Groupe de travail : Congruences sur la fonction τ de Ramanujan et représentations galoisiennes

Exposé du 2/10/2025

Plan :

I- Domaine fondamental pour l'action de $SL_2(\mathbb{Z})$ sur le demi-plan de Poincaré

II- Formule $k/12$

III- Dimension et base des espaces de formes modulaires

IV- La congruence modulo 691

Notations :

- $\Gamma = SL_2(\mathbb{Z})$, dont on rappelle qu'il agit sur le demi-plan de Poincaré $\mathbb{H}$
- M_k l'espace des formes modulaires de poids k, pour $k \in \mathbb{Z}$
- $E_k := \dfrac{G_k}{2\zeta(k)}$ la série d'Eisenstein normalisée de poids k

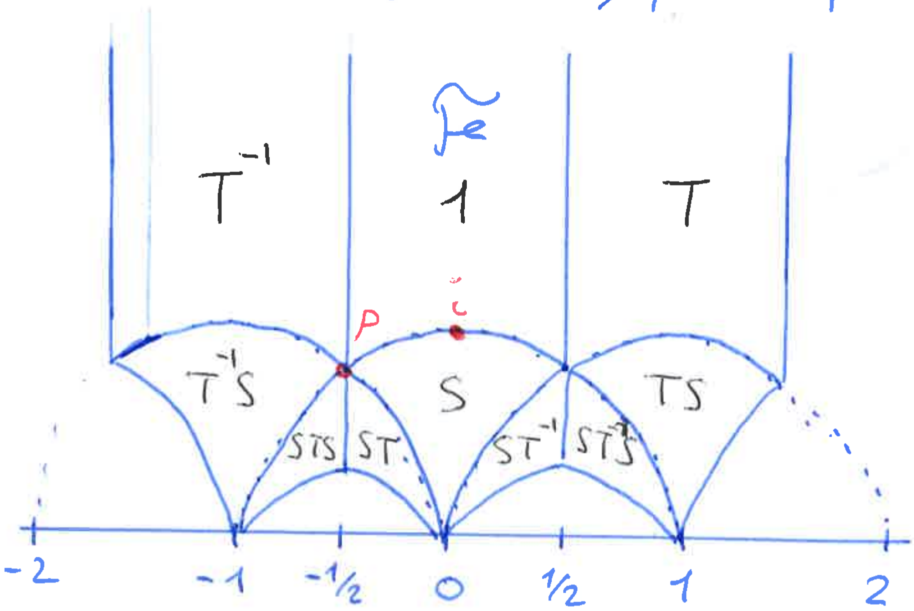
$$\left(= \frac{1}{2\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{0\}} \frac{1}{(mz+n)^k} \right)$$

- $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ deux éléments de Γ

I- Domaine fondamental pour l'action $\Gamma \curvearrowright \mathbb{H}$

On pose $\mathcal{F} := \{ z \in \mathbb{H} \mid |\mathrm{Re}\, z| \leq \frac{1}{2}$ ou $|z| \geq 1 \}$.

C'est ce qu'on appelle le domaine fondamental pour l'action $\Gamma \curvearrowright \mathbb{H}$. On remarque deux points importants de ce domaine : i et $\rho = e^{\frac{2i\pi}{3}}$, qui vérifient $Si = i$ et $ST\rho = \rho$.



Pavage de $\mathbb{H}$ par la Γ-orbite de $\mathcal{F}$

Thm : i- Pour tout $\tau \in \mathbb{H}$, l'orbite $\Gamma\tau$ rencontre $\mathcal{F}$

ii- Si τ, τ' sont deux points distincts de $\mathcal{F}$ tels que $\Gamma\tau = \Gamma\tau'$, alors :

- soit $\mathrm{Re}\,\tau = \pm\frac{1}{2}$ et $\tau' = \tau \pm 1 = T^{\pm 1}\tau$
- soit $|\tau| = 1$ et $\tau' = -\frac{1}{\tau} = S\tau$

iii- Si $\tau \in \mathcal{F}$ alors le stabilisateur de τ par Γ est :

- $\langle S \rangle$ si $\tau = i$
- $\langle ST \rangle$ si $\tau = \rho$ ou $-\rho^2$
- $\{\pm 1\}$ sinon

Rq : On a $S^2 = -1$ et $(ST)^3 = -1$

D/ i- On montre en fait que pour $\tau \in \mathbb{H}$, $G\tau \cap \mathcal{F} \neq \emptyset$ où $G = \langle S, T \rangle$.

On rappelle que pour $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ et $\tau \in \mathbb{H}$, on a :

$$\operatorname{Im}(\gamma\tau) = \det\gamma \cdot \frac{\operatorname{Im}\tau}{|c\tau+d|^2} = \frac{\operatorname{Im}\tau}{|c\tau+d|^2}$$

Or, la forme quadratique $\begin{array}{l}\mathbb{R}^2 \to \mathbb{R} \\ (c,d) \mapsto |c\tau+d|^2\end{array}$ est définie positive, elle admet donc un minimum sur $\mathbb{Z}^2 \setminus \{0\}$, on peut donc considérer $E \subset G\tau$ l'ensemble des $\tau' \in G\tau$ tels que $\operatorname{Im}\tau'$ est maximal.

E est invariant par T, on peut donc prendre $\tau' \in E$ tel que $|\operatorname{Re}\tau| \leq \frac{1}{2}$.

Mais $S\tau' = -\frac{1}{\tau'} \in G\tau$ et $\operatorname{Im}(-\frac{1}{\tau'}) = \frac{\operatorname{Im}\tau'}{|\tau'|^2}$ donc $|\tau'| \geq 1$.

D'où $\tau' \in G\tau \cap \mathcal{F}$.

ii- et iii- Soient $\tau, \tau' \in \mathcal{F}$ et $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ tels que $\operatorname{Im}\tau \geq \operatorname{Im}\tau'$ et $\tau' = \gamma\tau$.

On a $|c\tau+d| \leq 1$ donc $|c \operatorname{Im}\tau| \leq 1$ donc $|c| \leq 1$.

- Si $c = 0$ alors $a = d = \pm 1$ donc $\pm\gamma$ est T ou T^{-1} et on est dans le premier cas de ii-.
- Sinon, quitte à remplacer γ par $-\gamma$, on peut supposer que $c = 1$. On a $|\tau + d| \leq 1$ donc $|\tau| = 1$ et on est dans un des cas suivants :

1- $\tau \neq \rho, -\rho^2$ et $d = 0$, alors $b = -1$ et $\tau' = a - 1/\tau$, et ĉ $|\operatorname{Re}(-\frac{1}{\tau})| < \frac{1}{2}$ on a $a = 0$. Dc $\gamma = S$ et $\tau' = \tau = i$.

2- $\tau = \rho$ et $d = 0, 1$. Si $d = 0$, on a encore $b = -1$ et $\tau' = a - 1/\rho$, donc soit $\tau' = -\rho^2$, $a = 0$ alors $\gamma = \pm S$, soit $\tau' = \tau$, $a = -1$ et $\gamma = (ST)^2$.

Si $d = 1$, alors $\det \gamma = a - b = 1$

donc $\gamma\rho = \dfrac{(b+1)\rho + \rho}{\rho + 1} = -\dfrac{1}{\rho} + b = \rho + 1 + b$

donc $\tau = \rho$ et $b = -1$, $\gamma = ST$ (2^e cas de iii-)

ou $\tau = -\rho^2 = \rho + 1$ (2nd cas de ii-)

3- On traite de même le cas $\tau = -\rho^2$ et $d = 0, -1$.

$\square$

<u>Corollaire</u>: Γ est engendré par S et T.

D/ On reprend la notation de la démonstration précédente $G = \langle S, T \rangle$, et on fixe $\tau \in \mathring{\mathcal{F}}$. Soit $\gamma \in \Gamma$.

On a montré qu'il existe $g \in G$ tel que $g\gamma\tau \in \mathcal{F}$.

Alors $g\gamma \in \Gamma$ fixe τ, donc c'est ± 1.

Comme $-1 = S^2 \in G$, on a bien $\gamma \in G$.

$\square$

II- Formule $k/12$

Soit $f \in M_k$ et $P \in \mathbb{H}$. On note $v_P(f)$ l'ordre d'annulation de f en P et e_P le cardinal du stabilisateur de P sous l'action de $PSL_2(\mathbb{Z})$. Ces deux quantités sont des entiers positifs invariants sous l'action de Γ.
Le théorème énoncé dans la partie I- assure que $e_i = 2$, $e_\rho = 3$ et $e_P = 1$ si $P \in \mathbb{H} \setminus (\Gamma i \cup \Gamma \rho)$.
On note également $v_\infty(f)$ l'ordre d'annulation de $\tilde{f}$ en 0.

<u>Thm</u>: (formule $k/12$)

Soit $k \in \mathbb{Z}$ et $f \in M_k$ non nulle. On a :

$$v_\infty(f) + \sum_{P \in \Gamma \backslash \mathbb{H}} \frac{v_P(f)}{e_P} = \frac{k}{12}$$

<u>Rq</u>: • En particulier, cette somme est finie.

• La remarque précédente sur les valeurs possibles de e_P permet de réécrire cette formule en :

$$v_\infty(f) + \frac{v_i(f)}{2} + \frac{v_\rho(f)}{3} + \sum_{\substack{P \in \Gamma \backslash \mathbb{H} \\ P \neq [i],[\rho]}} v_P(f) = \frac{k}{12}$$

On a besoin d'un lemme d'analyse complexe avant d'entamer la preuve :

<u>Lemme</u> : Soit $a \in \mathbb{C}$, $R>0$ et $f : D^*(a,R) \to \mathbb{C}$ une fonction holomorphe sur le disque épointé telle que a est un pôle simple de f.

Alors pour $\theta \in [0, 2\pi[$, $\alpha \in]0,1[$ on a :

$$\lim_{r \to 0} \frac{1}{2i\pi} \int_{C_{\theta,\alpha,r}} f(z)\,dz = \alpha \cdot res_a(f)$$

où $C_{\theta,\alpha,r}$ est l'arc de cercle centré en a, de rayon r, allant de l'angle θ à $\theta + \alpha 2i\pi$.

D/ La série de Laurent de f en a s'écrit :

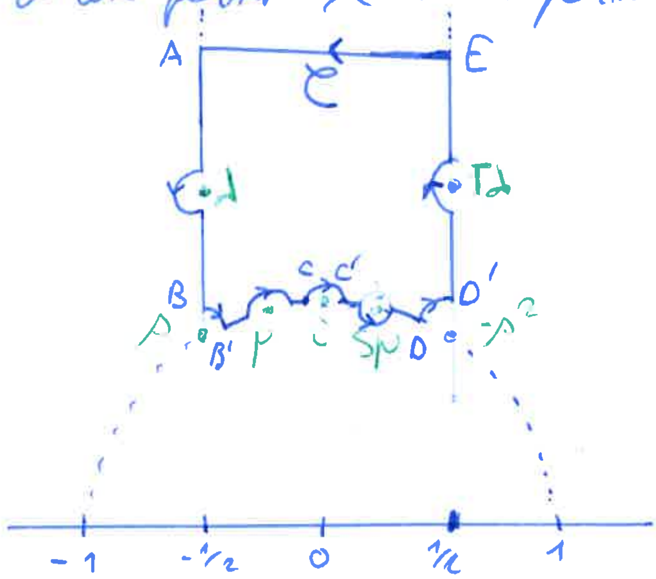
$$f(z) = \sum_{n \geq -1} a_n z^n = \frac{a_{-1}}{z} + g(z) \quad \text{où } g(z) = \sum_{n \geq 0} a_n z^n$$

Alors $$\frac{1}{2i\pi}\int_{C_{\theta,\alpha,r}} f(z)\,dz = \underbrace{\frac{1}{2i\pi}\int_{C_{\theta,\alpha,r}} \frac{a_{-1}}{z}\,dz}_{= \alpha a_{-1}} + \underbrace{\frac{1}{2i\pi}\int_{C_{\theta,\alpha,r}} g(z)\,dz}_{\xrightarrow[r \to 0]{} 0}$$

$\square$

Dém/ Pour $r>0$, on pose $\Omega_r = \{\tau\in\mathbb{H} \mid \operatorname{Im}\tau > r\}$. Comme $\tilde{f}$ est holomorphe en 0, il existe $r>0$ tel que f ne s'annule pas sur Ω_r. La partie $\mathcal{F}-\Omega_r$ est compacte, la fonction holomorphe f n'y a donc qu'un nombre fini de zéros. Cela montre la finitude de la somme.

On peut alors considérer le contour $\mathcal{C}$ dessiné ci-dessous : les zéros de f dans $\partial\mathcal{F}-\{i,\rho,-\rho^2\}$ sont notés α s'ils sont de partie réelle $-\frac{1}{2}$, et μ s'ils sont de module 1. On suppose que chaque petit cercle dessiné ne contient qu'un zéro. On note la portion de $\mathcal{C}$ allant d'un point X à un point Y γ_{XY}.



La formule des résidus appliquée à $\frac{f'}{f}$ donne :

$$\frac{1}{2i\pi}\int_{\mathcal{C}} \frac{f'(\tau)}{f(\tau)}\,d\tau = \sum_{\substack{P\in\Gamma\backslash\mathbb{H}\\ P\neq[i],[\rho]}} v_P(f)$$

On regarde les contributions des différentes portions.

- Le chemin $\omega : t \mapsto e^{2i\pi\gamma_{EA}(t)}$ est un cercle de centre 0 dans D tournant dans le sens indirect. On a :

$$\frac{1}{2i\pi}\int_{\gamma_{EA}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau = \frac{1}{2i\pi}\int_{\omega} \frac{\tilde{\ell}'(q)}{\tilde{\ell}(q)}\,dq = -v_\infty(\ell)$$

par changement de variable et théorème des résidus.

- On a $\displaystyle\int_{\gamma_{AB}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau = \int_{T\gamma_{AB}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau = \int_{\gamma_{ED}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau = -\int_{\gamma_{DE}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau$

donc les portions γ_{AB} et γ_{DE} s'annulent

- On a également par modularité de ℓ, $\displaystyle\frac{\ell'}{\ell} = -\frac{k}{\tau} + \frac{(\ell\circ S)'}{\ell\circ S}$

donc $\displaystyle\frac{1}{2i\pi}\int_{\gamma_{B'C}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau = -\frac{1}{2i\pi}\int_{\gamma_{B'C}} \frac{k}{\tau}\,d\tau + \frac{1}{2i\pi}\int_{S\gamma_{B'C}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau$

et comme $S\gamma_{B'C} = \gamma_{DC'}$, les portions $\gamma_{B'C}$ et $\gamma_{C'D}$ se somment à $\displaystyle -\frac{1}{2i\pi}\int_{\gamma_{B'C}} \frac{k}{\tau}\,d\tau$ qui tend, lorsque les rayons des disques autour de ρ et i tendent vers 0, vers $\displaystyle -\frac{k}{2i\pi}\int_{\rho\to i} \frac{d\tau}{\tau} = \frac{k}{12}$.

- En appliquant le lemme à $\displaystyle\frac{1}{2i\pi}\int_{\gamma_{BB'}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau$, on trouve que cette quantité tend vers $-\frac{1}{6}v_\rho(\ell)$ quand le rayon du cercle correspondant tend vers 0.

De même, $\displaystyle\frac{1}{2i\pi}\int_{\gamma_{DD'}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau \longrightarrow -\frac{1}{6}v_\rho(\ell)$ et $\displaystyle\frac{1}{2i\pi}\int_{\gamma_{CC'}} \frac{\ell'(\tau)}{\ell(\tau)}\,d\tau \longrightarrow -\frac{1}{2}v_i(\ell)$

On conclut en mettant ces relations bout à bout. $\square$

III - Dimension et base des espaces de formes modulaires

Si $k \geq 4$ est pair, on peut considérer $\varphi : \begin{array}{l} M_k \to \mathbb{C} \\ f \mapsto f(\infty) \end{array}$.

C'est une application linéaire, dont on note S_k le noyau.

On dit que S_k est le sous-espace des formes modulaires <u>paraboliques</u>.

<u>Prop:</u> Pour tout entier pair $k \geq 4$, on a $M_k = S_k \oplus \mathbb{C} E_k$

D/ $S_k = \ker \varphi$ est de codimension 1 et $\varphi(G_k) = G_k(\infty) = 1 \neq 0$. $\square$

On a ainsi une première décomposition des espaces M_k.

La formule $k/12$ permet également d'obtenir rapidement des résultats pour k petit :

<u>Prop:</u> Soit $k \in \mathbb{Z}$ pair.

i - Si $k < 0$ ou $k = 2$, alors $M_k = 0$

ii - $M_0 = \mathbb{C}1$ et si $k = 4, 6, 8, 10$, alors $M_k = \mathbb{C} E_k$

D/ i - Tous les termes de la somme dans la formule $k/12$ sont positifs, ils ne peuvent donc pas donner un terme négatif.

De plus, si $k = 2$, alors $\frac{k}{12} = \frac{1}{6}$ qui ne peut pas être obtenu avec des combinaisons linéaires par des entiers positifs de $\frac{1}{2}$ et $\frac{1}{3}$.

ii - Si $k < 12$, alors $\frac{k}{12} < 1$ donc $S_k = 0$ car pour $f \in S_k \setminus \{0\}$, $v_\infty(f) \geq 1$.

$\square$

On a montré la semaine dernière que Δ est une forme modulaire de poids 12 telle que $\Delta(\infty)=0$. La formule $k/12$ permet alors d'exprimer plus de propriétés sur Δ :

<u>Prop:</u> i- La fonction Δ ne s'annule pas sur $\mathbb{H}$ et on a $v_\infty(\Delta)=1$

ii- Si $k\in\mathbb{Z}$, alors $S_k=\Delta M_{k-12}$. En particulier, $S_{12}=\mathbb{C}\Delta$ est de dimension 1.

D/ i- On a $\Delta(\infty)=0$ donc $v_\infty(\Delta)\geq 1$ et $\frac{12}{12}=1$ donc la formule $k/12$ donne que $v_\infty(\Delta)=1$ et que $\forall p\in\mathbb{H}$, $v_p(\Delta)=0$.

ii- Si $f\in S_k$, alors $\frac{f}{\Delta}$ est une forme modulaire de poids $k-12$.

$\square$

Cela permet alors d'obtenir une autre écriture de Δ :

<u>Prop:</u> On a $\Delta=\frac{1}{1728}(E_4^3-E_6^2)$

D/ On a vu que Δ et $D:=\frac{1}{1728}(E_4^3-E_6^2)$ sont deux formes modulaires de poids 12.

De plus, on a $D(\infty)=\frac{1}{1728}\left(E_4(\infty)^3-E_6(\infty)^2\right)=\frac{1^3-1^2}{1728}=0$

donc on a $\Delta, D\in S_{12}$ qui est de dimension 1, Δ et D sont donc colinéaires.

Or, on a $\Delta(q)=\sum_{k\geq 1}\tau(k)q^k$ et $E_k(q)=1-\frac{2k}{B_k}\sum_{n\geq 1}\sigma_{k-1}(n)q^n$

Les valeurs connues des premiers termes de τ, B_k, σ_{k-1} permettent de montrer que $\tau(1)=a_1(D)$, donc $\Delta=D$.

$\square$

Thm : Soit $k \in \mathbb{Z}$. L'espace M_k admet pour base les $E_4^r E_6^s$ avec $r, s \in \mathbb{N}$ vérifiant $4r + 6s = k$.

D/ Le résultat est immédiat pour $k < 0$. Montrons le pour $k \geq 0$ pair.

Commençons par remarquer que pour $f \in M_k$, on a $f(i) = f(Si) = i^k f(i)$ donc $f(i) = 0$ si $k \not\equiv 0 [4]$

De même, $f(\rho) = 0$ si $k \not\equiv 0 [3]$.

Enfin on a alors $E_4(\rho) = 1$ donc $v_\rho(E_4) \geq 1$ et la formule $k/12$ nous donne que ρ est le seul point d'annulation de E_4, en particulier $E_4(i) \neq 0$.

- On montre la liberté de la famille par récurrence sur $k \geq 0$ pair. Le cas $k = 0$ est immédiat.

  Supposons alors $k > 0$ et soit $\lambda_{r,s}$ des complexes tels que :

$$\sum_{4r+6s=k} \lambda_{r,s} E_4^r E_6^s = 0$$

  Si $k \equiv 0 [4]$, en évaluant en i on a $\lambda_{k/4, 0} = 0$

  donc dans tous les cas on a $\lambda_{r,s} \neq 0 \Rightarrow s \neq 0$.

  Alors soit les $\lambda_{r,s}$ sont tous nuls, soit on a $k \geq 6$ et on peut simplifier l'équation ci-dessus par E_6.

  On conclut alors par récurrence.

- On montre également que cette famille est génératrice par récurrence sur $k \geq 0$ pair, le cas $k=0$ étant encore une fois trivial.

On peut supposer $k \geq 4$. On sait qu'il existe un couple (r,s) d'entiers naturels tels que $k = 4r + 6s$: on a soit $k \equiv 0\ [4]$, soit $k \equiv 6\ [4]$ et $k \geq 6$.

Soit (r,s) un tel couple. Alors pour $f \in M_k$, on a $f - f(\infty) E_4^r E_6^s \in S_k$. Mais $S_k = \Delta M_{k-12}$ et $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$. On conclut par récurrence. $\square$

On peut également déterminer la dimension des espaces M_k :

<u>Prop</u>: Soit $k \geq 0$ pair. On a $\dim M_k = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{si } k \equiv 2\ [12] \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{sinon} \end{cases}$

D/ On pourrait utiliser la base connue de M_k, mais il y a en fait plus simple.

On sait que cette formule est vraie pour $k < 12$.

Mais on sait également que pour $k \geq 12$, on a :

$M_k = S_k \oplus \mathbb{C} E_k = (\Delta M_{k-12}) \oplus \mathbb{C} E_k$.

donc $\dim M_k = \dim M_{k-12} + 1$

On conclut alors par récurrence immédiate. $\square$

IV- La congruence modulo 691

On veut montrer la congruence (CG) sur la fonction τ :
Pour tout premier p, on a :

$$(CG)\quad \tau(p) \equiv 1 + p^{11}\ [691]$$

On commence par remarquer que $(E_{12} - E_4^3)(\infty) = 1 - 1^3 = 0$
donc $E_{12} - E_4^3 \in S_{12} = \mathbb{C}\Delta$: il existe un unique $\lambda \in \mathbb{C}$ tel que $E_{12} - E_4^3 = \lambda\Delta$.

Or, on a $E_k(q) = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$ et on connait les valeurs de $-\frac{2k}{B_k}$ pour $k = 4, 12$ qui sont respectivement 240 et $\frac{65520}{691}$.

On a donc $E_4(q) = 1 + 240 \cdot 1 \cdot q + O(q^2)$
et $E_{12}(q) = 1 + \frac{65520}{691} \cdot 1 \cdot q + O(q^2)$

donc $E_{12} - E_4^3(q) = \left(\frac{65520}{691} - 720\right) q + O(q^2)$

donc $\lambda = \frac{65520}{691} - 720$

En multipliant par 691 l'équation $E_{12} - E_4^3 = \lambda\Delta$ et en prenant le modulo 691, on obtient alors pour $n \in \mathbb{N}^*$:

$$65520\, \tau(n) \equiv 65520\, \sigma_{11}(n) - 0\ [691]$$

Alors, $65520 \wedge 691 = 1$ et pour p premier, $\sigma_{11}(p) = 1 + p^{11}$, d'où :

$$\tau(p) \equiv 1 + p^{11} \; [691]$$