamma(\tau)} \circ \gamma \circ \delta_\tau(w) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ dla pewnego α, a ponadto ponieważ $\delta_{\gamma(\tau)} \circ \gamma \circ \delta_\tau \in \mathrm{Sl}_2(\mathbb{Z})$, to $\alpha := \frac{a}{b} = 1$. (jest to), więc:

$$\Psi_{\gamma(\tau)} \circ F \circ \Psi_\tau^{-1}(z) = z^{H/h}$$

jest holomorficzna.

Rozdział III

3.1.4 (a) zauważmy, że dla $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$:

$$\gamma\alpha_j^{-1} = \gamma\alpha_{-j} = \begin{bmatrix} * & * \\ c - dj & * \end{bmatrix}$$

oraz

$$\gamma\alpha_\infty^{-1} = \begin{bmatrix} * & * \\ -d & * \end{bmatrix}$$

więc:

1^o jeżeli $p|d$, to $\gamma\alpha_\infty^{-1} \in \Gamma_0(p)$ oraz $p \nmid c$ (ponieważ $p \nmid ad - bc = 1$), więc $\gamma\alpha_j^{-1} \notin \Gamma_0(p)$ dla $j = 0, \ldots, p-1$.

2^o jeżeli $p \nmid d$, to $\gamma\alpha_j^{-1} \in \Gamma_0(p)$ tylko dla $j \equiv cd^{-1} \pmod p$ oraz $\gamma\alpha_\infty^{-1} \notin \Gamma_0(p)$.

(b) niech $\frac{m}{n} \in \mathbb{Q} \cup \{\infty\}$ będzie cuspem ($NWD(m,n) = 1$). Rozważmy 2 przypadki:

1^o $p|n$, $p \nmid m$ – wtedy:

$$\underbrace{\begin{bmatrix} M & N \\ -n & m \end{bmatrix}}_{\in\Gamma_0(p)} \frac{m}{n} = \frac{1}{0} = \infty$$

gdzie M, N spełniają: $Mm + Nn = 1$.

2^o $p \nmid n$ – wtedy:

$$\underbrace{\begin{bmatrix} n & -m \\ pC & D \end{bmatrix}}_{\in\Gamma_0(p)} \frac{m}{n} = 0$$

gdzie C, D są takie, że $np \cdot D + m \cdot C = 1$ (zauważmy, że $NWD(np, m) = 1$).

Ponadto ∞ oraz 0 nie są równoważne – jeżeli $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \frac{0}{1} = \infty$, to $d = 0$, więc (ponieważ $p \nmid ad - bc = 1$) $p \nmid c$.

(c) jeżeli $\gamma \in \Gamma_0(p)$ jest rzędu 4 oraz $\gamma\alpha_j(i) = \alpha_j(i)$, to $\alpha_j^{-1}\gamma\alpha_j \in \mathrm{Sl}_2(\mathbb{Z})_i = \langle\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\rangle$. Ponieważ $ord(\alpha_j^{-1}\gamma\alpha_j) = ord(\gamma) = 4$, to $\alpha_j^{-1}\gamma\alpha_j = \pm\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Stąd takie γ istnieje wtw. gdy: $\pm\alpha_j \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \alpha_j^{-1} \in \Gamma_0(p)$. Ale $\pm\alpha_j \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \alpha_j^{-1} = \pm\begin{bmatrix} * & * \\ j^2+1 & * \end{bmatrix}$, więc takie γ istnieje wtw. gdy $\exists_j \quad j^2 \equiv -1 \pmod p$.

Na podstawie **[DS, Corollary 2.3.5.]** wszystkie eliptyczne punkty $\Gamma_0(p)$ wysokości 2 są postaci $\alpha_j(i)$, więc liczba punktów eliptycznych to $\#\{j \in \mathbb{Z}/p : j^2 \equiv -1 \pmod p\}$.

(d) analogiczne.

(e)

3.3.6 Niech $\mathcal{A}_2(\Gamma) \ni f \mapsto \omega = (\omega_i)_{i\in J} \in \Omega^1(X(\Gamma))$. Chcemy wykazać, że $f \in \mathcal{S}_2(\Gamma)$ wtw. gdy ω jest holomorficzna. Istotnie, niech $U_i \subset \mathcal{H}$ będzie otoczeniem cuspa s o szerokości h i niech $\alpha \in \mathrm{Sl}_2(\mathbb{Z})$, $\alpha(\infty) = s$. Wtedy: $\omega_i = \frac{g_i(q)}{2\pi i q/h}\,dq$, gdzie $f[\alpha]_2 = g_j(q_h)$ $(q_h = \exp(2\pi i z/h))$. Ale $v_0(\omega_i) \geqslant 0$ wtw. $v_0(g_i) \geqslant 1$ wtw. $\lim_{q\to 0} g_i(q) = 0$ wtw. $\lim_{z\to i\infty} f[\alpha]_2(z) = 0$ wtw. f jest cusp formą.

Pozostaje zauważyć, że jeżeli f jest cusp formą, to ω jest holomorficzna w pozostałych punktach. Niech $U_i \subset \mathcal{H}$ będzie otoczeniem $\tau \in \mathcal{H}$, zaś $h = h_\tau$ będzie periodem τ. Wtedy $\omega_i = \frac{g_j(q)}{hq}\,dq$, gdzie $zf[\alpha]_2 = g_i(z^h)$, $\alpha = \begin{bmatrix} 1 & -\tau \\ 1 & -\overline{\tau} \end{bmatrix}^{-1}$. Zauważmy, że $v_0(g_i) = \frac{1}{h}v_0(zf[\alpha]_2) = \frac{1+v_0(f[\alpha]_2)}{h}$. Korzystając z:

Fakt $v_0(F) = v_\tau(F[\delta]_2)$, gdzie $\delta = \begin{bmatrix} 1 & -\tau \\ 1 & -\overline{\tau} \end{bmatrix}$, $\tau \in \mathcal{H}$.

Dowód: niech $F(z) = \sum_{n=N}^{\infty} a_n z^n$, $a_N \neq 0$. Wtedy

$$F\left(\frac{z-\tau}{z-\overline{\tau}}\right) = \frac{(z-\tau)^N}{(z-\overline{\tau})^N}\underbrace{\left(a_N + a_{N+1}\frac{z-\tau}{z-\overline{\tau}} + \ldots\right)}_{\text{nie zeruje się w } \tau}$$

czyli: $v_0(F(z)) = N = v_\tau(F(\frac{z-\tau}{z-\overline{\tau}}))$. Wystarczy teraz zauważyć, że $F[\delta]_2(z) = \underbrace{\quad * \quad}_{\text{nie zeruje się w } \tau} \cdot F(\frac{z-\tau}{z-\overline{\tau}})$.

Stąd $v_0(f[\alpha]_2) = v_\tau(f[\alpha\delta]_2) = v_\tau(f)$. Korzystając z:

Fakt Jeżeli $f \in \mathcal{M}_2(\Gamma)$, $\tau \in \mathcal{H}$, $h = h_\tau$, to $v_\tau(f) \geqslant h - 1$.

Dowód: Załóżmy, że $h > 1$ i niech $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_\tau \setminus \{\pm I\}$. Wtedy: $(cz+d)^2 f(z) = f(Bz)$. Podstawiając $z := \tau$: $(c\tau+d)^2 f(\tau) = f(\tau)$, więc $(c\tau+d)^2 = 1$ (co jest niemożliwe, bo $c \neq 0$ oraz $\tau \neq \frac{\pm 1 - d}{c}$) lub $f(\tau) = 0$.
Załóżmy, że $h = 3$. Wtedy różniczkując $(cz+d)^2 f(z) = f(Bz)$ dostajemy: $2(cz+d)f(z) + (cz+d)^2 f'(z) = \frac{1}{(cz+d)^2} f'(Bz)$. Podstawmy $z := \tau$, dostaniemy: $(c\tau+d)^2 f'(z) = \frac{1}{(c\tau+d)^2} f'(\tau)$. Stąd $f'(\tau) = 0$ lub $(c\tau+d)^4 = 1$ – to jest jednak niemożliwe, bo wtedy byłoby $c\tau + d \in \{\pm 1, \pm i\}$ oraz $c \neq 0$, czyli $c\tau + d \in \mathbb{Q}(i) \setminus \mathbb{Q}$. Ale $h = 3$, więc (**[DS, Corollary 2.3.5.]**) $\tau\,\mathrm{Sl}_2(\mathbb{Z}) = \mu_3\,\mathrm{Sl}_2(\mathbb{Z})$, w szczególności $\tau \in \mathbb{Q}(\mu_3)$. Wystarczy zauważyć, że $\mathbb{Q}(\mu_3) \cap \mathbb{Q}(i) = \mathbb{Q}$. Stąd musi być $f'(\tau) = f(\tau) = 0$, więc $v_\tau(f) \geqslant 2$.

dostajemy:

$$v_0(g_i) = \frac{1 + v_\tau(f)}{h} \geqslant \frac{1 + (h-1)}{h} = 1$$

oraz $v_0(\omega_i) = v_0(\frac{g_j(q)}{hq}) = v_0(g_i) - 1 \geqslant 0$.

3.5.3

★ **Równość** $M_n(\mathrm{Sl}_2(\mathbb{Z})) = S_n(\mathrm{Sl}_2(\mathbb{Z})) \oplus \mathbb{C}E_n$**:**

Oczywiście $S_n(\mathrm{Sl}_2(\mathbb{Z})) \cap \mathbb{C}E_n = \{0\}$ (jeżeli $\alpha E_n \in S_n(\mathrm{Sl}_2(\mathbb{Z}))$, to porównując zerowe wsp. Fouriera: $\alpha = 0$). Ponadto: $f(z) = \sum_n a_n q^n \in M_k(\mathrm{Sl}_2(\mathbb{Z}))$ (gdzie $q = \exp(2\pi i z)) \Rightarrow \quad f - a_0 E_k \in S_n(\mathrm{Sl}_2(\mathbb{Z}))$.

★ **Równość** $S_n(\mathrm{Sl}_2(\mathbb{Z})) = \Delta M_{n-12}(\mathrm{Sl}_2(\mathbb{Z}))$**:**

Oczywiście $S_n(\mathrm{Sl}_2(\mathbb{Z})) \supset \Delta M_{n-12}(\mathrm{Sl}_2(\mathbb{Z}))$. Jeżeli zaś $f \in S_n(\mathrm{Sl}_2(\mathbb{Z}))$, to (ponieważ Δ ma zero tylko w $i\infty$, oraz f ma tam zero) f/Δ jest holomorficzną formą automorficzną wagi $n - 12$, czyli formą modularną.

★ $M(\mathrm{Sl}_2(\mathbb{Z})) = \mathbb{C}(E_4, E_6)$ – **sposób I:** Zauważmy najpierw, że E_4 oraz E_6 są algebraicznie niezależne nad $\mathbb{C}$.

Lemat x, y są algebraicznie niezależne nad ciałem K wtw. gdy x^n, y^m są algebraicznie niezależne nad K dla pewnych m, n.
Dowód: Bez straty ogólności $n = 1$ (wystarczy zamienić zmienne). x, y^m są alg. zależne nad K $\Rightarrow$ $[K(x, y^m) : K(x)] < \infty \Rightarrow$ $[K(x, y) : K(x)] = [K(x, y) : K(x, y^m)] \cdot [K(x, y^m) : K(x)] \leqslant m \cdot [K(x, y^m) : K(x)] < \infty \Rightarrow$ x, y są alg. zależne nad K. Implikacja odwrotna – oczywista.

Wystarczy więc wykazać, że $A = E_4^3$, $B = E_6^2$ są algebraicznie niezależne nad $\mathbb{C}$. Załóżmy nie wprost, że $p(A, B) = 0$, $p(X, Y) = \sum_d p_d(X, Y) \in \mathbb{C}[X, Y]$ (p_d – części jednorodne). Wtedy, porównując wagi stwierdzamy, że $\forall_d\, p_d(A, B) = 0$. Niech $p_d(X, Y) \not\equiv 0$, $p_d(X, Y) = \prod_{i=1}^{d}(X - \alpha_i Y)$ dla $\alpha_i \in \mathbb{C}$. Wtedy $\forall_{z \in \mathbb{C}} p_d(A(z), B(z)) = 0 \Rightarrow$ $\exists_j$ $A(z) = \alpha_j B(z)$. Ale E_4, E_6 mają 1 za zerowy współczynnik Fouriera, więc $\alpha_j = 1$, $E_4(z)^2 = E_6(z)^3$. To jest jednak niemożliwe (wystarczy np. porównać współczynniki Fouriera przy q).

Stąd $M_{2n}(\mathrm{Sl}_2(\mathbb{Z}))$ ma podprzestrzeń $\bigoplus_{4a+6b=2n} \langle E_4^a E_6^b \rangle$, wymiaru $d_{2n} := \#\{(a, b) \in \mathbb{Z}_{\geqslant 0} : 4a{+}6b\}$. Wiemy, że $\dim M_{2n}(\mathrm{Sl}_2(\mathbb{Z})) = \begin{matrix} \lfloor 2n/12 \rfloor - 1, & 2n \equiv 2 \ (\mathrm{mod}\ 1)2 \\ \lfloor 2n/12 \rfloor, & 2n \not\equiv 2 \ (\mathrm{mod}\ 1)2 \end{matrix}$ Stąd $\dim M_{2n}(\mathrm{Sl}_2(\mathbb{Z})) = \dim M_{2n-12}(\mathrm{Sl}_2(\mathbb{Z}))$. Wystarczy wykazać, że (d_n) spełnia tą samą rekurencję – warunki początkowe są oczywiste, zaś ponieważ każde rozwiązanie $4a + 6b = 2n$ spełniające $b \geqslant 2$ odpowiada rozwiązaniu $4a + 6(b - 2) = 2n - 12$ oraz dokł. 1 z równań $4a = 2n$, $4a + 6 = 2n$ ma rozwiązanie, to $d_{2n} = d_{2n-12} + 1$. Stąd: $M_{2n}(\mathrm{Sl}_2(\mathbb{Z})) = \bigoplus_{4a+6b=2n} \langle E_4^a E_6^b \rangle$.

★ $M(\mathrm{Sl}_2(\mathbb{Z})) = \mathbb{C}(E_4, E_6)$ – **sposób II:** Wykażemy to indukcyjnie. Dla pierwszych wartości mamy (zauważmy, że znamy wymiary tych przestrzeni):

$M_0(\mathrm{Sl}_2(\mathbb{Z})) = \mathbb{C}, M_2(\mathrm{Sl}_2(\mathbb{Z})) = 0, M_4(\mathrm{Sl}_2(\mathbb{Z})) = \langle E_4 \rangle, M_6(\mathrm{Sl}_2(\mathbb{Z})) = \langle E_6 \rangle, M_10(\mathrm{Sl}_2(\mathbb{Z})) = \langle E_4 E_6 \rangle, M_{12}(\mathrm{Sl}_2(\mathbb{Z})) = \langle E$

Załóżmy, że teza jest prawdziwa dla liczb mniejszych od n. Niech $4a + 6b = 2n$ (takie liczby $a, b \in \mathbb{N}$ zawsze istnieją). Wtedy $M_n(\mathrm{Sl}_2(\mathbb{Z})) = \langle E_4^a E_6^b \rangle \oplus S_n(\mathrm{Sl}_2(\mathbb{Z}))$ (jeżeli $f(z) = \sum_n a_n q^n \in M_n(\mathrm{Sl}_2(\mathbb{Z}))$, to $f - a_0 E_4^a E_6^b \in S_n(\mathrm{Sl}_2(\mathbb{Z}))$). Ponadto $S_n(\mathrm{Sl}_2(\mathbb{Z})) = \Delta \cdot M_{n-12}(\mathrm{Sl}_2(\mathbb{Z})) = (\text{zał. ind.}) = \Delta \cdot (\mathbb{C}[E_4, E_6] \cap M_{n-12}(\mathrm{Sl}_2(\mathbb{Z})))$ i wystarczy zauważyć, że Δ jest (z definicji) kombinacją E_4 oraz E_6.

3.5.4 (a) oczywiście $\mathcal{S}_2(\Gamma_0(p)) \cap \mathbb{C}G_{2,p} = \{0\}$ oraz $\mathcal{S}_2(\Gamma_0(p)) \oplus \mathbb{C}G_{2,p} \subset M_2(\Gamma_0(p))$. Równość wynika z równości wymiarów, które obliczamy ze wzorów ze str. 88:

$$\dim M_2(\Gamma_0(p)) - \dim \mathcal{S}_2(\Gamma_0(p)) = ((g - 1) + \varepsilon_\infty) - g = \varepsilon_\infty - 1 = 1$$

(b)

(c)

3.7.1 (a) jeżeli $\gamma \in \mathrm{Sl}_2(\mathbb{Z})$ generuje nietrywialną grupę izotropii, to jest $\mathrm{Sl}_2(\mathbb{Z})$-sprzężona z jedną z macierzy $\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}^{\pm 1}$, $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^{\pm 1}$, $\begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}^{\pm 1}$ – wystarczy więc pokazać, że te macierze nie są $\mathrm{Gl}_2^+(\mathbb{Q})$-sprzężone ze swoimi odwrotnościami. Załóżmy, że $\alpha\gamma\alpha^{-1} = \gamma^{-1}$ dla $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $\gamma \in \left\{ \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \right\}$.

Wtedy dla $\gamma = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ mamy:

$$\begin{bmatrix} -b & a - b \\ -d & c - d \end{bmatrix} = \alpha\gamma = \gamma^{-1}\alpha = \begin{bmatrix} -a - c & -b - d \\ a & b \end{bmatrix}$$

co daje $a = -d$, $b = a + c$ i w rezultacie $\alpha = \begin{bmatrix} a & a + c \\ c & -a \end{bmatrix}$, $\det \alpha = -a^2 - ac - c^2 < 0$

Analogicznie w pozostałych przypadkach dostajemy: $\det \alpha < 0$, co daje sprzeczność.

3.7.6 (a)

(b) oznaczmy: $\gamma_n = \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix}^{-1} = \begin{bmatrix} n & -1 \\ n^2 - n + 1 & 1 - n \end{bmatrix}$ dla $n^2 - n + 1 \equiv 0 \pmod N$. Wystarczy wykazać, że ideały $J_{\gamma_n} := Ann(L_{\gamma_n}/L_0(N))$ (odpowiadające punktom eliptycznym $\Gamma_0(N) \begin{bmatrix} 1 & 0 \\ n & 1 \end{bmatrix} \mu_6$) są różne dla różnych n. Zauważmy, że

$$J_{\gamma_n} = \{a + b\mu_6 \in \mathbb{Z}[\mu_6] : (a + b\gamma_n)[x, y]^T \in L_0(N)\} =$$

$$= \{a + b\mu_6 \in \mathbb{Z}[\mu_6] : (a + b\gamma_n)[1, 0]^T \equiv [*, 0]^T \pmod N, (a + b\gamma_n)[0, 1]^T \equiv [*, 0]^T \pmod N\} =$$

$$= \{a+b\mu_6 \in \mathbb{Z}[\mu_6] : [a+bn, b(n^2-n+1)]^T \equiv [*, 0]^T \pmod N, [0, a+b(1-n)]^T \equiv [*, 0]^T \pmod N\} =$$

(bo $N|n^2 - n + 1$)

$$= \{a + b\mu_6 \in \mathbb{Z}[\mu_6] : a + b(1 - n) \equiv 0 \pmod N\} =$$

$$\{a + b\mu_6 \in \mathbb{Z}[\mu_6] : a \equiv bn^2 \pmod N\} = \{(bn^2 + cN) + b\mu_6 \in \mathbb{Z}[\mu_6] : b, c \in \mathbb{Z}\} =$$

$$= (n^2 + \mu_6)\mathbb{Z} + N\mathbb{Z}$$

Załóżmy, że $J_{\gamma_n} = J_{\gamma_m}$ – wtedy w szczególności $m^2 + \mu_6 \in (n^2 + \mu_6)\mathbb{Z} + N\mathbb{Z}$, czyli $m^2 + \mu_6 = A(n^2 + \mu_6) + BN$ dla $A, B \in \mathbb{Z}$. Porównując współczynniki przy μ_6 dostajemy: $A = 1$, więc $m^2 = n^2 + BN$ oraz $m \equiv m^2 + 1 \equiv n^2 + 1 \equiv n \pmod N$ oraz $m = n$.

(c)

3.7.7 Chcemy pokazać, że zbiór reprezentantów warstw dla $\Gamma_0(M)/\Gamma_0(p^eM)$ to $\{\alpha_1, \ldots, \beta_1, \ldots\}$. Niech $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(M)$, gdzie $c = MC$. Zauważmy, że $ad - bc = 1$, więc p dzieli co najwyżej jedną z liczb c, d. Ponadto:

$$\gamma\alpha_j^{-1} = \begin{bmatrix} * & * \\ M(C - dj) & * \end{bmatrix}, \qquad \gamma\beta_j^{-1} = \begin{bmatrix} * & * \\ M(Cm_jp - d) & * \end{bmatrix}$$

Rozważmy 2 przypadki:

1^o $p \nmid d$:

Z powyższych wzorów mamy wtedy: $p \nmid Cm_jp - d$, więc $\gamma\beta_j^{-1} \notin \Gamma_0(p^eM)$, a ponadto $\gamma\alpha_j^{-1} \in \Gamma_0(p^eM)$ tylko i wyłącznie dla $j \equiv d^{-1}C \pmod{p^e}$.

2^o $p|d$, $d = pD$:

Z powyższych wzorów mamy wtedy: $p \nmid C - dj$ (bo $p \nmid c = MC$), więc $\gamma\alpha_j^{-1} \notin \Gamma_0(p^eM)$. Ponadto $Cm_jp - d \equiv 0 \pmod{p^e}$ wtw. gdy $C(m+jM) \equiv D \pmod{p^{e-1}}$, czyli wtw. gdy $j \equiv (CM)^{-1}(D - Cm) \pmod{p^{e-1}}$.

Reszta zadania wynika z teorii grup: jeżeli $A/B = \{[a_i] : i = 1, \ldots\}$, $B/C = \{[b_j] : j = 1, \ldots\}$, to $A/C = \{[a_ib_j] : i, j = 1, \ldots\}$.

Rozdział IV

Podrozdział 4.2

4.2.2 Jeżeli γ_1, γ_2 są reprezentantami tej samej warstwy $\Gamma(N) \setminus \Gamma$, to $\gamma_1 = \gamma\gamma_2$ dla pewnego $\gamma \in \Gamma(N)$, więc $E_k^{\overline{v}}[\gamma_1]_k = (E_k^{\overline{v}}[\gamma]_k)[\gamma_2]_k = E_k^{\overline{v}}[\gamma_2]_k$ (skorzystaliśmy z modlarności $E_k^{\overline{v}}$ wg $\Gamma(N)$). Stąd $E_{k,\Gamma}^{\overline{v}}$ nie zależy od wyboru reprezentantów.

Ponadto jeżeli $\Gamma(N)\setminus\Gamma=\{[\gamma_1],\dots,[\gamma_m]\}$ oraz $\gamma\in\Gamma$, to:

$$E^{\overline{v}}_{k,\Gamma}[\gamma]_k=\sum_j(E^{\overline{v}}_k[\gamma_j]_k)[\gamma]_k=\sum_j E^{\overline{v}}_k[\gamma_j\gamma]_k=\sum_j E^{\overline{v}}_k[\gamma_j]_k$$

($[\gamma_j]\mapsto[\gamma_j\gamma]$ jest bijekcją w $\Gamma(N)\setminus\Gamma$), co dowodzi słabej modularności. Holomorficzność na $\mathcal{H}$ oraz w cuspach wynika z tego, że wszystkie składniki je spełniają.

4.2.4

(a) jeżeli $n=\prod_{i\in J}p_i^{a_i}>1$ to:

$$\sum_{d|n}\mu(d)=\text{(zapominając o składnikach podzielnych przez kwadrat)}=\sum_{A\subset J}\mu(\prod_{i\in A}p_i^{a_i})=$$

$$=\sum_{A\subset J}(-1)^{|A|}=\sum_{k=1}^{|A|}\binom{|A|}{k}(-1)^k=(1-1)^{|A|}=0$$

(b)

$$E^{\overline{v}}_k(\tau)=\varepsilon_N\sum_{\substack{(c,d)\equiv v \pmod N,\\ NWD(c,d)=1}}(c\tau+d)^{-k}=\varepsilon_N\sum_{(c,d)\equiv v \pmod N}(c\tau+d)^{-k}\sum_{n|NWD(c,d)}\mu(n)=$$

$$=\varepsilon_N\sum_{(c,d)\equiv v \pmod N}\sum_{n|NWD(c,d)}\mu(n)(c\tau+d)^{-k}=$$

Zamieniamy kolejność sumowania oraz sumując najpierw po n (dla $k\geqslant 3$ szereg jest bezwzględnie zbieżny); korzystamy z tego, że $NWD(c,d,N)=1$ (bo $(c,d)\equiv v \pmod N$)

$$=\varepsilon_N\sum_{NWD(n,N)=1}\left(\mu(n)\sum_{\substack{n|c,d\\(c,d)\equiv v \pmod N}}(c\tau+d)^{-k}\right)=$$

(podstawiamy $c=nC$, $d=nD$)

$$\varepsilon_N\sum_{NWD(n,N)=1}\left(\mu(n)\sum_{(C,D)\equiv n^{-1}v \pmod N}n^{-k}(C\tau+D)^{-k}\right)=\varepsilon_N\sum_{NWD(n,N)=1}\frac{\mu(n)}{n^k}G_k^{n^{-1}v}(\tau)=$$

(grupując wyrazy wg reszty modulo N)

$$=\varepsilon_N\sum_{n\in(\mathbb{Z}/N)^*}\left(\sum_{m\equiv n \pmod N}\frac{\mu(m)}{m^k}\right)\cdot G_k^{n^{-1}v}(\tau)=\varepsilon_N\sum_{n\in(\mathbb{Z}/N)^*}\zeta_+^n(k)G_k^{n^{-1}v}(\tau)$$

Podrozdział 4.3

4.3.2 (a) oczywiste

(b)

$$\sum_{n=0}^{N-1}\chi(n)\mu_N^{nm}=\sum_{n\in\mathbb{Z}/N}\chi(n)\mu_{N'}^{nm'h}=$$

(jako że $NWD(m',N)=1$, to mnożenie przez m' jest bijekcją na $\mathbb{Z}/N$ – możemy więc sumować po nm')

$$=\sum_{n\in\mathbb{Z}/N}\chi(m'^{-1}n)\mu_{N'}^{nh}=\overline{\chi(m')}\sum_{n\in\mathbb{Z}/N}\chi(n)\mu_{N'}^{nh}=$$

(grupując n wg przystawania modulo N')

$$=\overline{\chi(m')}\sum_{n'=0}^{N'-1}\left(\sum_{\substack{n=0\\ n\equiv n' \pmod{N'}}}^{N-1}\chi(n)\mu_{N'}^{nh}\right)=\overline{\chi(m')}\sum_{n'=0}^{N'-1}\left(\sum_{\substack{n=0\\ n\equiv n' \pmod{N'}}}^{N-1}\chi(n)\right)\mu_{N'}^{n'h}$$

Załóżmy, że $N' < N$ (tzn. $g > 1$). Z prymitywności χ wynika istnienie $a_1, a_2 \in (\mathbb{Z}/N)^*$ takich, że $a_1 \equiv a_2 \pmod{N'}$ oraz $\chi(a_1) \neq \chi(a_2)$ – wtedy biorąc $a \equiv a_1^{-1}a_2 \pmod{N}$ dostajemy: $a \in K$, $\chi(a) \neq 1$. Ale $aK = K$, więc: $\chi(a)\sum_{n\in K}\chi(n) = \sum_{n\in K}\chi(an) = \sum_{n\in aK}\chi(n) = \sum_{n\in K}\chi(n)$, więc $\sum_{n\in K}\chi(n) = 0$.

Dla $g = 1$ mamy: $K = 1$, więc $\sum_{n\in K}\chi(n) = 1$.

Mamy:

$$\sum_{\substack{n=0 \\ n\equiv n' \pmod{N'}}}^{N-1} \chi(n) = \sum_{n\in n'K}\chi(n) = \chi(n')\sum_{n\in K}\chi(n) = \begin{cases} \chi(n), & g=1 \\ 0, & g>1 \end{cases}$$

Jeżeli $g > 1$, to $\chi(m) = 0$ oraz (z powyższej linijki) $\sum_{\substack{n=0 \\ n\equiv n' \pmod{N'}}}^{N-1} \chi(n)\mu_{N'}^{n'h} = 0$, więc obie strony są równe.

Jeżeli $g = 1$, to $m = m'$, $h = 1$, $N = N'$ oraz:

$$\sum_{n=0}^{N-1}\chi(n)\mu_N^{nm} = \overline{\chi(m')}\sum_{n'=0}^{N-1}\left(\sum_{\substack{n=0 \\ n\equiv n' \pmod{N}}}^{N-1}\chi(n)\right)\mu_N^{n'} = \overline{\chi(m')}\sum_{n'=0}^{N-1}\chi(n')\mu_N^{n'} = \overline{\chi}(m)g(\chi)$$

4.3.3

(a) jeżeli $\gamma \in \Gamma_0(N)$, to $NWD(d_\gamma, N) = 1$ (bo $N|c_\gamma \Rightarrow \quad a_\gamma d_\gamma \equiv b_\gamma c_\gamma + 1 \equiv 1 \pmod{N}$), więc $1_N(d_\gamma) = 1$. Stąd: $f \in \mathcal{M}_k(\Gamma_0(N))$ wtw. gdy $f[\gamma]_k = f = \chi(d_\gamma)f$ dla każdego $\gamma \in \Gamma_0(N)$.

(b) jeżeli $f \neq 0$, $f \in \mathcal{M}_k(N, \chi)$, to $(-1)^k f = f\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}_k = \chi(-1)f$, więc $\chi(-1) = (-1)^k$.

4.3.4 Oznaczmy: $m = \phi(N)$. Niech $\widehat{(\mathbb{Z}/N)}^* = \{\chi_1, \ldots, \chi_m\}$, zaś $\{\gamma_1, \ldots, \gamma_m\}$ będą reprezentantami warstw $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N)^*$, $\gamma_i = \begin{bmatrix} * & * \\ * & d_i \end{bmatrix}$ – wtedy $\{d_1, \ldots, d_m\} = (\mathbb{Z}/N)^*$.
Niech $f \in \Gamma_1(N)$ – szukamy funkcji $f_1, \ldots, f_m$ spełniających równania:

$$f[\gamma]_k = \sum_{i=1}^{m}\chi_i(d_\gamma)f_i$$

– zauważmy, że aby były one spełnione dla dowolnego $\gamma \in \Gamma_0(N)$ potrzeba i wystarczy, by były spełnione dla $\gamma_1, \ldots, \gamma_m$ (bo $\gamma\gamma_i^{-1} \in \Gamma_1(N)$ dla pewnego i, więc $f[\gamma]_k = f[\gamma_i]_k$). Dostajemy więc układ m równań z m niewiadomymi:

$$f[\gamma_j]_k = \sum_{i=1}^{m}\chi_i(d_j)f_i, \qquad \text{dla } j = 1, \ldots, m$$

– w postaci macierzowej:

$$\begin{bmatrix} f[\gamma_1]_k \\ \cdots \\ f[\gamma_m]_k \end{bmatrix} = [\chi_j(d_i)]_{i,j}\begin{bmatrix} f_1 \\ \cdots \\ f_m \end{bmatrix}$$

Relacje ortogonalności można jednak zapisać w postaci: $[\chi_j(d_i)]_{i,j}\,[\chi_j(d_i)]_{i,j}^* = mI$, czyli $[\chi_j(d_i)]_{i,j}^{-1} = \frac{1}{m}[\overline{\chi_i}(d_j)]_{i,j}$ co oznacza, że powyższy układ ma dokł. 1 rozwiązanie dane wzorem:

$$\begin{bmatrix} f_1 \\ \cdots \\ f_m \end{bmatrix} = [\frac{1}{m}\overline{\chi_i}(d_j)]_{i,j}\begin{bmatrix} f[\gamma_1]_k \\ \cdots \\ f[\gamma_m]_k \end{bmatrix}$$

czyli $f_i = \sum_{j=1}^{m}\frac{1}{m}\chi_i(d_j)f[\gamma_j]_k$.

Pozostaje wykazać, że $f_i \in \mathcal{M}_k(N, \chi_i)$. Ustalmy $d_l \in (\mathbb{Z}/N)^*$. Mnożenie przez d_l jest bijekcją na $(\mathbb{Z}/N)^* \cong \Gamma_0(N)/\Gamma_1(N)$; niech $d_i d_l \equiv d_{\sigma(i)} \pmod N$ dla pewnej permutacji σ (wtedy $\gamma_i\gamma_l \equiv \gamma_{\sigma(i)} \pmod{\Gamma_1(N)}$). Niech E_σ będzie macierzą permutacji σ (tzn. E_σ ma jedynki na miejscach $(i, \sigma(i))$ oraz zera na posostałych miejscach).

$$\begin{bmatrix} f_1[\gamma_l]_k \\ \dots \\ f_m[\gamma_l]_k \end{bmatrix} = [\frac{1}{m}\overline{\chi_i}(d_j)]_{i,j} \begin{bmatrix} f[\gamma_1]_k[\gamma_l]_k \\ \dots \\ f[\gamma_m]_k[\gamma_l]_k \end{bmatrix} = [\frac{1}{m}\overline{\chi_i}(d_j)]_{i,j} \begin{bmatrix} f[\gamma_1\gamma_l]_k \\ \dots \\ f[\gamma_m\gamma_l]_k \end{bmatrix} = [\frac{1}{m}\overline{\chi_i}(d_j)]_{i,j} \begin{bmatrix} f[\gamma_{\sigma(1)}]_k \\ \dots \\ f[\gamma_{\sigma(m)}]_k \end{bmatrix} =$$

$$= [\frac{1}{m}\overline{\chi_i}(d_j)]_{i,j} \cdot E_\sigma \cdot \begin{bmatrix} f[\gamma_1]_k \\ \dots \\ f[\gamma_m]_k \end{bmatrix} = [\frac{1}{m}\overline{\chi_i}(d_{\sigma(j)})]_{i,j} \cdot \begin{bmatrix} f[\gamma_1]_k \\ \dots \\ f[\gamma_m d]_k \end{bmatrix} =$$

$$= [\frac{1}{m}\overline{\chi_i}(d_l d_j)]_{i,j} \cdot \begin{bmatrix} f[\gamma_1]_k \\ \dots \\ f[\gamma_m]_k \end{bmatrix} = diag(\chi_1(d_l), \dots, \chi_m(d_l)) \cdot [\frac{1}{m}\overline{\chi_i}(d_j)]_{i,j} \cdot \begin{bmatrix} f[\gamma_1]_k \\ \dots \\ f[\gamma_m]_k \end{bmatrix} =$$

$$= diag(\chi_1(d_l), \dots, \chi_m(d_l)) \cdot \begin{bmatrix} f_1 \\ \dots \\ f_m \end{bmatrix} = \begin{bmatrix} \chi_1(d_l) f_1 \\ \dots \\ \chi_m(d_l) f_m \end{bmatrix}$$

czyli $f_i[\gamma_l]_k = \chi_i(d_l) f_i$, co daje tezę.

Podrozdział 4.4

4.4.1 (a) $\Gamma(1) = \int_0^\infty e^{-t}\,dt = [-e^{-t}]_0^\infty = 0 - (-1) = 1$,

(b) $\Gamma(1/2) = \int_0^\infty e^{-t} t^{-1/2}\,dt =$ (podstawiając $s = \sqrt{t}$) $= 2\int_0^\infty e^{-s^2}\,ds = \int_\infty^\infty e^{-s^2}\,ds = \sqrt{\int_{x=\infty}^\infty \int_{y=\infty}^\infty e^{-x^2-y^2}\,dy\,dx} =$ (przechodząc na współrzędne biegunowe) $= \sqrt{\int_{\phi=0}^{2\pi}\int_{r=0}^\infty re^{-r^2}\,dr\,d\phi} = \sqrt{2\pi\int_{r=0}^\infty re^{-r^2}\,dr} = \sqrt{2\pi[-e^{-r^2}/2]_0^\infty} = \sqrt{\pi}$.

(c) całkując przez części:

$$\Gamma(s+1) = \int_0^\infty e^{-t}t^s\,dt = (u = t^s, dv = e^{-t}; du = st^{s-1}, v = -e^{-t}) = [-t^s e^{-t}]_0^\infty + s\int_0^\infty e^t t^{s-1}\,dt = 0 + s\Gamma(s)$$

(d) mamy: $(1 - t/n)^n t^{s-1}\chi_{[0,n]} \nearrow e^{-t}t^{s-1}$ (znany fakt), więc dla $s \in \mathbb{R}$ z tw. o zbieżności monotonicznej dla całki Riemanna mamy: $\lim_n I_n(s) = \Gamma(s)$ (dla $s \in \mathbb{C}$ można zastosować to tw. osobno do części rzeczywistej i zespolonej funkcji podcałkowej).

Podstawiając $t \mapsto t/n$, a następnie całkując przez części dostajemy:

$$I_n(s) = n^s\int_0^1 (1-t)^n t^{s-1}\,dt = (u = (1-t)^n, dv = t^{s-1}) = n^s[-n(1-t)^{n-1}\cdot t^s/s]_0^1 + \frac{n^s\cdot n}{s}\int_0^1 (1-t)^{n-1}t^s\,dt$$

$$= 0 + \frac{n^s \cdot n}{s\cdot(n-1)^{s+1}} I_{n-1}(s+1) = \frac{1}{s}(n/(n-1))^{s+1} I_{n-1}(s+1) =$$

$$= \frac{1}{s}(n/(n-1))^{s+1}\cdot\frac{1}{s+1}((n-1)/(n-2))^{s+2}\cdot I_{n-2}(s+2) = \ldots =$$

$$= \prod_{j=1}^{n-1}(\frac{j+1}{j})^{s+n-j}\frac{1}{s+n-j-1}\cdot I_1(s+n-1)$$

Ale $I_1(s+n-1) = \int_0^1 (1-t)t^{s+n-1} = \frac{1}{s+n} - \frac{1}{s+n+1}$, więc:

$$I_n(s) = \prod_{j=1}^{n-1}\left((\frac{j+1}{j})^{s+n-j}\frac{1}{s+n-j-1}\right)\cdot\frac{1}{(s+n)(s+n+1)} = n^s\cdot\frac{\prod_{j=1}^{n-1}(j+1)}{\prod_{j=1}^{n-1}(s+n-j-1)}\cdot\frac{1}{(s+n)(s+n+1)} =$$

$$= n^s \cdot \frac{\prod_{j=1}^{n-1}(j+1)}{\prod_{j=1}^{n-1}(s+j-1)} \cdot \frac{1}{(s+n)(s+n+1)} = \frac{n^s}{s\prod_{j=1}^{n}(1+s/j)}$$

Stąd:

$$I_n(s)I_n(-s) = \frac{1}{-s^2\prod_{j=1}^{n}(1+s/j)(1-s/j)} = \frac{1}{-s^2\prod_{j=1}^{n}(1-s^2/j^2)}$$

co po przejściu $n \to \infty$ daje: $\Gamma(s)\Gamma(-s) = -\frac{\pi}{s\sin(\pi s)}$, więc:

$$\Gamma(s)\Gamma(1-s) = -s\Gamma(s)\Gamma(-s) = \frac{\pi}{\sin(\pi s)}$$

4.4.3 (a) wystarczy zauważyć, że $(t\,\frac{d}{dt})^{(n)}(t^k) = (t\,\frac{d}{dt})^{(n-1)}(kt^k) = \ldots = k^n t^k$; reszta jest oczywista.

(b) mamy: $(f(e^X))' = e^X f'(e^X)$, więc $t\,\frac{d}{dt} = \frac{d}{dX}$.

Proste obliczenia dają:

$$\frac{1}{\pi i}\left(G(z) - 2G(2z)\right) = \frac{1}{\pi i}\left(\pi i\frac{e^{2\pi iz}+1}{e^{2\pi iz}-1} - 2\pi i\frac{e^{4\pi iz}+1}{e^{4\pi iz}-1}\right) =$$

$$= \frac{1-e^{2\pi iz}}{1+e^{2\pi iz}} = -\frac{e^{2\pi iz}}{e^{2\pi iz}+1} + \frac{e^{-2\pi iz}}{e^{-2\pi iz}+1} = -F(z) + F(-z)$$

więc porównując szeregi Taylora:

$$\frac{1}{\pi i}\left(G(z) - 2G(2z)\right) = \sum_{n=1}^{\infty}\frac{2(2^{2n}-1)\zeta(2n)}{i\pi}z^{2n-1} = \sum_{n=1}^{\infty}\frac{2(2^{2n}-1)\zeta(1-2n)(2\pi i)^{2n-1}}{(2n-1)!}z^{2n-1} = -F(z)+F(-z)$$

co daje: $\frac{2(2^{2n}-1)\zeta(2n)}{i\pi} = \frac{2(2^{2n}-1)\zeta(1-2n)(2\pi i)^{2n-1}}{(2n-1)!}$, czyli tezę ($\Gamma(2n) = (2n-1)!$).

(c)

$$\pi^{-k/2}\Gamma(k/2)\zeta(k) \overset{(b)}{=} \underbrace{\frac{(2\pi i)^k}{2\Gamma(k)}}_{=C_k/2}\zeta(1-k) \overset{(4.16)}{=} \pi^{-(1-k)/2}\Gamma((1-k)/2)\zeta(1-k)$$

4.4.5 (a) $(-r)^s = e^{s\ln r + is\pi} = e^{s\ln r}e^{is\pi} = (-1)^s r^s$

(b) dla $\Re s > 1$ z podpunktu (a) mamy:

$$\sum_{m\equiv n \pmod N} m^{-s} = \sum_{\substack{m\equiv n \pmod N,\\ m>0}} m^{-s} + \sum_{\substack{m\equiv n \pmod N,\\ m<0}} m^{-s} = \sum_{\substack{m\equiv n \pmod N,\\ m>0}} m^{-s} + (-1)^s \sum_{\substack{m\equiv -n \pmod N,\\ m>0}} m^{-s}$$

(obie strony są zbieżne, więc grupowanie/rozgrupowywanie wyrazów jest dozwolone)

(c) pierwszy wzór wynika ze wzoru $\zeta_+^n(s) = \frac{1}{\phi(N)}\sum_\chi \chi(n^{-1})L(s,\chi)$ ze str. 122. Granica wynika z zadania 4.4.4 oraz znanej granicy: $\lim_{s\to 1}(s-1)\zeta(s) = 1$:

$$\lim_{s\to 1}\frac{1}{\phi(N)}(1+(-1)^{-s})L(s,1_N) = \lim_{s\to 1}\frac{1}{\phi(N)}(1+(-1)^{-s})\prod_{p|N}(1-p^{-s})\zeta(s) =$$

$$= \lim_{s\to 1}\frac{1+(-1)^{-s}}{s-1}\cdot((s-1)\zeta(s))\cdot\frac{\prod_{p|N}(1-p^{-s})}{N\prod_{p|n}(1-\frac{1}{p})} =$$

$$= \lim_{s\to 1}\frac{1+(-1)^{-s}}{s-1}\cdot\frac{1}{N} = \lim_{s\to 1}\frac{1+e^{-i\pi s}}{s-1}\cdot\frac{1}{N} =$$

$$= \lim_{s\to 1}\frac{1+e^{-i\pi s}}{s-1}\cdot\frac{1}{N} = \lim_{s\to 1} -\frac{e^{-i\pi(s-1)}-1}{s-1}\cdot\frac{1}{N} = \lim_{s\to 1} -\left(-i\pi + \frac{(-i\pi)^2}{2!}(s-1) + \frac{(-i\pi)^3}{3!}(s-1)^2 + \ldots\right)\cdot\frac{1}{N} = \frac{i\pi}{N}$$

(d) pierwsza równość wynika z (c). Dowód drugiej równości – mamy:

$$\sum_{\chi\neq 1_N}\chi(n^{-1})L(1,\chi) = \sum_{\chi\neq 1_N}\chi(n^{-1})\sum_{l=1}^{\infty}\frac{\chi(l)}{l} = \sum_{l=1}^{\infty}\sum_{\chi\neq 1_N}\frac{\chi(n^{-1}l)}{l} = \sum_{k\geqslant 0}\sum_{m\in(\mathbb{Z}/N)^*}\frac{1}{Nk+m}\sum_{\chi\neq 1_N}\chi(n^{-1}l) =$$

(pogrupowaliśmy wyrazy – w każdej grupie jest po $\phi(N)$; jest to dozwolone, o ile obie strony są zbieżne), a ponadto

$$\sum_{\chi\neq 1_N}\chi(n^{-1}l)=\begin{cases}\phi(N)-1, & l\equiv n \pmod N\\ -1, & l\not\equiv n \pmod N\end{cases}$$

więc:

$$=\sum_{k\geqslant 0}\left(\frac{\phi(N)}{Nk+n}-\sum_{m\in(\mathbb{Z}/N)^*}\frac{1}{Nk+m}\right)$$

i analogicznie:

$$\sum_{\chi\neq 1_N}\chi((-n)^{-1})L(1,\chi)=\sum_{\chi\neq 1_N}\chi((N-n)^{-1})L(1,\chi)=\sum_{k\geqslant 0}\left(\frac{\phi(N)}{Nk+N-n}-\sum_{m\in(\mathbb{Z}/N)^*}\frac{1}{Nk+m}\right)$$

co daje:

$$\zeta^n(1)=\frac{\pi i}{N}+\frac{1}{\phi(N)}\sum_{\chi\neq 1_N}\chi(n^{-1})L(1,\chi)-\frac{1}{\phi(N)}\sum_{\chi\neq 1_N}\chi((-n)^{-1})L(1,\chi)=\frac{\pi i}{N}+\sum_{k\geqslant 0}\left(\frac{1}{Nk+n}-\frac{1}{Nk+N-n}\right)=$$

$$\overset{(*)}{=}\frac{\pi i}{N}+\frac{1}{N}\left(\frac{1}{n/N}+\sum_{k\geqslant 1}\left(\frac{1}{k+n/N}+\frac{1}{k-n/N}\right)\right)=\frac{\pi i}{N}+\frac{\pi}{N}\cot(\pi n/N)$$

(uzasadnienie (*) – jeżeli $a_i\to 0$, oraz szeregi $\sum_{i\geqslant 0}(a_{2i}+a_{2i+1})$, $a_0+\sum_{i\geqslant 0}(a_{2i+1}+a_{2i+2})$ są zbieżne, to są równe, bo ich sumy częściowe różnią się o elementy dążące do zera).

4.4.6

$$\Gamma(a)\Gamma(b)=2\int_{t=0}^{\infty}e^{-t^2}t^{2a}\frac{dt}{t}\cdot 2\int_{u=0}^{\infty}e^{-u^2}u^{2b}\frac{du}{u}=4\int_{\mathbb{R}^2_+}e^{-t^2-u^2}t^{2a-1}u^{2b-1}dt\,du=$$

(przechodząc na współrzędne biegunowe)

$$=4\int_{r=0}^{\infty}\int_{\phi=0}^{\pi/2}re^{-r^2}(r\cos\phi)^{2a-1}(r\sin\phi)^{2b-1}\,dr\,d\phi=4\int_{r=0}^{\infty}e^{-r^2}r^{2(a+b)-1}\,dr\cdot\int_{\phi=0}^{\pi/2}(\cos\phi)^{2a-1}(\sin\phi)^{2b-1}\,d\phi=$$

$$=2\Gamma(a+b)\int_{\phi=0}^{\pi/2}(\cos\phi)^{2a-1}(\sin\phi)^{2b-1}\,d\phi=(x=\cos^2\phi)=\Gamma(a+b)\int_0^1 x^{a-1}(1-x)^{b-1}\,dx$$

Ostatnia w zadaniu równość wynika z podstawienia $x=1-t^m$.

Podrozdział 4.7

4.7.4

$$g_r(s)=\int_0^{\infty}\sum_{n=0}^{\infty}e^{-(r+n)t}t^{s-1}\,dt=\sum_{n=0}^{\infty}\int_0^{\infty}e^{-(r+n)t}t^{s-1}\,dt=\ \text{(podstawienie } u=(r+n)t)=$$

$$=\sum_{n=0}^{\infty}\frac{1}{(n+r)^s}\int_0^{\infty}e^{-u}u^{s-1}\,du=\sum_{n=0}^{\infty}\frac{1}{(n+r)^s}\Gamma(s)=\zeta(s,r)\Gamma(s)$$

4.7.5 (a) stosujemy twierdzenie o residuach – funkcja ta jest holomorficzna na dowolnym pierścieniu kołowym wokół zera tej postaci:

(b) przyjmując dla $t > 0$ w pierwszej całce: $(-t)^s = t^s e^{-i\pi s}$ oraz w drugiej całce: $(-t)^s = t^s e^{i\pi s}$, a następnie podstawiając $z = -t$ dostajemy:

$$\int_{[-\infty,-\varepsilon]\cup[-\varepsilon,-\infty]} \widetilde{f}_r(z)z^{s-1}\frac{dz}{z} = \int_{\varepsilon}^{\infty} \widetilde{f}_r(-t)t^{s-1}e^{-i\pi(s-1)}\frac{dt}{t} - \int_{\varepsilon}^{\infty} \widetilde{f}_r(-t)t^{s-1}e^{i\pi(s-1)}\frac{dt}{t} =$$

Korzystając z równości: $\widetilde{f}_r(-t) = tf_r(t)$:

$$= \int_{\varepsilon}^{\infty} f_r(t)t^s e^{-i\pi(s-1)}\frac{dt}{t} - \int_{\varepsilon}^{\infty} f_r(t)t^{s-1}e^{i\pi(s-1)}\frac{dt}{t} =$$

$$= g_r(s)\cdot(e^{-i\pi s} - e^{i\pi s}) \overset{\text{zad. 4.7.4}}{=} -2i\Gamma(s)\zeta(s,r)\sin(\pi s)$$

(c) funkcja $\widetilde{f}_r(z)$ ma usuwalną nieciągłość w zerze (licznik i mianownik mają pojedyncze zera), więc jest ciągła w 0, czyli ograniczona w pewnym otoczeniu 0: $|\widetilde{f}_r(z)| \leqslant c_1$. Ponadto: $|z^{s-2}| = \frac{|z|^{\Re(s-2)}}{e^{arg\,z\cdot\Im(s)}} \leqslant c_2 \cdot |z|^{\Re(s-2)}$. Stąd: $|\int_{C(0,\varepsilon)} \widetilde{f}_r(z)z^{s-2}\,dz| \leqslant |C(0,\varepsilon)|\cdot c_1c_2\cdot\varepsilon^{\Re(s-2)} = C\cdot\varepsilon^{\Re s-1}$ oraz $\lim_{\varepsilon\to 0}\int_{C(0,\varepsilon)} \widetilde{f}_r(z)z^{s-2}\,dz = 0$.

Podrozdział 4.8

4.8.3 Rozwijając w szereg geometryczny:

$$\eta_2(\tau) = (2\pi i)^2/12(-1+24\sum_m \frac{mq^m}{1-q^m}) = (2\pi i)^2/12\cdot(-1+24\sum_{m\geqslant 1}\sum_{k\geqslant 1} mq^{km}) =$$

$$= (2\pi i)^2/12\cdot(-1+24\sum_{n\geqslant 1} q^n\left(\sum_{d|n} d\right)) = \frac{\pi^2}{3} - 8\pi^2\sum_{n\geqslant 1}\sigma(n)q^n = G_2(\tau)$$

(skorzystałem ze wzoru na G_2 ze str. 18 oraz $\zeta(2) = \pi^2/6$; bezwzględna zbieżność pozwala na zmianę kolejności sumowania).

4.8.7

(a) podnosząc równanie (ze str. 12) $\theta(\frac{\tau}{4\tau+1}) = \sqrt{4\tau+1}\cdot\theta(\tau)$ stronami do potęgi s (gdzie $2|s$) dostajemy:

$$\theta(\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}, s) = \theta(\frac{\tau}{4\tau+1})^s = (4\tau+1)^{s/2}\cdot\theta(\tau)^s = \left(\theta(\cdot,s)[\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}]_{s/2}\right)(\tau)$$

więc (ponieważ θ jest 1 okresowa oraz z zadania 1.2.3 macierze $\pm\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ oraz $\pm\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}$ generują $\Gamma_1(4)$), $\theta(\begin{bmatrix} 1 & 0 \\ 4 & 1 \end{bmatrix}, s) \in \mathcal{M}_{s/2}(\Gamma_1(4))$.

(b) zauważmy, że dla $\Gamma_1(4)$ mamy (z zadania 3.8.7 oraz ostatniego wzoru na stronie 102): $\varepsilon_\infty^{irr} = 1$, $\varepsilon_\infty^{reg} = 2$, czyli $\varepsilon_\infty^{reg} > 2g-2 = -2$ (z tabeli 3.4. mamy: $g = genus(\Gamma_1(4)) = 0$), więc z twierdzenia 3.6.1 mamy: $\mathcal{S}_1(\Gamma_1(4)) = 0$, $\dim\mathcal{M}_1(\Gamma_1(4)) = \varepsilon_\infty^{reg}/2 = 1$.

Z tabeli 3.4 dostajemy ponadto: $\mathcal{S}_3(\Gamma_1(4)) = 0$, $\dim\mathcal{M}_3(\Gamma_1(4)) = \frac{3-1+2}{2} = 2$, $\mathcal{S}_4(\Gamma_1(4)) = 0$, $\dim\mathcal{M}_4(\Gamma_1(4)) = \frac{4-1+3}{2} = 3$.

(c)

Zauważmy, że mamy 2 charaktery modulo 4: $\mathbf{1}$ – trywialny (o przewodniku 1) oraz χ spełniający: $\chi(n) = (-1)^{(n-1)/2}$ dla $2\nmid n$, $\chi(2) = 0$ (o przewodniku 4). Stąd $\mathcal{M}_{s/2}(\Gamma_1(4)) = \mathcal{M}_{s/2}(4,\mathbf{1})\oplus\mathcal{M}_{s/2}(4,\mathbf{1})$. Ponadto (wg oznaczeń z 4.8): $A_{4,1} = \{(\{\chi,\mathbf{1}\},1)\}$, więc z twierdzenia 4.8.1: $\mathcal{M}_1(\Gamma_1(4)) = \langle E_1^{\chi,\mathbf{1},1}\rangle$. Stąd: $\theta(\tau,2) \in \mathcal{M}_1(\Gamma_1(4)) \Rightarrow\ \ \theta(\tau,2) = cE_1^{\chi,\mathbf{1},1} \Rightarrow$ porównując współczynniki w rozwinięciach Fouriera: $r(n,2) = C\cdot\sigma_0^{\chi,\mathbf{1}}(n) = C\cdot\sum_{d|n}\chi(d) = C\cdot\sum_{d|n,2\nmid d}(-1)^{(d-1)/2}$ (gdzie c, C są stałymi). Porównując strony np. dla $n = 2$ dostajemy $C = 4$.

Dla $s/2 = 3$ mamy: $\mathcal{M}_3(4, \mathbf{1}) = 0$ (ponieważ $\mathbf{1}(-1) \neq (-1)^3$) oraz $A_{4,3} = \{(\chi, \mathbf{1}, 1), (\mathbf{1}, \chi, 1)\}$, więc

$$\mathcal{M}_1(\Gamma_1(4)) = \langle E_1^{\chi,\mathbf{1},1} \rangle \oplus \langle E_1^{\mathbf{1},\chi,1} \rangle$$

co oznacza, że $r(n, 3) = C\sigma_2^{\chi,\mathbf{1}}(n)+D\sigma_2^{\mathbf{1},\chi}(n) = \sum_{d|n} d^2 \cdot (C\chi(n)+D\chi(n/d))$ dla pewnych C, D. Porównując strony np. dla $n = 2, 3$ dostajemy $(C, D) =?$.

Dla $s/2 = 4$ mamy: $\mathcal{M}_4(4, \chi) = 0$ (ponieważ $\chi 1(-1) \neq (-1)^4$) oraz $A_{4,4} = \{(\mathbf{1}, \mathbf{1}, 1), (\mathbf{1}, \mathbf{1}, 2), (\mathbf{1}, \mathbf{1}, 4)\}$, więc

$$\mathcal{M}_1(\Gamma_1(4)) = \langle E_1^{\mathbf{1},\mathbf{1},1} \rangle \oplus \langle E_1^{\mathbf{1},\mathbf{1},2} \rangle \oplus \langle E_1^{\mathbf{1},\mathbf{1},4} \rangle$$

co oznacza, że $r(n, 4) = c\sigma_3^{\mathbf{1},\mathbf{1}}(n) + d\sigma_3^{\mathbf{1},\mathbf{1}}(n/2) + e\sigma_3^{\mathbf{1},\mathbf{1}}(n/4)$ dla pewnych c, d, e. Porównując strony np. dla $n = 2, 3, 4$ dostajemy $(c, d, e) =?$.

Podrozdział 4.9

4.9.4

$$\widehat{f}(d) = \int_{y=0}^{\infty} y^{s-1} e^{2\pi i y\tau} e^{-2\pi i d\cdot y}\, dy = \int_{y=0}^{\infty} y^{s-1} e^{2\pi i y(\tau-d)}\, dy = \Big(\text{podstawienie } -2\pi i y(\tau-d) = z\Big) =$$

$$= (\tau - d)^{-s}(-2\pi i)^{-s} \quad \int_L e^{-z} z^{s-1}\, dz$$

gdzie L jest półprostą o początku w 0, przechodzącą przez $\tau - d$. Z twierdzenia o residuach: $\int_L e^{-z} z^{s-1}\, dz = \int_0^\infty e^{-y} y^{s-1}\, dy = \Gamma(s)$ (funkcja f jest holomorficzna na obszarze ograniczonym przez półproste L oraz $(0, \infty)$, oraz mały łuk C_ε wokół zera, więc całka po tym konturze jest równa 0. Ale $|\int_{C_\varepsilon} e^{-z} z^{s-1}| \leqslant C\varepsilon^{\Re(s)}$, co daje równość przy przejściu $\varepsilon \to 0$). Stąd:

$$\widehat{f}(d) = (\tau - d)^{-s}(-2\pi i)^{-s}\Gamma(s)$$

co daje:

$$(-2\pi i)^{-s}\Gamma(s) \sum_{d\in\mathbb{Z}} (\tau + d)^{-s} = \sum_{d\in\mathbb{Z}} \widehat{f}(d) e^{2\pi i 0\cdot d} = \sum_{m\in\mathbb{Z}} f(0 + m) = \sum_{m\geqslant 1} m^{s-1} q^m$$

Podrozdział 4.10

4.10.8

(a)

$$\begin{aligned}
\widehat{a}(C, D) &= \frac{1}{N} \sum_{A,B\in\mathbb{Z}/N} a(A, B)\mu_n^{-AD+BC} = (a(A, B) = 0 \text{ dla } v \nmid A, \text{ zaś dla reszty: } A = vA' \text{ dla } A' \in \mathbb{Z}/u) = \\
&= \frac{1}{N} \sum_{A'\in\mathbb{Z}/u, B\in\mathbb{Z}/n} a(vA', B)\mu_n^{-vA'D+BC} = \frac{1}{N} \sum_{A'\in\mathbb{Z}/u, B\in\mathbb{Z}/n} \psi(A')\overline{\varphi}(B)\mu_n^{-vA'D+BC} = \\
&= \frac{1}{N} \left(\sum_{A'\in\mathbb{Z}/u} \psi(A')\mu_u^{-A'D} \right) \cdot \left(\sum_{B\in\mathbb{Z}/n} \overline{\varphi}(B)\mu_n^{BC} \right)
\end{aligned}$$

Załóżmy najpierw, że $u \nmid C$ – wtedy $1 \neq \mu_u^C = \mu_N^{Cv}$, więc dla $S = \sum_{B\in\mathbb{Z}/n} \overline{\varphi}(B)\mu_n^{BC}$:

$$\begin{aligned}
\mu_N^{Cv} S &= \sum_{B\in\mathbb{Z}/n} \overline{\varphi}(B)\mu_n^{(v+B)C} = (\varphi \text{ jest charakterem} \pmod v) = \sum_{B\in\mathbb{Z}/n} \overline{\varphi}(v + B)\mu_n^{(v+B)C} = \\
&= (\text{podstawiając } B \mapsto v + B) = \sum_{B\in\mathbb{Z}/n} \overline{\varphi}(B)\mu_n^{BC} = S
\end{aligned}$$

więc $S = 0$ oraz w tym przypadku $\overline{a}(C, D) = 0$.

Załóżmy teraz, że $u|C$, $C=-cu$. Wtedy:

$$\overline{a}(C,D) = \frac{1}{N}\left(\sum_{A'\in\mathbb{Z}/u}\psi(A')\mu_u^{-A'D}\right)\cdot\left(\sum_{B\in\mathbb{Z}/n}\overline{\varphi}(B)\mu_n^{-Bcu}\right) = \frac{1}{N}\left(\sum_{A'\in\mathbb{Z}/u}\psi(A')\mu_u^{-A'D}\right)\cdot\left(\sum_{B\in\mathbb{Z}/n}\overline{\varphi}(B)\mu_v^{-Bc}\right) =$$

(zauważmy, że składniki sumy w drugim nawiasie zależą tylko od reszty $B \pmod v$), więc każdy wyraz występuje u razy)

$$= \frac{1}{N}\left(\sum_{A'\in\mathbb{Z}/u}\psi(A')\mu_u^{-A'D}\right)\cdot\left(u\cdot\sum_{B\in\mathbb{Z}/v}\overline{\varphi}(B)\mu_v^{-Bc}\right)$$

Wreszcie, korzystając z formuły (4.11) ze strony 118 (na "przekręcone" sumy Gaussa):

$$= \frac{1}{N}\left(\overline{\psi(-D)}g(\psi)\right)\cdot(u\cdot\varphi(-c)\cdot g(\overline{\varphi})) = (\text{bo } N=uv) = \frac{1}{v}\overline{\psi}(-D)\varphi(-c)g(\psi)g(\overline{\varphi})$$

coś tu nie gra ze znakami $->$ c powinno być -c

(b) ze wzoru (4.46):

$$\begin{aligned}
G_k^a(\tau,s) &= \sum_{C,D\in\mathbb{Z}/N} a(C,D)G_k^{(C,D)}(\tau,s) + (-1)^k\sum_{C,D\in\mathbb{Z}/N}\widehat{a}(-C,-D))G_k^{(C,D)}(\tau,s) = \\
&= (\text{uwzględniając zerowanie się } a \text{ oraz } \widehat{a}) = \\
&= \sum_{c,e\in\mathbb{Z}/u,d\in\mathbb{Z}/v} a(cu,d+ev)G_k^{(C,D)}(\tau,s) + (-1)^k\sum_{c,e\in\mathbb{Z}/u,d\in\mathbb{Z}/v}\widehat{a}(-cu,-(d+ev)))G_k^{(cu,d+ev)}(\tau,s) = \\
&= (\text{z podpunktu (a)}) = \sum_{c,e\in\mathbb{Z}/u,d\in\mathbb{Z}/v}\psi(c)\overline{\varphi}(d)G_k^{(cu,d+ev)}(\tau,s) \\
&+ (-1)^k\frac{g(\psi)g(\overline{\varphi})}{v}\sum_{c,e\in\mathbb{Z}/u,d\in\mathbb{Z}/v}\psi(d)\overline{\varphi}(c)G_k^{(cu,d+ev)}(\tau,s) = \\
&= G_k^{\psi,\varphi}(\tau,s) + (-1)^k\frac{g(\psi)g(\overline{\varphi})}{v}G_k^{\varphi,\psi}(\tau,s)
\end{aligned}$$

(c) z liniowości transformaty Fouriera oraz wzorów: $g(\overline{\psi}) = \psi(-1)\overline{g(\psi)}$, $(-1)^k = \psi(-1)\varphi(-1)$, $|g(\psi)|^2 = u$ dostajemy $(-1)^k g(\psi) = \varphi(-1)\frac{u}{g(\overline{\psi})}$

$$G_k^b(\tau,s) = \frac{v}{g(\overline{\varphi})}G_k^a(\tau,s) = \frac{v}{g(\overline{\varphi})}(G_k^{\psi,\varphi}(\tau,s) + (-1)^k\frac{g(\psi)g(\overline{\varphi})}{v}G_k^{\varphi,\psi}(\tau,s)) = E_k^{\psi,\varphi}(\tau,s) + \varphi(-1)E_k^{\varphi,\psi}(\tau,s)$$

Podrozdział 4.11

4.11.3

(a) Zauważmy, że dla $p\nmid m$ mamy:

$$\sum_{r\in\mathbb{Z}/p\mathbb{Z}}\mathbf{e}(mr^2/p) = \sum_{k\in\mathbb{Z}/p}\mathbf{e}(k/p)\cdot\#\{r : r^2\equiv m^{-1}k \pmod p\} = \sum_{k\in\mathbb{Z}/p}\mathbf{e}(k/p)\cdot\left(1+\left(\frac{m^{-1}k}{p}\right)\right) =$$

$$= \left(\text{mamy: }\left(\frac{m^{-1}}{p}\right) = \left(\frac{m}{p}\right)\right) = \sum_{k\in\mathbb{Z}/p}\mathbf{e}(k/p) + \left(\frac{m}{p}\right)\sum_{k\in\mathbb{Z}/p}\cdot\left(\frac{k}{p}\right) = 0 + \left(\frac{m}{p}\right)g(\chi)$$

Ponadto $g(\chi)^2 = (-1/p)p$ (Ireland, Rosen).

Dowód równości: zauważmy, że dla $p\neq 2$ liczba 2 jest odwracalna $\pmod p$, więc $A/pA = \mathbb{Z}[\frac{1+i\sqrt{3}}{2}]/p\mathbb{Z}[\frac{1+i\sqrt{3}}{2}] \cong \mathbb{Z}[i\sqrt{3}]/p\mathbb{Z}[i\sqrt{3}] = \mathbb{Z}/p\oplus i\sqrt{3}\cdot\mathbb{Z}/p$ (ostatnia równość jest równością $\mathbb{Z}/p$-modułów, a nie pierścieni). Stąd:

$$\varphi_{b,p} = \sum_{\overline{v}\in\mathbb{Z}[i\sqrt{3}]/p\mathbb{Z}[i\sqrt{3}]}\mathbf{e}(b|v|^2/p) = \sum_{r_1,r_2\in\mathbb{Z}/p}\mathbf{e}(b|r_1+i\sqrt{3}r_2|^2/p) = \sum_{r_1,r_2\in\mathbb{Z}/p}\mathbf{e}(b(r_1^2+3r_2^2)/p) =$$

$$= \left(\sum_{r_1\in\mathbb{Z}/p}\mathbf{e}(br_1^2/p)\right)\cdot\left(\sum_{r_2\in\mathbb{Z}/p}\mathbf{e}(3br_2^2/p)\right) = \left(\frac{b}{p}\right)\cdot\left(\frac{3b}{p}\right)g(\chi)^2 = \left(\frac{3}{p}\right)g(\chi)^2 =$$

$$= \left(\frac{3}{p}\right)\left(\frac{-1}{p}\right)p = (\text{prawo wzajemności}) = \left(\frac{p}{3}\right)\cdot(-1)^{\frac{(p-1)(3-1)}{4}}(-1)^{(p-1)/2} = \left(\frac{p}{3}\right)p$$

(b) jak łatwo zauważyć, mamy:

$$\forall_{w\in A}\ \mathrm{tr}(xw^*)\in\mathbb{Z} \qquad \Leftrightarrow \qquad x\in B$$

Stąd, jeżeli $x\in B$ to $\sum_{\overline{w}\in A/NA}\mathbf{e}(\mathrm{tr}(xw^*))=\sum_{\overline{w}\in A/NA}1=N^2$. Jeżeli zaś $x\notin B$, to istnieje $w_0\in A$ takie, że $\mathbf{e}(\mathrm{tr}(xw_0^*))\neq 1$. Wtedy:

$$\mathbf{e}(\mathrm{tr}(xw_0^*))\cdot\sum_{\overline{w}\in A/NA}\mathbf{e}(\mathrm{tr}(xw^*))=\sum_{\overline{w}\in A/NA}\mathbf{e}(\mathrm{tr}(x(w+w_0)^*))=\sum_{\overline{w}\in A/NA}\mathbf{e}(\mathrm{tr}(xw^*))$$

więc $\sum_{\overline{w}\in A/NA}\mathbf{e}(\mathrm{tr}(xw^*))$. Analogicznie dowodzimy drugiej równości.

(c) zauważmy, że $A/p^tA=\{\overline{v}+p^{t-1}\overline{w}:\overline{v}\in A/p^{t-1}A,\ \overline{w}\in A/pA\}$, więc:

$$\begin{aligned}
\varphi_{b,p^t} &= \sum_{\overline{u}\in A/p^tA}\mathbf{e}(b|u|^2/p^t)=\sum_{\overline{v}\in A/p^{t-1}A}\sum_{\overline{w}\in A/pA}\mathbf{e}(b|v+p^{t-1}w|^2/p^t)=\\
&= \sum_{\overline{v}\in A/p^{t-1}A}\sum_{\overline{w}\in A/pA}\mathbf{e}(b(|v|^2+p^{2(t-1)}|w|^2+p^{t-1}\,\mathrm{tr}(vw^*))/p^t)=\\
&= \sum_{\overline{v}\in A/p^{t-1}A}\mathbf{e}(b|v|^2/p^t)\cdot\sum_{\overline{w}\in A/pA}\mathbf{e}(\mathrm{tr}(bvw^*))/p)=\\
&\quad (\text{ z (b) ta suma jest równa } p^2 \text{ dla } bv/p\in B \text{ oraz } 0 \text{ w przeciwnym wypadku. Ale } b\in(\mathbb{Z}/p)^*,\\
&\quad \text{więc } bv\in pB\Leftrightarrow\ \ v\in pB,\text{ czyli } v\in pB\cap A=pA\Leftrightarrow\ \ \overline{v}=p\overline{w}\text{ dla }\overline{w}\in A/p^{t-2}A)\\
&= \sum_{\overline{w}\in A/p^{t-2}A}\mathbf{e}(b|pw|^2/p^t)p^2=p^2\varphi_{b,p^{t-2}}=\ (\text{założenie indukcyjne})\ =p^2(p^{t-2}/3)p^{t-2}=(p^t/3)p^t
\end{aligned}$$

(d) Zauważmy, że z Chińskiego Tw. o resztach, dla $(d_1,d_2)=1$ mamy: $A/d_1A\times A/d_2A\cong A/d_1d_2A$, $(\overline{u_1},\overline{u_2})\mapsto\overline{u_1}\overline{d_1}+\overline{u_2}\overline{d_2}$. Stąd:

$$\begin{aligned}
\varphi_{b,d_1d_2} &= \sum_{\overline{v}\in A/d_1d_2A}\mathbf{e}(b|v|^2/(d_1d_2))=\sum_{\overline{u}_1\in A/d_1A}\sum_{\overline{u}_2\in A/d_2A}\mathbf{e}(b|u_1d_1+u_2d_2|^2/(d_1d_2))=\\
&= \sum_{\overline{u}_1\in A/d_1A}\sum_{\overline{u}_2\in A/d_2A}\mathbf{e}(bd_1|u_1|^2/d_2)\cdot\mathbf{e}(bd_2|u_2|^2/d_1)\cdot\mathbf{e}(\mathrm{tr}(bu_1u_2^*))=(\text{mamy: }\mathrm{tr}(bu_1u_2^*)=1,\\
&\quad \text{więc }\mathbf{e}(\mathrm{tr}(bu_1u_2^*))=1)=\left(\sum_{\overline{u}_1\in A/d_1A}\mathbf{e}(bd_1|u_1|^2/d_2)\right)\cdot\left(\sum_{\overline{u}_2\in A/d_2A}\mathbf{e}(bd_2|u_2|^2/d_1)\right)=\\
&= \varphi_{bd_1,d_2}\cdot\varphi_{bd_2,d_1}=(d_2/3)d_2\cdot(d_1/3)d_1=(d_1d_2/3)d_1d_2
\end{aligned}$$

Rozdział V

5.2.5 (a) splot funkcji multyplikatywnych (tutaj: $\psi(m)$ oraz $\phi(m)m^{k-1}$) jest multyplikatywny,

(b)

$$\begin{aligned}
\sigma_{k-1}^{\psi,\phi}(np) &= \sigma_{k-1}^{\psi,\phi}(n')\cdot\sigma_{k-1}^{\psi,\phi}(p^{e+1})=\sigma_{k-1}^{\psi,\phi}(n')\cdot\left(\sum_{l=0}^{e+1}\psi(p^{e+1-l})\phi(p^l)p^{l(k-1)}\right)=\\
&= \sigma_{k-1}^{\psi,\phi}(n')\cdot\left(\psi(p)\sigma_{k-1}^{\psi,\phi}(p^e)+\psi(1)\phi(p^{e+1})p^{(e+1)(k-1)}\right)=\\
&= \psi(p)\sigma_{k-1}^{\psi,\phi}(n)+\phi(p^{e+1})p^{(e+1)(k-1)}\sigma_{k-1}^{\psi,\phi}(n')
\end{aligned}$$

Drugą formułę dostajemy, podstawiając w pierwszej $n\mapsto n/p$ oraz mnożąc stronami przez $\chi(p)p^{k-1}$. Trzeci wzór wynika ze zsumowania dwóch pierwszych.

(c)

$$\begin{aligned}
a_n(T_pE_k^{\psi,\phi,t}) &= a_{np}(E_k^{\psi,\phi,t})+1_N(p)\cdot p^{k-1}a_{n/p}(\langle p\rangle E_k^{\psi,\phi,t})=a_{np}(E_k^{\psi,\phi,t})+1_N(p)\cdot\chi(p)p^{k-1}a_{n/p}(E_k^{\psi,\phi,t})=\\
&= 2\sigma_{k-1}^{\psi,\phi}(np/t)+2\cdot 1_N(p)\cdot\chi(p)p^{k-1}\sigma_{k-1}^{\psi,\phi}(n/(tp))
\end{aligned}$$

Jeżeli $p \nmid N$, to prawa strona to:

$$= \quad 2\sigma_{k-1}^{\psi,\phi}(np/t) + 2\cdot\chi(p)p^{k-1}\sigma_{k-1}^{\psi,\phi}(n/(tp)) \overset{(b)}{=} 2(\psi(p)+\phi(p)p^{k-1})\sigma_{k-1}^{\psi,\phi}(n) = (\psi(p)+\phi(p)p^{k-1})a_n(E_k^{\psi,\phi,t})$$

Jeżeli $p|N$, $uv=N$ to $p|u$ lub $p|v$, więc $1_N(p)=\chi(p)=0$ oraz prawa strona to:

$$= \quad 2\sigma_{k-1}^{\psi,\phi}(np/t) + 2\cdot\chi(p)p^{k-1}\sigma_{k-1}^{\psi,\phi}(n/(tp))$$

5.3.1 Niech $f=\sum_l a_l q^l$.Mamy:

$$\sum_{\substack{d|n\\(n/d,N)=1}}\sum_{j=0}^{d-1} f[\begin{pmatrix} n/d & j\\ 0 & d\end{pmatrix}]_k(\tau) = \sum_{\substack{d|n\\(n/d,N)=1}}\sum_{j=0}^{d-1}\det\begin{pmatrix} n/d & j\\ 0 & d\end{pmatrix}^{k-1}\cdot d^{-k} f(\frac{n/d\tau+j}{d}) =$$

$$= \sum_{\substack{d|n\\(n/d,N)=1}}\sum_{j=0}^{d-1} n^{k-1}\cdot\sum_{l\geqslant 0} a_l \exp\left(2\pi i l\cdot\left(\frac{n/d\tau+j}{d}\right)\right) = \sum_{\substack{d|n\\(n/d,N)=1}}\sum_{l\geqslant 0} n^{k-1}d^{-k}a_l e^{2\pi i\cdot ln\tau/d^2}\sum_{j=0}^{d-1}\zeta_d^{l\cdot j} =$$

(korzystając ze wzoru: $\sum_{j=0}^{d-1}\zeta_d^{l\cdot j} = \begin{cases} 0, & d\nmid l\\ d, & d|l\end{cases}$)

$$= \sum_{\substack{d|n\\(n/d,N)=1}}\sum_{d|l} n^{k-1}d^{-k+1}\cdot a_l\cdot e^{2\pi i\cdot ln\tau/d^2} = (\text{podstawiając } l\mapsto ld) = \sum_{\substack{d|n\\(n/d,N)=1}}\sum_{l\geqslant 0}(n/d)^{k-1}\cdot a_{ld}\cdot e^{2\pi i\cdot ln\tau/d} =$$

$$= (\text{zamieniając d na n/d}) = \sum_{\substack{d|n\\(d,N)=1}}\sum_{l\geqslant 0} d^{k-1}\cdot a_{ln/d}\cdot e^{ld\tau} =$$

Zastanówmy się, ile razy $e^{2\pi i\cdot m\tau}$ występuje w danej sumie – w tym celu sumujemy współczynniki dla l,d spełniających $m=ld$, $d|(m,n)$, $(d,N)=1$ (pamiętając, że $l=m/d$):

$$=\sum_m\left(\sum_{\substack{d|(m,n)\\(d,N)=1}} a_{mn/d^2}\right)e^{2\pi i\cdot m\tau} = \sum_m\left(\sum_{d|(m,n)} 1_N(d)a_{mn/d^2}\right)e^{2\pi i\cdot m\tau} = T_n f(\tau)$$

co wynika z Proposition 5.3.1., jako że $f\in\mathcal{M}_k(\Gamma_0(N)) = M_k(1_N,N)$.

5.4.3 Niech $\mathrm{Sl}_2(\mathbb{Z})/\Gamma = \{\Gamma\alpha_1,\dots,\Gamma\alpha_n\}$ oraz $\Gamma/\Gamma' = \{\Gamma'\beta_1,\dots,\Gamma'\beta_m\}$ – wtedy $\mathrm{Sl}_2(\mathbb{Z})/\Gamma' = \{\Gamma\alpha_i\beta_j,:\ i=1,\dots,m,\quad j=1,\dots,n\}$. Stąd dla dowolnych $f,g\in\mathcal{S}_k(\Gamma)$:

$$\begin{aligned}
\langle f,g\rangle_{\Gamma'} &= \frac{1}{V_{\Gamma'}}\sum_{i,j}\int_{\mathcal{D}^*} f(\alpha_i\beta_j(t))g(\alpha_i\beta_j(t))(Im(\alpha_i\beta_j(t)))^k\,d\mu = (\text{słaba modularność}) =\\
&= \frac{1}{V_{\Gamma'}}\sum_{i,j}\int_{\mathcal{D}^*}(j(\alpha_i,\beta_j(t))^k f(\beta_j(t)))\cdot(j(\alpha_i,\beta_j(t))^k g(\beta_j(t)))\left(\frac{Im(\beta_j(t))}{j(\alpha_i,\beta_j(t))}\right)^k d\mu =\\
&= \frac{1}{V_{\Gamma'}}\sum_{i,j}\int_{\mathcal{D}^*} f(\beta_j(t))g(\beta_j(t))Im(\beta_j(t))^k\,d\mu =\\
&= \frac{[\Gamma:\Gamma']}{V_{\Gamma'}}\sum_{j}\int_{\mathcal{D}^*} f(\beta_j(t))g(\beta_j(t))Im(\beta_j(t))^k\,d\mu =\\
&= \frac{1}{V_{\Gamma}}\sum_{j}\int_{\mathcal{D}^*} f(\beta_j(t))g(\beta_j(t))Im(\beta_j(t))^k\,d\mu = \langle f,g\rangle_\Gamma
\end{aligned}$$

5.4.4

$$\begin{aligned}
V_\Gamma \cdot \langle f, tr\, g\rangle_\Gamma &= = \sum_i \int_{X(\Gamma)} f(t)\cdot g[\alpha_i]_k(t)\cdot (Im(t))^k\, d\mu = \\
&= \sum_i \int_{X(\Gamma)} f(t)\cdot \big(j(\alpha_i,t)^{-k} g(\alpha_i(t))\big)\cdot (Im(t))^k\, d\mu = (\text{słaba modularność f}) = \\
&= \sum_i \int_{X(\Gamma)} \big(j(\alpha_i,t)^{-k} f(\alpha_i(t))\big)\cdot \big(j(\alpha_i,t)^{-k} g(\alpha_i(t))\big)\cdot \big(j(\alpha_i,t)^2\cdot Im(\alpha_i(t))\big)^k\, d\mu = \\
&= \sum_i \int_{X(\Gamma)} f(\alpha_i(t))\cdot g(\alpha_i(t))\cdot Im(\alpha_i(t))^k d\mu = \\
&= \int_{X(\Gamma')} f(t)\cdot g(t)\cdot Im(t)^k d\mu = V_{\Gamma'}\cdot\langle f,g\rangle_{\Gamma'}
\end{aligned}$$

5.6.3 Przez $T_q^{(M)}$ będziemy oznaczali operator Heckego na $\mathcal{M}_k(\Gamma_1(M))$.

(a) Zauważmy, że $(i_p \circ \begin{bmatrix} T^{(N/p)} & 0 \\ 0 & T^{(N/p)} \end{bmatrix})(f,g) = T^{(N/p)}f + T^{(N/p)}(g[\alpha_p])$ oraz $T^{(N/p)} \circ i_p(f,g) = T^{(N/p)}f + (T^{(N/p)}g)[\alpha]_p$. Ponadto dla $T = \langle d\rangle$ $(NWD(d,N)=1)$ lub $T = T_q$ (dla $q \neq p$) mamy $T^{(N)} = T^{(N/p)}|_{\Gamma_1(N)}$. Wystarczy więc wykazać, że $T(g[\alpha_p]) = (Tg)[\alpha]_p$.

Niech $T = T_q$, $q \neq p$. Jeżeli $q \nmid p$, to wybierzmy q', N' takie, że $qq' - NN' = 1$. Wtedy za ostatnią macierz w definicji $T_q^{(N/p)}$ można przyjąć zarówno $\begin{bmatrix} q' & N'p \\ N/p & q \end{bmatrix}$, jak i $\begin{bmatrix} q' & N' \\ N & q \end{bmatrix}$.

$$\begin{aligned}
T(g[\alpha_p]) &= \Big(\sum_{j=0}^{q-1} g[\begin{bmatrix} 1 & j \\ 0 & q \end{bmatrix}]_k + [q\nmid N]\cdot g[\begin{bmatrix} q' & N'p \\ N/p & q \end{bmatrix}\begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix}]_k\Big)[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}]_k = \\
&= \sum_{j=0}^{q-1} g[\begin{bmatrix} 1 & j \\ 0 & q \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}]_k + [q\nmid N]\cdot g[\begin{bmatrix} q' & N'p \\ N/p & q \end{bmatrix}\begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}]_k \\
&= \sum_{j=0}^{q-1} g[\begin{bmatrix} p & j \\ 0 & q \end{bmatrix}]_k + [q\nmid N]\cdot g[\begin{bmatrix} q'qp & N'p \\ Nq & q \end{bmatrix}]_k
\end{aligned}$$

oraz

$$\begin{aligned}
(Tg)[\alpha]_p &= \sum_{j=0}^{q-1} g[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & j \\ 0 & q \end{bmatrix}]_k + [q\nmid N]\cdot g[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} q' & N' \\ N & q \end{bmatrix}\begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix}]_k = \\
&= \sum_{j=0}^{q-1} g[\begin{bmatrix} p & pj \\ 0 & q \end{bmatrix}]_k + [q\nmid N]\cdot g[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} q' & N' \\ N & q \end{bmatrix}\begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix}]_k =
\end{aligned}$$

Zauważmy, że mnożenie przez p jest automorfizmem na $\mathbb{Z}/q$, oraz

$$g[\begin{bmatrix} p & pj \\ 0 & q \end{bmatrix}]_k = g[\begin{bmatrix} 1 & [pj/q] \\ 0 & 1 \end{bmatrix}]_k[\begin{bmatrix} p & (pj \pmod q) \\ 0 & q \end{bmatrix}]_k = g[\begin{bmatrix} p & (pj \pmod q) \\ 0 & q \end{bmatrix}]_k$$

więc:

$$\begin{aligned}
(Tg)[\alpha]_p &= \sum_{j=0}^{q-1} g[\begin{bmatrix} p & j \\ 0 & q \end{bmatrix}]_k + [q\nmid N]\cdot g[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} q' & N' \\ N & q \end{bmatrix}\begin{bmatrix} q & 0 \\ 0 & 1 \end{bmatrix}]_k = \\
&= \sum_{j=0}^{q-1} g[\begin{bmatrix} p & j \\ 0 & q \end{bmatrix}]_k + [q\nmid N]\cdot g[\begin{bmatrix} q'qp & N'p \\ Nq & q \end{bmatrix}]_k
\end{aligned}$$

co dowodzi przemienności.

(b) jeżeli $p \nmid N/p$, to niech $p'p - N'\frac{N}{p} = 1$. Wtedy $\langle p\rangle^{(N/p)} = [\begin{bmatrix} p' & N' \\ N/p & p \end{bmatrix}]_k$. Mamy:

$$i_p \circ \begin{bmatrix} T_p^{(N/p)} & p^{k-1} \\ -\langle p\rangle^{(N/p)} & 0 \end{bmatrix}(f,g) = i_p(T_p^{(N/p)} f + p^{k-1}g, -\langle p\rangle^{(N/p)} f) = T_p^{(N/p)} f + p^{k-1}g - (\langle p\rangle^{(N/p)} f)[\alpha_p]_k =$$

$$= \left(\textstyle\sum_{j=0}^{p-1} f[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}]_k + [p \nmid N/p] \cdot f[\begin{bmatrix} p' & N' \\ N/p & p \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}]_k \right) + p^{k-1}g - [p \nmid N/p] \cdot f[\begin{bmatrix} p' & N' \\ N/p & p \end{bmatrix}\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}]_k$$

$$= \textstyle\sum_{j=0}^{p-1} f[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}]_k + p^{k-1}g$$

oraz

$$T_p^{(N)} \circ i_p(f,g) = T_p^{(N)}(f + g[\alpha]_p) = \sum_{j=0}^{p-1} f[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}]_k + \sum_{j=0}^{p-1} g[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}] =$$

$$= \sum_{j=0}^{p-1} f[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}]_k + \sum_{j=0}^{p-1} p^{k-1} \cdot p^{-1} g(\frac{p\tau + pj}{p}) = \sum_{j=0}^{p-1} f[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}]_k + \sum_{j=0}^{p-1} p^{k-1} \cdot p^{-1} g(\tau + j) =$$

$$= (\text{g jest 1-okresowa}) = \sum_{j=0}^{p-1} f[\begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix}]_k + p^{k-1}g$$

co dowodzi przemienności.

(c) powyższe diagramy pokazują, że dla $T = \langle d\rangle, T_q, T_p$ mamy: $T \circ i_p(f,g) = i_p(*)$, więc operatory Heckego od staroformy przyjmują wartości w staroformach. Dla $T = T_{q^r}, T_{p^r}$ wystarczy skorzystać z rekurencji – $T_1 = id$, T_q, T_{q^r}, $\langle q\rangle, \langle p\rangle = 0$ zachowują staroformy, więc $T_{q^{r+1}} = T_q T_{q^r} - q^{k-1}\langle q\rangle T_{q^{r-1}}$ oraz $T_{p^{r+1}} = T_p T_{p^r}$ również.

(d) jeżeli $f \in \mathcal{S}_k(\Gamma_1(N))^{new} = (\mathcal{S}_k(\Gamma_1(N))^{old})^{\perp}$, to $T_n f \in \mathcal{S}_k(\Gamma_1(N))^{new}$, bo dla dowolnego $g \in \mathcal{S}_k(\Gamma_1(N))^{old}$ mamy:

$$(T_n f, g) = (f, \underbrace{T_n^* g}_{\in \mathcal{S}_k(\Gamma_1(N))^{old}}) = 0$$

więc $T_n f \in (\mathcal{S}_k(\Gamma_1(N))^{old})^{\perp} = \mathcal{S}_k(\Gamma_1(N))^{new}$.

(e)

$$i_p \circ \begin{bmatrix} 0 & p^{k-1}w_{N/p} \\ w_{N/p} & 0 \end{bmatrix}(f,g) = i_p(p^{k-1}g[\begin{bmatrix} 0 & 1 \\ -N/p & 0 \end{bmatrix}]_k, f[\begin{bmatrix} 0 & 1 \\ -N/p & 0 \end{bmatrix}]_k) =$$

$$= p^{k-1}g[\begin{bmatrix} 0 & 1 \\ -N/p & 0 \end{bmatrix}]_k + f[\begin{bmatrix} 0 & 1 \\ -N/p & 0 \end{bmatrix}]_k[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}]_k = p^{k-1}g[\begin{bmatrix} 0 & 1 \\ -N/p & 0 \end{bmatrix}]_k + f[\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}]_k$$

oraz

$$\begin{aligned} w_N \circ i_p(f,g) &= (f + g[\alpha_p]_k)[\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}]_k = f[\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}]_k + g[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}]_k \\ &= f[\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}]_k + g[\begin{bmatrix} 0 & p \\ -N & 0 \end{bmatrix}]_k = f[\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}]_k + g[\begin{bmatrix} 0 & 1 \\ -N/p & 0 \end{bmatrix}]_k[\begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}]_k = \\ &= (\text{macierze skalarne działają na formach mnożeniem przez potęgę wyznacznika}) = \\ &= f[\begin{bmatrix} 0 & 1 \\ -N & 0 \end{bmatrix}]_k + p^{k-1}g[\begin{bmatrix} 0 & 1 \\ -N/p & 0 \end{bmatrix}]_k \end{aligned}$$

co dowodzi przemienności.

5.7.2 Niech $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \in \Gamma_d = \Gamma_1(N) \cap \Gamma^0(N/d)$ – z definicji mamy wtedy:

$$A, D \equiv 1 \pmod{N}, \qquad C \equiv 0 \pmod{N}, \qquad B \equiv 0 \pmod{N/d} \qquad (*)$$

Niech $B' = \frac{B}{N/d}$.

Wykażemy, że istnieje dokładnie jedno $0 \leqslant b < d$ takie, że $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} 1 & bN/d \\ 0 & 1 \end{bmatrix}^{-1} \in \Gamma(N)$. Istotnie:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} 1 & bN/d \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} 1 & -bN/d \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} A & A \cdot (-\frac{bN}{d}) + B \\ C & C \cdot (-\frac{bN}{d}) + D \end{bmatrix} \in \Gamma(N) \Leftrightarrow$$

$$\Leftrightarrow A \equiv 1 \pmod N, \quad A \cdot (-\frac{bN}{d}) + B \equiv 0 \pmod N, \quad C \equiv 0 \pmod N, \quad C \cdot (-\frac{bN}{d}) + D \equiv 0 \pmod N$$

Z kongruencji (*) dostajemy, że wszystkie te kongruencje zachodzą automatycznie, za wyjątkiem drugiej, więc:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} 1 & bN/d \\ 0 & 1 \end{bmatrix}^{-1} \in \Gamma(N) \quad \Leftrightarrow \quad A \cdot (-\frac{bN}{d}) + B \equiv 0 \pmod N \Leftrightarrow 1 \cdot (-\frac{bN}{d}) + B \equiv 0 \pmod N \Leftrightarrow$$

$$\Leftrightarrow \quad B \equiv \frac{bN}{d} \pmod N \Leftrightarrow \frac{N}{d} \cdot (B' - b) \equiv 0 \pmod N$$

zaś ostatnia kongruencja jest równoważna: $b \equiv B' \pmod d$. To oznacza, że b istnieje i jest wyznaczone jednoznacznie $\pmod d$.

5.8.4 Jeżeli $a_1(f) = 0$, to z rozumowania na końcu strony 195 wynika, że $f \in S^{old}(\Gamma^1(N))$. Załóżmy więc, że $f = g + h$ jest unormowaną formą własną ($a_1(f) = 1$) oraz $g \in \mathcal{S}^{old}(\Gamma^1(N))$, $h \in \mathcal{S}^{new}(\Gamma^1(N))$. Niech $T_n f = \lambda_n f$, wtedy:

$$\lambda_n = \lambda_n \cdot a_1(f) = a_1(\lambda_n f) = a_1(T_n(f)) = a_n(f) \qquad (*)$$

Ponadto $T_n g + T_n h = T_n f = a_n(f) f = a_n(f) g + a_n(f) h$ oraz $\langle n \rangle g + \langle n \rangle h = \langle n \rangle f = \chi(n) f = \chi(n) g + \chi(n) h$. Ale $T_n g \in \mathcal{S}^{old}(\Gamma^1(N))$, $T_n h \in \mathcal{S}^{new}(\Gamma^1(N))$ oraz $S^{old}(\Gamma^1(N))$, $S^{new}(\Gamma^1(N))$ są liniowo rozłączne, więc z równości $T_n g + T_n h = a_n(f) g + a_n(f) h$ wynika, że $T_n g = a_n(f) g$, $T_n h = a_n(f) h$; analogicznie $\langle n \rangle g = \chi(n) g$, $\langle n \rangle h = \chi(n) h$.

Ale to oznacza (na mocy Theorem 5.8.2 lub rozważań podobnych do (*)), że $a_n(h) = c \cdot a_n(f)$ dla pewnego $c \in \mathbb{C}$ i wszystkich n. Stąd jednak: $h = \sum a_n(h) q^n = c \sum a_n(f) q^n = cf$. Jeżeli $c = 0$, to $h = 0$, więc $f = g \in \mathcal{S}^{old}(\Gamma^1(N))$. Jeżeli $c \neq 0$, to $f = c^{-1} h \in \mathcal{S}^{new}(\Gamma^1(N))$

5.8.6

(a) niech $\{f_1, \ldots, f_r\}$ będą wszystkimi nowoformami rzędu dzielącego N. Załóżmy nie wprost, że dla każdego i istnieje $p_i \nmid N$ takie, że $a_{p_i}(g) \neq a_{p_i}(f_i)$. Zgodnie z twierdzeniem 5.8.3 mamy: $g(\tau) = \sum_i c_{i,j} f_i(n_{i,j}\tau)$ dla pewnych $c_{i,j} \in \mathbb{C}$. Rozważmy operator $\prod_i (T_{p_i} - a_{p_i}(f_i))$. Zauważmy, że $(T_{p_i} - a_{p_i}(f_i))(f_j) = (a_{p_i}(f_j) - a_{p_i}(f_i)) \cdot f_j$, więc:

$$\prod_i (T_{p_i} - a_{p_i}(f_i))(f_j) = \prod_i (a_{p_i}(f_j) - a_{p_i}(f_i)) \cdot f_j = 0$$

co daje:

$$\prod_i (T_{p_i} - a_{p_i}(f_i))(g) = \prod_i (T_{p_i} - a_{p_i}(f_i)) \left(\sum_i c_{i,j} f_i(n_{i,j}\tau) \right) = 0$$

(zauważmy, że $p_i \nmid N$, więc $p_i \nmid n_{i,j}$ – to gwarantuje, że $T_{p_i} \circ [\alpha_{n_{i,j}}] = [\alpha_{n_{i,j}}] \circ T_{p_i}$; wynika to np. z zadania 5.6.3 a. Stąd $T_{p_i}(f(n\,\cdot))(\tau) = T(f)(n\tau)$) Z drugiej strony, g jest unormowaną formą własną, więc

$$T_{p_i} g = \lambda_i g \Rightarrow \lambda_i = a_1(T_{p_i}(g)) = a_{p_i}(g)$$

czyli $T_{p_i} g = a_{p_i}(g) g$ oraz

$$0 = \prod_i (T_{p_i} - a_{p_i}(f_i))(g) = \prod_i (a_{p_i}(g) - a_{p_i}(f_i)) \cdot g$$

czyli $a_{p_i}(g) = a_{p_i}(f_i)$ dla pewnego i. Sprzeczność kończy dowód Proposition 5.8.4.

(b) niech f_k będzie funkcją znalezioną w poprzednim podpunkcie. Niech $g(\tau) = \sum_{i,j} c_{i,j} f_i(n_{i,j}\tau)$. Załóżmy nie wprost, że $c_{s,t} \neq 0$ dla pewnych (s,t), $s \neq k$ Wtedy:

$$T_p(g(\tau)) = T_p(\sum_{i,j} c_{i,j} f_i(n_{i,j}\tau)) = \sum_{i,j} c_{i,j} a_p(f_i) f_i(n_{i,j}\tau)$$

a z drugiej strony:

$$T_p(g(\tau)) = a_p(g)g = a_p(g) \cdot \sum_{i,j} c_{i,j} f_i(n_{i,j}\tau)$$

więc $\sum_{i,j} c_{i,j} a_p(f_i) f_i(n_{i,j}\tau) = \sum_{i,j} a_p(g) c_{i,j} f_i(n_{i,j}\tau)$ oraz z liniowej niezależności (Theorem 5.3.3) mamy: $c_{i,j} a_p(f_i) = c_{i,j} a_p(f_i)$. W szczególności $a_p(f_s) = a_p(g) = a_p(f_k)$ dla każdego $p \nmid N$, co przeczy *Strong Muliplicity One*. Stąd $g(\tau) = \sum_j c_{k,j} f_k(n_{i,j}\tau) \in Span\{f_k(n\tau) : nM|N\}$.

5.9.1

(a) rozważmy funkcję $g : X(\Gamma) \to \mathbb{R}$, $g(\tau) = \begin{cases} |Im(\tau)^{k/2} \cdot f(\tau)|, & \tau \in \mathcal{H} \\ 0, & \tau \text{ jest cuspem} \end{cases}$ – zauważmy najpierw, że jest ona dobrze określona: jeżeli $\alpha \in \Gamma$, to z modularności mamy:

$$g(\alpha(\tau)) = |Im(\alpha(\tau))^{k/2} \cdot f(\alpha(\tau))| = \left| \frac{Im(\tau)^{k/2}}{|c_\alpha\tau + d_\alpha|^k} \cdot (c_\alpha\tau + d_\alpha)^k f(\tau) \right| = |Im(\tau)^{k/2} \cdot f(\tau)| = g(\tau)$$

Ponadto jest ona ciągła – dla $\tau \in \mathcal{H}$ jest ona ciągła, więc wystarczy sprawdzić ciągłość w cuspach. Niech s będzie cuspem, zaś $\beta \in \mathrm{Sl}_2(\mathbb{Z})$, $\beta(\infty) = s$. Wtedy wystarczy sprawdzić ciągłość $g \circ \beta$ w ∞. Ale f jest cusp formą, więc $f[\beta]_k(\tau) = (c_\alpha\tau + d_\alpha)^{-k} f(\beta(\tau)) = q \cdot \sum_n a_n q^n$. Stąd:

$$\lim_{Im(\tau)\to\infty} g(\beta(\tau)) = \lim_{Im(\tau)\to\infty} |\frac{Im(\tau)^{k/2}}{|c_\alpha\tau + d_\alpha|^k} \cdot q \cdot \sum_n a_n q^n| = |a_0| \cdot \lim_{Im(\tau)\to\infty} \frac{Im(\tau)^{k/2}}{|c_\alpha\tau + d_\alpha|^k} e^{-2\pi i Im(\tau)} = 0$$

Stąd funkcja g jest ciągła na zwatej przestrzenii, więc ma maksimum, i jest ograniczona.

(b) mamy:

$$\begin{aligned} 1 \quad &\leqslant \quad \frac{n^{k-1} + \ldots + 1^{k-1}}{n^{k-1}} = \frac{\sum_{d|n} d^{k-1}}{n^{k-1}} = \sum_{d|n} (d/n)^{k-1} \\ &= \quad (\text{podstawiając } d' = n/d) = \sum_{d'|n} (1/d')^{k-1} << \sum_{d' \geqslant 0} (1/d')^{k-1} = \zeta(k-1) \end{aligned}$$

Dowolny szereg Eisensteina wagi k jest kombinacją szeregów $E_k^{\overline{v}}$ dla $\overline{v} \in (\mathbb{Z}/N)^2$, więc wystarczy to sprawdzić dla tych szeregów. Ale ich współczynniki Fouriera dane są wzorami:

$$c \cdot \sigma_{k-1}^{\overline{v}}(n) = c \cdot \sum_{d|n} sgn(d) \mu_N^{d_v m} d^{k-1}$$

(c to stała) więc wartości bezwzględne ich współczynników są $\leqslant \sigma_{k-1}(n) \leqslant C \cdot n^{k-1}$.

5.9.3 Współczynniki Fouriera $\frac{1}{2}E_k^{\psi,\phi}$ dane są wzorem $\sigma_{k-1}^{\psi,\phi} = (\psi * (\phi \cdot p_{k-1}))(n)$ (gdzie $p_{k-1}(n) = n^{k-1}$), zaś splot odpowiada mnożeniu szeregów Dirichleta, więc:

$$\begin{aligned} L(s, \frac{1}{2}E_k^{\psi,\phi}) \quad &= \quad \sum_n \frac{\sigma_{k-1}^{\psi,\phi}(n)}{n^s} = \left(\sum_n \frac{\psi(n)}{n^s} \right) \cdot \left(\sum_n \frac{\phi(n) n^{k-1}}{n^s} \right) = \\ &= \quad \left(\sum_n \frac{\psi(n)}{n^s} \right) \cdot \left(\sum_n \frac{\phi(n)}{n^{s-k+1}} \right) = L(\psi, s) \cdot L(\phi, s-k+1) \end{aligned}$$

Z zadania 5.9.1 (b) wynika, że $|\sigma_{k-1}^{\psi,\phi}(n)| \leqslant \sigma_{k-1}(n) \leqslant \zeta(k-1) \cdot n^{k-1}$, więc $L(s, \frac{1}{2}E_k^{\psi,\phi})$ jest zbieżne dla $\Re(s) > k$.

Chyba nie trzeba pokazywać, że jest rozbieżny dla $\Re(s) < k$ – "what is **a** half plane..."

5.11.3

(a) Niech:

$$\{E_k^{\phi,\varphi} : \phi, \varphi \text{ są charakterami modulo } u, v; \phi\varphi = \psi, tuv|M\} = \{E_1, \ldots, E_r\}$$

– wiemy, że $\mathcal{E}_k(M, \psi) = Span\{E_i(t\tau) : tu_iv_i|M\}$.

Wykażemy, że jeżeli $g \in \mathcal{E}_k(M, \psi)$ jest unormowaną formą własną to dla pewnego i zachodzi $\forall_{p\nmid M} \quad a_p(E_i/2) = a_p(g)$. Dowód przebiega dokładnie jak w zadaniu 5.8.6(a). Zauważmy najpierw, że g jest unormowaną formą własną, więc

$$T_{p_i}g = \lambda_i g \Rightarrow \lambda_i = a_1(T_{p_i}(g)) = a_{p_i}(g)$$

czyli $T_{p_i}g = a_{p_i}(g)g$ i podobnie dla $E_i/2$.

Załóżmy nie wprost, że dla każdego i istnieje $p_i \nmid M$ takie, że $a_{p_i}(g) \neq a_{p_i}(\frac{1}{2}E_i)$. Wtedy $g \in Span\{E_i(t\tau) : i = 1, \ldots, r; \quad tu_iv_i|M\}$, więc $g(\tau) = \sum_i \sum_j c_{i,j}\frac{1}{2}E_i(t_{i,j}\tau)$ dla pewnych $c_i \in \mathbb{C}$. Rozważmy operator $\prod_i(T_{p_i} - a_{p_i}(\frac{1}{2}E_i))$. Zauważmy, że $(T_{p_i} - a_{p_i}(\frac{1}{2}E_i))(\frac{1}{2}E_j) = (a_{p_i}(\frac{1}{2}E_j) - a_{p_i}(\frac{1}{2}E_i)) \cdot \frac{1}{2}E_j$, więc:

$$\prod_i(T_{p_i} - a_{p_i}(\frac{1}{2}E_i))(\frac{1}{2}E_j) = \prod_i(a_{p_i}(\frac{1}{2}E_j) - a_{p_i}(\frac{1}{2}E_i)) \cdot \frac{1}{2}E_j = 0$$

(zauważmy, że $p_i \nmid M$, więc $p_i \nmid t_{i,j}$ – to gwarantuje, że $T_{p_i} \circ [\alpha_{t_{i,j}}] = [\alpha_{t_{i,j}}] \circ T_{p_i}$; wynika to np. z zadania 5.6.3 a. Stąd $T_{p_i}(\frac{1}{2}E_i(t_{i,j}\,\cdot))(\tau) = T(\frac{1}{2}E_i)(t_{i,j}\tau))$ co daje:

$$\prod_i(T_{p_i} - a_{p_i}(\frac{1}{2}E_i))(g) = \prod_i(T_{p_i} - a_{p_i}(\frac{1}{2}E_i))\left(\sum_i\sum_j c_{i,j}\frac{1}{2}E_i(t_{i,j}\tau)\right) = 0$$

Z drugiej strony:

$$0 = \prod_i(T_{p_i} - a_{p_i}(\frac{1}{2}E_i))(g) = \prod_i(a_{p_i}(g) - a_{p_i}(\frac{1}{2}E_i)) \cdot g$$

czyli $a_{p_i}(g) = a_{p_i}(\frac{1}{2}E_i)$ dla pewnego i. Sprzeczność kończy dowód.

(b) z podpunktu (a) (zauważmy, że z Section 5.9 θ_χ jest unormowaną formą własną): $a_p(\theta_\chi) = a_p(\frac{1}{2}E_k^{\phi,\varphi})$. To daje:

$$\phi(p) + \varphi(p) = \sigma_0^{\phi,\varphi}(p) = a_p(\frac{1}{2}E_k^{\phi,\varphi}) = a_p(\theta_\chi) = \begin{cases} 2 & p \equiv 1 \pmod 3, \quad d \text{ jest sześcianem} \pmod p \\ -1 & p \equiv 1 \pmod 3, \quad d \text{ nie jest sześcianem} \pmod p \\ 0 & p \equiv 2 \pmod 3, \quad d \text{ lub } p|3d \pmod p \end{cases}$$

Stąd dla dowolnego $p \equiv 2 \pmod 3$: $\phi(p) + \varphi(p) = 0$. Wybierzmy dowolne $n \in (\mathbb{Z}/3N^2)^*$, $n \equiv 2 \pmod 3$ – wtedy z twierdzenia Dirichleta o liczbach pierwszych w postępach arytmetycznych istnieje $p \equiv n \pmod{3N^2}$ oraz $\phi(n) + \varphi(n) = \phi(p) + \varphi(p) = 0$, tzn. $\phi(n) = \underbrace{(\frac{n}{3})}_{=-1}\varphi(n)$.

Jeżeli $n \equiv 1 \pmod 3$, to $-n \equiv 2 \pmod 3$, więc z powyższych rozważań i wzoru $\phi(-1)\varphi(-1) = -1$ dostajemy: $\phi(n) = \phi(-1)\phi(-n) = \varphi(-1)\phi(-n) = \varphi(-1)\varphi(-n) = \varphi(n)$. Stąd dla $3 \nmid n$ mamy: $\phi(n) = (\frac{n}{3})\varphi(n)$.

(c) dla $p \equiv 1 \pmod 3$ mamy:

$$\{2, -1\} \ni \phi(p) + \varphi(p) = \phi(p)(1 + (\frac{p}{3})) = 2\phi(p)$$

więc $\phi(p) = 1$. Stąd: $(\frac{p}{3})\chi(p) = \phi(p)\varphi(p) = (\frac{p}{3})\phi^2(p) = (\frac{p}{3})$ dla $p \neq 3$, więc $\chi(p) = 1$. Korzystając znowu z twierdzenia Dirichleta: $\chi(n) = 1$ dla wszystkich $n \in (\mathbb{Z}/3N^2)^*$. Sprzeczność kończy dowód – charakter χ nie może być nietrywalny. [1]

[1] z rozwiązania wynika, że ϕ^2 jest trywialne – $\chi(n)^2 = \chi(n^2) = 1$, bo $n^2 \equiv 1 \pmod 3$ – ale nie jest mi to potrzebne w dalszej części