

Classification des congruences de la fonction τ

Youssef Guindy

1^{er} février 2026

1 Quelques préliminaires

1.1 Rappels

Dans tout l'exposé, les lettres p et ℓ désigneront des nombres premiers. Rappelons que τ est multiplicative et que $\tau(p^{n+1}) = \tau(p)\tau(p^n) - p^{11}\tau(p^{n-1})$, donc pour connaître les valeurs de $\tau(n)$, il suffit de connaître $\tau(p)$ pour p premier.

Nous cherchons à classifier les congruences de la fonction τ modulo un nombre premier ℓ . L'aboutissement de la partie formes modulaires du groupe de travail était la preuve des deux théorèmes suivants :

Théorème 1.1. *Soit ℓ un nombre premier et a, b tels que $a + b \equiv 11 \pmod{\ell - 1}$. On suppose que pour tout $p \neq \ell$, $\tau(p) \equiv p^a + p^b \pmod{\ell}$, alors on a nécessairement $\ell \in \{2, 3, 5, 7, 691\}$ et les congruences sont alors :*

$$\begin{aligned}\tau(p) &\equiv 0 \pmod{2} \\ \tau(p) &\equiv p + p^2 \pmod{3} \\ \tau(p) &\equiv p + p^2 \pmod{5} \\ \tau(p) &\equiv p + p^4 \pmod{7} \\ \tau(p) &\equiv 1 + p^{11} \pmod{691}\end{aligned}$$

Théorème 1.2. *Soit ℓ tel que pour tout p non carré modulo ℓ , on a $\tau(p) \equiv 0 \pmod{\ell}$. Alors $\ell = 23$.*

Nous avons donc trouvé un nombre fini de congruences possibles en supposant une certaine forme pour les congruences. Nous allons expliquer pourquoi en fait ces formes sont les seules formes possibles.

1.2 Le théorème de Deligne

Le résultat qui motive la forme des congruences est le théorème suivant, qu'on admet, qui est un cas particulier d'un théorème de Deligne.

Théorème 1.3 (Deligne pour la fonction τ). *Pour tout premier ℓ , il existe un corps de nombres K_ℓ galoisien sur \mathbb{Q} , non ramifié hors de ℓ , et une représentation $\rho_\ell : \text{Gal}(K_\ell/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$ fidèle*

et semisimple telle que pour tout premier $p \neq \ell$,

$$\begin{aligned}\mathrm{tr}(\rho_\ell(\mathrm{Frob}_p)) &= \tau(p) \\ \mathrm{det}(\rho_\ell(\mathrm{Frob}_p)) &= p^{11} .\end{aligned}$$

Remarque. 1. Pour $p \neq \ell$, p est non ramifié, donc Frob_p est une classe de conjugaison dans $\mathrm{Gal}(K_\ell/\mathbb{Q})$, et donc son image par ρ_ℓ est dans une classe de conjugaison de matrices, donc on peut parler de sa trace et de son déterminant.

2. Les égalités sur la trace et le déterminant sont dans \mathbb{F}_ℓ , donc ce sont en fait des congruences modulo ℓ .

Ainsi, les formes des congruences deviennent déjà un peu plus naturelle puisqu'on exprime la trace d'une matrice de $\mathrm{GL}_2(\mathbb{F}_\ell)$ comme somme de deux entiers modulo ℓ .

2 La classification des congruences

Comme ρ_ℓ est injective, $G := \mathrm{Gal}(K_\ell/\mathbb{Q})$ est isomorphe à $G_\ell := \rho_\ell(\mathrm{Gal}(K_\ell/\mathbb{Q}))$ qui est un sous-groupe de $\mathrm{GL}_2(\mathbb{F}_\ell)$. Or nous avons classifié ces sous-groupes. Commençons par une remarque qui motive la suite.

Remarque. Soit $g \in G$. Par le théorème de Cebotarev, il existe p tel que $g \in \mathrm{Frob}_p$. On a alors $\mathrm{det}(\rho_\ell(g)) \equiv p^{11} \pmod{\ell}$, donc $\mathrm{det}(G_\ell) \subseteq \mathbb{F}_\ell^{\times,11}$ le sous-groupe des puissances onzièmes. Si G_ℓ contient $\mathrm{SL}_2(\mathbb{F}_\ell)$, alors toutes les traces modulo ℓ sont possibles, donc nous considérerons dans ce cas qu'il n'y a pas de congruences. Rendons cette affirmation plus précise.

2.1 Cas sans congruences

Théorème 2.1. *Si $\mathrm{SL}_2(\mathbb{F}_\ell) \subseteq G_\ell$, alors pour tous $q \in \mathbb{N}^*$, $a \in (\mathbb{Z}/q\mathbb{Z})^\times$ et $b \in \mathbb{Z}/\ell\mathbb{Z}$, il existe p premier tel que*

$$\begin{cases} p \equiv a \pmod{q} \\ \tau(p) \equiv b \pmod{\ell} . \end{cases}$$

Remarque. Ce théorème affirme que dans le cas où G_ℓ contient SL_2 , aucune congruence sur p ne donne de congruence sur $\tau(p)$ modulo ℓ !

Démonstration. Nous allons nous contenter de traiter le cas où $q = p$. La preuve dans le cas général est très similaire à ceci près qu'il faut distinguer les cas où $\ell \mid q$ et où $\ell \nmid q$.

Considérons le diagramme suivant :

$$\begin{array}{ccc} \mathrm{Gal}(K_\ell(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) & \longrightarrow & \mathrm{Gal}(K_\ell/\mathbb{Q}) \xrightarrow{\mathrm{det} \circ \rho_\ell} \mathbb{F}_\ell^{\times,11} \\ \downarrow & & \\ \mathrm{Gal}(\mathbb{Q}(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) & & \\ \omega_\ell \downarrow & & \\ \mathbb{F}_\ell^\times & & \end{array}$$

où ω_ℓ est le caractère cyclotomique. Il est clair que Frob_p dans $\text{Gal}(K_\ell(e^{\frac{2i\pi}{\ell}})/\mathbb{Q})$ se restreint à Frob_p dans les deux autres groupes de Galois. Par le théorème de Chebotarev, tout élément est un dans un certain Frob_p , donc on a $\det \circ \rho_\ell = \omega_\ell^{11}$. Par théorie de Galois, on a alors

$$\text{Gal}(K_\ell(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) \cong \{(M, d) \in G_\ell \times (\mathbb{Z}/\ell\mathbb{Z})^\times \mid \det M \equiv d^{11} [\ell]\}.$$

Comme le caractère cyclotomique est surjectif, il vient que $\det \circ \rho_\ell$ est surjectif sur les puissance onzièmes dans \mathbb{F}_ℓ^\times , donc il existe $M_0 \in G_\ell$ telle que $\det M_0 = a^{11}$. Or comme G_ℓ contient SL_2 il contient toutes les matrices de déterminant a^{11} , donc il existe $M \in G_\ell$ telle que $\det M = a^{11}$ et $\text{tr}(M) = b$. Ainsi $(M, a) \in \text{Gal}(K_\ell(e^{\frac{2i\pi}{\ell}})/\mathbb{Q})$, donc par le théorème de Chebotarev, il existe un nombre premier p tel que $(M, a) \in \text{Frob}_p$, donc on a bien, toujours par restriction des Frobenius,
$$\begin{cases} p \equiv a [\ell] & (\text{par le caractère cyclotomique}) \\ \tau(p) \equiv b [\ell] & (\text{par la représentation de Deligne}) \end{cases} \quad \square$$

Ceci motive donc la définition suivante, qui correspond au cas où on pourrait avoir des congruences.

Définition 2.2. Un nombre premier ℓ est dit *exceptionnel* lorsque $\text{SL}_2(\mathbb{F}_\ell) \not\subseteq G_\ell$.

Dans la suite, on considère alors $\ell > 2$ un nombre premier exceptionnel (le cas $\ell = 2$ a déjà été traité).

2.2 Premier cas : G_ℓ est inclus dans un Borel

Nous rappelons que c'est le cas où G_ℓ est inclus dans le stabilisateur d'une droite $D := \mathbb{F}_\ell v$ de \mathbb{F}_ℓ^2 . Comme la représentation est semisimple, D a un supplémentaire stable, donc en fait G_ℓ est inclus dans un sous-groupe de Cartan déployé, c'est à dire que dans une base adaptée, toutes les matrices de G_ℓ sont diagonales, donc de la forme $\begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$, où $\chi_1, \chi_2 : G \rightarrow \mathbb{F}_\ell^\times$. Le lemme suivant donne la forme possible d'un caractère $\chi : G \rightarrow \mathbb{F}_\ell^\times$.

Lemme 2.3. Soit $\chi : G \rightarrow \mathbb{F}_\ell^\times$. Alors il existe $k \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ tel que $\chi(\text{Frob}_p) = p^k$.

Démonstration. Le noyau $H := \text{Ker}(\chi)$ est un sous-groupe distingué de G , et χ se factorise par H en un morphisme injectif de G/H dans \mathbb{F}_ℓ^\times , donc G/H est abélien, d'ordre divisant $\ell-1$. Par théorie de Galois, la sous-extension K_ℓ^H de K_ℓ fixée par H est abélienne sur \mathbb{Q} , non ramifiée hors de ℓ car c'est une sous-extension de K_ℓ/\mathbb{Q} qui est non ramifiée hors de ℓ , et son degré divise $\ell-1$, donc est premier avec ℓ . Par le théorème de Kronecker-Weber, c'est un sous-corps de $\mathbb{Q}(e^{\frac{2i\pi}{\ell}})$. On a $\text{Gal}(K_\ell^H/\mathbb{Q}) = G/H$, d'où le diagramme :

$$\begin{array}{ccc} G & \xrightarrow{\chi} & \mathbb{F}_\ell^\times \\ & \searrow & \nearrow \\ & G/H & \\ & \uparrow & \\ \text{Gal}(\mathbb{Q}(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) & \xrightarrow{\omega_\ell} & \mathbb{F}_\ell^\times \end{array}$$

Or un morphisme de groupes de $\mathbb{F}_\ell^\times \rightarrow \mathbb{F}_\ell^\times$ envoie un générateur g sur g^k pour $k \in \mathbb{Z}/(\ell-1)\mathbb{Z}$, donc est de la forme $x \mapsto x^k$. Comme les Frobenius s'envoient sur les Frobenius correspondants dans les groupes de Galois, et que $\omega_\ell(\text{Frob}_p) = p$, on a $\chi(\text{Frob}_p) = p^k$. \square

Il existe alors d'après le lemme $a, b \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ tels que $\rho_\ell(\text{Frob}_p) = P \begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix} P^{-1}$. Ainsi, la condition sur le déterminant donne $a + b \equiv 11 \pmod{\ell-1}$, donc on se ramène au cas du théorème 1.1 déjà traité.

2.3 Une réciproque du premier cas

En fait nous avons la proposition suivante.

Proposition 2.4. *Soit a, b tels que $\tau(p) \equiv p^a + p^b \pmod{\ell}$ pour tout $p \neq \ell$. Alors G_ℓ est inclus dans un Borel.*

Démonstration. On considère

$$\begin{aligned} \rho'_\ell : \text{Gal}(\mathbb{Q}(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) &\rightarrow \text{GL}_2(\mathbb{F}_\ell) \\ g &\mapsto \begin{pmatrix} \omega_\ell(g)^a & 0 \\ 0 & \omega_\ell(g)^b \end{pmatrix}, \end{aligned}$$

puis $\theta_\ell : \text{Gal}(K_\ell(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(e^{2i\pi/\ell})/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_\ell)$, qui envoie Frob_p sur $\begin{pmatrix} p^a & 0 \\ 0 & p^b \end{pmatrix}$. Ainsi θ_ℓ a la même trace que la représentation de Deligne car c'est vrai pour les Frob_p pour p premier, ce qui suffit par le théorème de Chebotarev. Comme $\ell > 2$, la dimension de la représentation est strictement plus petite que la caractéristique, donc θ_ℓ et ρ_ℓ ont même polynôme caractéristique et sont semisimples, donc elles sont isomorphes! \square

2.4 Deuxième cas : G_ℓ est inclus dans un Cartan non-dépolé

Dans ce cas, il existe D une droite de $\mathbb{F}_{\ell^2}^2$ non définie sur \mathbb{F}_ℓ qui est stabilisée par G_ℓ , donc on considère

$$\tilde{\rho}_\ell : \text{Gal}(K_\ell/\mathbb{Q}) \hookrightarrow \text{GL}_2(\mathbb{F}_\ell) \hookrightarrow \text{GL}_2(\mathbb{F}_{\ell^2}).$$

Théorème 2.5. *Ce deuxième cas n'arrive pas.*

Commençons par un lemme qui sera utile dans la preuve.

Lemme 2.6. *Soit $\varphi : \mathbb{F}_\ell^\times \rightarrow \mathbb{F}_{\ell^2}^\times$ un morphisme de groupes. Alors $\text{im}(\varphi) \subseteq \mathbb{F}_\ell^\times$.*

Démonstration. Soit $x \in \mathbb{F}_\ell^\times$. On a $\varphi(x)^{\ell-1} = \varphi(x^{\ell-1}) = 1$, donc

$$\text{im}(\varphi) \subseteq \{y \in \mathbb{F}_{\ell^2}^\times \mid y^{\ell-1} = 1\} = \mathbb{F}_\ell^\times.$$

\square

Démonstration du théorème. Dans une base adaptée de $\mathbb{F}_{\ell^2}^2$, toutes les matrices de G_ℓ sont diagonales comme dans le premier cas.

Lemme 2.7. *Soit $\chi : G \rightarrow \mathbb{F}_{\ell^2}^\times$ un morphisme de groupes. Alors $\text{im}(\chi) \subseteq \mathbb{F}_\ell^\times$.*

Démonstration. On peut de même factoriser χ par son noyau qui donne une extension intermédiaire L abélienne sur \mathbb{Q} , non ramifiée hors de ℓ , de degré divisant $\ell^2 - 1$ donc premier avec ℓ . Par Kronecker-Weber (cf. premier cas pour plus de détails), on a le diagramme suivant :

$$\begin{array}{ccc}
 \text{Gal}(K_\ell/\mathbb{Q}) & \xrightarrow{\chi} & \mathbb{F}_{\ell^2}^\times \\
 \downarrow & \nearrow & \\
 \text{Gal}(L/\mathbb{Q}) & & \\
 \uparrow & & \\
 \text{Gal}(\mathbb{Q}(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) & \xrightarrow{\omega_\ell} & \mathbb{F}_\ell^\times
 \end{array}$$

On a donc un morphisme de groupes $\mathbb{F}_\ell^\times \rightarrow \mathbb{F}_{\ell^2}^\times$. Ainsi, par le théorème de Cebotarev et le lemme précédent, $\text{im}(G) \subseteq \mathbb{F}_\ell^\times$. \square

On a alors les mêmes congruences que pour le premier cas. D'après la réciproque, ce cas n'arrive pas. \square

2.5 Troisième cas : G_ℓ est inclus dans le normalisateur d'un Cartan

2.5.1 Cartan déployé

Nous rappelons que si G_ℓ est inclus dans le normalisateur d'un Cartan déployé mais pas dans le Cartan déployé, alors dans une base adaptée de \mathbb{F}_ℓ^2 , toutes les matrices de G_ℓ sont diagonales ou antidiagonales, et on a donc un morphisme non trivial $G \rightarrow \mathbb{Z}/2\mathbb{Z}$ correspondant au fait d'échanger ou pas les deux droites du sous-groupe de Cartan.

On a alors $N \trianglelefteq G$ et une suite exacte courte

$$1 \rightarrow N \rightarrow G \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow 1 .$$

Il vient qu'on a une sous extension Q_ℓ de K_ℓ/\mathbb{Q} telle que $[Q_\ell : \mathbb{Q}] = 2$. De plus, Q_ℓ est non ramifiée hors de ℓ .

Lemme 2.8. *Soit Q_ℓ une extension de \mathbb{Q} de degré 2 non ramifiée hors de ℓ . Alors $Q_\ell = \mathbb{Q}(\sqrt{\ell^*})$, où $\ell^* = (-1)^{\frac{\ell-1}{2}} \ell$.*

Démonstration. Il existe classiquement $n \in \mathbb{Z}$ sans facteur carré tel que $Q_\ell = \mathbb{Q}(\sqrt{n})$. Dans ce cas

$$\mathcal{O}_{Q_\ell} = \begin{cases} \mathbb{Z} \left[\frac{1 + \sqrt{n}}{2} \right] & \text{si } n \equiv 1 \pmod{4} \\ \mathbb{Z}[\sqrt{n}] & \text{si } n \equiv 2, 3 \pmod{4} \end{cases} , \text{ donc le discriminant vaut } n \text{ ou } 4n \text{ respectivement. Or}$$

il faut que le discriminant soit divisible uniquement par $\ell > 2$, donc on a nécessairement $n \equiv 1 \pmod{4}$ pour ne pas avoir 4 qui divise le discriminant, et d'autre part on a $|n| = \ell$. Ceci donne exactement

$$Q_\ell = \mathbb{Q}(\sqrt{\ell^*}) .$$

\square

Par Kronecker-Weber, $\mathbb{Q}(\sqrt{\ell^*})$ est inclus dans $\mathbb{Q}(e^{\frac{2i\pi}{\ell}})$, donc on a un morphisme de groupes $(\mathbb{Z}/\ell\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}(e^{\frac{2i\pi}{\ell}})/\mathbb{Q}) \rightarrow \text{Gal}(\mathbb{Q}(\ell)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ qui envoie Frob_p sur Frob_p .

D'une part, le seul morphisme de groupes $(\mathbb{Z}/\ell\mathbb{Z})^\times \rightarrow \mathbb{Z}/2\mathbb{Z}$ non trivial est $x \mapsto \begin{cases} 0 & \text{si } p \text{ carré modulo } \ell \\ 1 & \text{sinon} \end{cases}$
car un générateur de \mathbb{F}_ℓ^\times est nécessairement envoyé sur 1. Ainsi, comme $\omega_\ell(\text{Frob}_p) = p$, on a

$$\text{Frob}_p = 0 \text{ dans } \mathbb{Z}/2\mathbb{Z} \iff p \text{ carré modulo } \ell .$$

Or s'envoyer sur 0 c'est exactement correspondre à une matrice diagonale, donc on trouve que si p non carré modulo ℓ , alors $\tau(p) \equiv \text{tr}(\rho_\ell(\text{Frob}_p)) \equiv 0 \pmod{\ell}$. On est alors dans le cas du théorème 1.2 déjà traité!

Remarque. D'autre part, si $p\mathcal{O}_{Q_\ell} = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, alors $fg = 2$ où $f = \dim_{\mathbb{F}_\ell}(\mathcal{O}_{Q_\ell}/\mathfrak{p}_i)$. Or on a alors que f est l'ordre de Frob_p dans le groupe de Galois, donc on a l'équivalence :

$$\begin{aligned} \text{Frob}_p = 0 \text{ dans } \mathbb{Z}/2\mathbb{Z} &\iff \text{ord}(\text{Frob}_p) = 1 \text{ dans } \mathbb{Z}/2\mathbb{Z} \\ &\iff p \text{ se décompose dans } \mathcal{O}_{Q_\ell} \\ &\iff X^2 - \ell^* \in \mathbb{F}_p[X] \text{ se factorise} \\ &\iff \ell^* \text{ carré modulo } p \end{aligned}$$

Donc on retrouve *la loi de réciprocité quadratique* : p est carré modulo ℓ si et seulement si ℓ^* est carré modulo p .

2.5.2 Cartan non-déployé

Rappelons que quand G_ℓ est inclus dans le normalisateur d'un Cartan non-déployé mais pas dans le Cartan non-déployé, dans une base adaptée de $\mathbb{F}_{\ell^2}^\times$, toutes les matrices de G_ℓ sont diagonales ou antidiagonales, avec au moins une matrice antidiagonale. Nous avons donc un morphisme non trivial $G \rightarrow \mathbb{Z}/2\mathbb{Z}$ et on est exactement dans le sous-cas précédent. On est donc ramené au théorème 1.2.

2.6 Groupes exceptionnels

Si on n'est pas dans l'un des cas précédents, alors en considérant H_ℓ l'image de G_ℓ dans $\text{PGL}_2(\mathbb{F}_\ell)$, on a $H_\ell \cong \mathcal{A}_4, \mathfrak{S}_4$ ou \mathcal{A}_5 . En notant $\mathbb{F}_\ell^{\times,2}$ le sous-groupe des carrés, on a $\overline{\det} \circ \rho_\ell : G_\ell \rightarrow \mathbb{F}_\ell/\mathbb{F}_\ell^{\times,2}$ qui se factorise en un morphisme non trivial $H_\ell \rightarrow \mathbb{F}_\ell^\times/\mathbb{F}_\ell^{\times,2} \cong \mathbb{Z}/2\mathbb{Z}$, qui lui-même se factorise par l'abélianisé H_ℓ^{ab} .

Or $\mathcal{A}_4^{ab} \cong \mathbb{Z}/3\mathbb{Z}$ qui n'a pas de morphisme non trivial vers $\mathbb{Z}/2\mathbb{Z}$ et \mathcal{A}_5 est simple. Ceci élimine \mathcal{A}_4 et \mathcal{A}_5 .

Éliminons maintenant \mathfrak{S}_4 .

Lemme 2.9. *Si $H_\ell \cong \mathfrak{S}_4$, alors pour tout $g \in G_\ell$, on a $\frac{\text{tr}(g)^2}{\det g} \in \{0, 1, 2, 4\}$.*

Remarque. Ceci a un sens car si on multiplie g par λI_2 , on multiplie la trace par λ et le déterminant par λ^2 , donc on a bien ici une quantité "homogène".

Démonstration. Commençons par remarquer que tout élément de \mathfrak{S}_4 est d'ordre 1, 2, 3 ou 4. Soit $g \in G_\ell$ et soient $x, y \in \mathbb{F}_{\ell^2}$ ses valeurs propres. Notons \bar{g} son image dans $\text{PGL}_2(\mathbb{F}_\ell)$.

- Si $\bar{g} = 1$, alors $x = y$, donc $\frac{\text{tr}(g)^2}{\det g} = \frac{4x^2}{x^2} = 4$.
- Si $\text{ord}(\bar{g}) = 2$, alors $x^2 = y^2$ mais $x \neq y$, donc $\frac{\text{tr}(g)^2}{\det g} = 0$.
- Si $\text{ord}(\bar{g}) = 3$, alors $x^3 = y^3$ mais $x \neq y$, donc $x^2 + xy + y^2 = 0$, d'où $\frac{\text{tr}(g)^2}{\det g} = \frac{xy}{xy} = 1$.
- Si $\text{ord}(\bar{g}) = 4$, alors $x^4 = y^4$ mais $x^2 \neq y^2$, donc $x^2 = -y^2$, d'où $\frac{\text{tr}(g)^2}{\det g} = \frac{2xy}{xy} = 2$.

□

Ainsi on a dans ce cas

$$\forall p \neq \ell, \frac{\tau(p)^2}{p^{11}} \equiv 0, 1, 2, \text{ ou } 4 \pmod{\ell}.$$

Supposons que $\ell \notin \{2, 3, 5, 7, 23\}$ qu'on a déjà traités.

Pour $p = 2$, on trouve que ℓ doit diviser $\tau(2)^2, \tau(2)^2 - 2^{11}, \tau(2)^2 - 2^{12}$ et $\tau(2)^2 - 2^{13}$, donc on trouve en factorisant

$$\ell \in \{2, 3, 5, 7, 11, 17, 23\}.$$

Pour $p = 5$, on trouve

$$\ell \in \{2, 3, 5, 7, 23, 79, 89, 4831, 12911, 1486547\}.$$

Finalement $\ell = 2, 3, 5, 7$ ou 23 , donc ce cas n'arrive pas!