ANNALES SCIENTIFIQUES
DE L'UNIVERSITÉ DE CLERMONT-FERRAND 2
Série Mathématiques

PAUL RIVOIRE

Dernier théorème de Fermat et groupes de classes dans certains corps quadratiques imaginaires

Annales scientifiques de l'Université de Clermont-Ferrand 2, tome 68, série *Mathématiques*, n° 18 (1979), p. 1-35

<http://www.numdam.org/item?id=ASCFM_1979__68_18_1_0>

DERNIER THEOREME DE FERMAT ET GROUPES DE CLASSES DANS CERTAINS CORPS QUADRATIQUES IMAGINAIRES

Paul RIVOIRE

Université de Clermont

Comme l'a déjà montré Euler, la courbe

(E) $\qquad R(1-R) = \wedge^p$ («courbe d'Euler»)

du plan affine est la transformée rationnelle de la courbe

(F) $\qquad X^p + Y^p = Z^p$ («courbe de Fermat»)

par la transformation

(T) $\qquad R = \dfrac{X^p}{Z^p}$, $\wedge = \dfrac{XY}{Z^2}$.

Il en résulte qu'à tout point rationnel tel que $Z \neq 0$ de la courbe de Fermat, c'est-à-dire à toute solution entière rationnelle $P = (x, y, z)$ de l'équation de Fermat (F) (considérée à un coefficient de proportionalité près) correspond un point rationnel $T.P = (r = \dfrac{x^p}{z^p}, \lambda = \dfrac{xy}{z^2})$ de la courbe d'Euler.

Le mathématicien suédois Bendz (Upsala, 1901) a montré que ce sont les *seuls points rationnels* de cette courbe. (Ce résultat a été redécouvert en 1939 par M. Krasner, dans sa première Note intitulée «Sur le théorème de Fermat»).

En effet :

Si (r, λ) est un tel point, mettons r sous la forme d'une fraction irréductible α / β . Alors on a $1-r = \dfrac{\beta - \alpha}{\beta}$, d'où $\dfrac{\alpha(\beta-\alpha)}{\beta^2} = \lambda^p$. Comme α , β , $\beta - \alpha$ sont mutuellement premiers, chacun de ces entiers doit être une puissance $p^{ème}$. Il existe donc des entiers x, y, z tels que $\alpha = x^p$, $\beta - \alpha = y^p$, et $\beta = z^p$, d'où résulte $x^p + y^p = z^p$. On a, de plus,

$$T.(x, y, z) = \left(\frac{x^p}{z^p}, \frac{xy}{z^2}\right) = \left(\frac{\alpha}{\beta}, \sqrt[p]{\frac{\alpha(\beta-\alpha)}{\beta^2}}\right) = (r, \epsilon\lambda),$$

où ϵ désigne une racine p-ième de l'unité. Mais, comme $\dfrac{xy}{z^2}$ et λ sont tous deux rationnels,

ϵ est nécessairement égal à un, et $T(x, y, z) = (r, \lambda)$.

Si l'on appelle une solution (x, y, z) de l'équation (F) non-triviale quand $xyz \neq 0$, et si l'on appelle non-triviale celle, rationnelle, (r, λ) de l'équation (E) quand $\lambda \neq 0$, le résultat précédent montre que l'existence des solutions entières non-triviales de (F) équivaut à celle des solutions rationnelles non-triviales de (E). On exprimera brièvement ce fait en disant que *(E) et (F) sont équivalentes dans le corps rationnel Q.*

Dans la note citée, M. Krasner a généralisé ce résultat à certains corps quadratiques imaginaires, en montrant que si $k = Q(\sqrt{-m})$ est un tel corps dont le nombre des classes d'idéaux h(k) ne se divise pas par p-supposé premier impair et, en outre, $m \neq 3$ quand $p = 3$, *(E) et (F) sont encore équivalentes au sens précédent dans le corps k.*

En effet, si $P = (x, y, z)$ $z \neq 0$ est une solution de (F) en entiers de k, T.P en est une de (E) en nombres de k. Soit, réciproquement, (r, λ) une solution de (E) en nombres de k.

Selon l'abus de langage habituel en théorie des nombres algébriques, on appellera «*idéaux entiers*» (ou plus simplement *idéaux,* si aucune confusion n'est à craindre) d'un corps k de nombres algébriques, les idéaux $\mathfrak{a}$ de l'anneau des entiers $\mathfrak{J}$ de k. On appellera *idéaux fractionnaires* de k les A-modules f de k pour lesquels existe un $\alpha \in k^*$ tel que $\alpha f \subset \mathfrak{J}$ (on sait que ces idéaux forment un groupe multiplicatif engendré par les idéaux entiers de k).

Soit $(r) = \frac{\mathfrak{a}}{\mathfrak{c}}$ la représentation de l'idéal principal (r) de k sous forme de quotient d'idéaux entiers de ce corps, premiers entre eux. Il existe un entier u de k divisible par $\mathfrak{c}$, et tel que $\frac{(u)}{\mathfrak{c}}$ soit premier à un idéal entier de k fixé d'avance. Alors, $(ur) = \mathfrak{a} \frac{(u)}{\mathfrak{c}}$ est un idéal entier, donc ur est un entier, et le p.g.c.d. (ur, u) de ur et de $u = \mathfrak{c} \frac{(u)}{\mathfrak{c}}$, est $\frac{(u)}{\mathfrak{c}}$. Mais $u(1-r) = u - ur$ est un entier de k, et $(ur,u) = (u-ur,u) = (ur,u-ur)$. Par suite, $(u(1-r)) = \mathfrak{b} \frac{(u)}{\mathfrak{c}}$, où $\mathfrak{b}$ est premier avec $\mathfrak{a}$ et avec $\mathfrak{c}$. Par suite, $(r(1-r)) = \frac{\mathfrak{a}\mathfrak{b}}{\mathfrak{c}^2} = (\lambda \mathfrak{p}) = (\lambda)\mathfrak{p}$. Puisque $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ sont premiers entre eux, il doit exister des idéaux entiers $\mathfrak{r}, \mathfrak{y}, \mathfrak{z}$ de k tels que

$$\mathfrak{a} = \mathfrak{r}^p, \quad \mathfrak{b} = \mathfrak{y}^p, \quad \mathfrak{c} = \mathfrak{z}^p.$$

Par suite, on a $(r) = (\frac{\mathfrak{r}}{\mathfrak{z}})^p$, $(1-r) = (\frac{\mathfrak{y}}{\mathfrak{z}})^p$.

Donc $\mathfrak{r} / \mathfrak{z}$ et $\mathfrak{y} / \mathfrak{z}$ sont des idéaux dont la puissance p-ième est principale. Mais, puisque $h(k) \not\equiv 0 \pmod{p}$, il en résulte qu'ils sont eux-mêmes principaux. Il existe donc des éléments ξ', η' de k tels que $\frac{\mathfrak{r}}{\mathfrak{z}} = (\xi')$ et $\frac{\mathfrak{y}}{\mathfrak{z}} = (\eta')$. Par suite, il existe des unités ϵ_1, ϵ_2 de ce corps, telles que

$$\underline{r = \epsilon_1 \xi'^p}, \quad \underline{1-r = \epsilon_2 \eta'^p}.$$

Mais, en vertu du théorème de Dirichlet, les seules unités de k sont les racines de l'unité qui lui appartiennent. Or, sauf $Q(\sqrt{-3})$, qui contient toutes les racines sixièmes de l'unité - et celles-là seulement -, tous les autres corps quadratiques imaginaires ne contiennent qu'une partie des racines quatrièmes de l'unité. Donc l'exposant de ces racines de l'unité est premier à p, excepté dans le seul cas $[p, k] = [3, Q(\sqrt{-3})]$. Ainsi, sauf dans ce cas, il existe des racines de l'unité

ϵ'_1 ϵ'_2 $\in$ k telles que $\epsilon_1 = \epsilon'^{p}_1$, $\epsilon_2 = \epsilon'^{p}_2$, d'où si l'on pose $\xi = \epsilon'_1 \xi'$, $\eta = \epsilon'_2 \eta'$ il vient :

$$r = \xi^p \quad , \quad 1-r = \eta^p .$$

Mais, dès lors si z est un entier arbitraire de k divisible par $\mathfrak{d}$ et si l'on pose $x = \xi z$, $y = \eta z$, on a d'abord :

$$(x) = \mathfrak{x} \frac{(z)}{\mathfrak{d}} \quad , \qquad (y) = \mathfrak{y} \frac{(z)}{\mathfrak{d}} \quad ,$$

donc x, y, z sont des entiers de k.

Et d'autre part, on a :

$$x^p + y^p = z^p(\xi^p + \eta^p) = z^p(r + 1 - r) = z^p ;$$

avec aussi :

$$r = \xi^p = \frac{x^p}{z^p} \quad , \quad \lambda^p = r(1-r) = \xi^p \eta^p \equiv \left(\frac{xy}{z^2}\right)^p .$$

La dernière égalité montre que $\lambda : \frac{xy}{z^2}$ est une racine $p^{ème}$ de l'unité, et comme k n'en contient aucune autre que 1, on a : $\lambda = \frac{xy}{z^2}$; donc, $\underline{\underline{(r , \lambda) = T.(x,y,z)}}$.

Il est à remarquer qu'on peut choisir z de manière que $\frac{(z)}{\mathfrak{d}}$ soit premier à tout idéal de k fixé d'avance. En particulier, on peut le prendre *premier à p*. Une solution (x, y, z) de (F) est dite «du premier cas» si (xyz, p) = 1. Mais alors, si $(r, \lambda) = T.(x,y,z)$, $\lambda = \frac{xy}{z^2}$ est une p-unité de k. Réciproquement, si une solution (r, λ) de (E) dans k est telle que λ soit une p-unité, l'égalité $\frac{\mathfrak{x}\,\mathfrak{y}}{\mathfrak{d}^2}(\lambda)$, jointe au fait que $\mathfrak{x}$, $\mathfrak{y}$, $\mathfrak{d}$ sont premiers entre eux, montre qu'ils sont tous premiers à p. Si donc, on choisit z de manière que $\frac{(z)}{\mathfrak{d}}$ soit premier à (p), $(x) = \mathfrak{x} \frac{(z)}{\mathfrak{d}}$, $(y) = \mathfrak{y} \frac{(z)}{\mathfrak{d}}$, et $(z) = \mathfrak{d} \frac{(z)}{\mathfrak{d}}$ le sont aussi.

Donc $(r, \lambda) = T.(x,y,z)$, où (x,y,z) est une solution du 1er cas.

Indiquons à présent certains corps quadratiques où l'équation (E) a des solutions telles que λ soit rationnel. Si l'on donne à Λ une valeur rationnelle $\lambda = \frac{u}{v} \neq 0$, par ailleurs quelconque (où u et v sont supposés premiers entre eux), l'équation (E) a des solutions :

$$\Lambda = \lambda , \quad R = r = \frac{1 \pm \sqrt{1-4\lambda^p}}{2} \quad ,$$

dans le corps quadratique $k = Q(\sqrt{1-4\lambda^p}) = Q\left(\sqrt{\frac{v^p - 4u^p}{v^p}}\right)$, qu'on peut mettre

sous la forme $k = Q(\sqrt{m'})$, où, en posant $v = 2^s v' v''^2$, v' désignant le quadratfrei impair qui divise v, on a :

$$m' = \begin{cases} v'(v'^p v''^{2p} - 4u^p), & \text{si } s = 0 \\ 2v'(2^{sp-2} v'^p v''^{2p} - u^p), & \text{si } s \text{ est impair} \\ v'(2^{sp-2} v'^p v''^{2p} - u^p), & \text{si } s > 0 \text{ est pair} \end{cases}$$

Le corps k est quadratique imaginaire si, et seulement si $4\lambda^p > 1$, autrement dit $4u^p > v^p$, et on posera, dans ce cas, $m' = -m$. Si $p = 3$, ce corps est égal à $Q(\sqrt{-3})$, s'il existe un entier rationnel t tel que :

$$m' = -3t^2$$

ce qui arrive, en particulier, si l'on prend $\lambda = 1$.

Supposant que $h(k) \not\equiv 0 \pmod p$, la solution particulière considérée de (E) est la transformée par (T) d'une solution du 1er cas de (F) si, et seulement si λ *est une p-unité,* autrement dit *u et v sont premiers à p.*

Supposons que, k de la forme considérée étant quadratique imaginaire et, pour $p = 3$, distinct de $Q(\sqrt{-3})$, on arrive à démontrer que (F) n'a dans k aucune solution non-triviale. Alors (E) et (F) n'y sont pas équivalentes, *ce qui entraîne* $h(k) \equiv 0 \pmod p$. Si, de plus, λ est une p-unité, il suffit pour obtenir un tel résultat, de prouver que (F) n'a dans k aucune solution du 1er cas. Ceci suggère une méthode pour prouver, pour certains entiers m de la forme précédente, la divisibilité de $h(Q\sqrt{-m})$ par p. M. Krasner a déjà utilisé cette méthode, dans le cas $p = 3$, dans sa note citée. En effet, Fueter avait démontré que si le nombre des classes d'idéaux h(k) d'un corps quadratique imaginaire ne se divise pas par 3, l'équation (F) n'a aucune solution non-triviale dans k. Mais, si $k = Q(\sqrt{1-4\lambda^3}) \neq Q(\sqrt{-3})$, où $\lambda^3 > \frac{1}{4}$, la même hypothèse entraîne que (E), qui possède de telles solutions dans k, est équivalente à (F) dans k. Ceci est absurde, d'où résulte que $h(Q(\sqrt{1-4\lambda^3}) \equiv 0 \pmod 3$.

J'ai appliqué la même idée au cas de $p > 3$ quelconque, mais en me bornant aux $\lambda = \frac{u}{v}$ donnant les solutions de (E) qui sont des transformées par T des solutions de (F) du 1er cas, c'est-à-dire en me limitant aux *u, v premiers à p.* Afin de prouver que, pour certains de ces λ, (F) n'a dans $k = Q(\sqrt{1-4\lambda^p})$ aucune solution du 1er cas, j'ai généralisé aux corps quadratiques imaginaires k tels que $h(k) \not\equiv 0 \pmod p$ la méthode classique «élémentaire» de Sophie Germain, aussi bien sous son ancienne forme explicite de Wendt, que sous la forme plus moderne que lui a donnée M. Krasner (voir «Matematika», t. 16, 1940).

L'idée de la méthode de Sophie Germain - que je vais donner, en me bornant, d'abord, au cas rationnel, où on l'a appliquée primitivement - est, en gros, la suivante :

Soit (x, y, z) une solution du premier cas de (F'), équation déduite de (F) par «symétrisation», dans l'anneau des entiers rationnels Z. Alors, on a, en particulier, si q est un nombre premier quelconque :

$$x^p + y^p + z^p \equiv 0 \pmod q$$

ce qui ne peut avoir lieu que d'une et d'une seule des deux manières suivantes :

(a) - q divise xyz ,

(b) - Φ_q désignant le corps fini de q éléments, et $\bar{x}, \bar{y}, \bar{z}$ désignant les classes des x, y, z (modulo q), $(\bar{x}, \bar{y}, \bar{z})$ est une solution non-triviale de l'équation (F') dans Φ_q.

Ainsi donc, si l'on prouve, pour un certain nombre premier q, les deux hypothèses suivantes :

[A] *L'équation* (F')

$$X^p + Y^p + Z^p = 0$$

n'a aucune solution non-triviale dans Φ_q.

[B] *L'hypothèse* A *étant supposée démontrée, et* (x, y, z) *désignant une solution entière rationnelle de* (F') . *q ne peut diviser* x, y, z.

Cela montre l'inexistence de solutions du premier cas, pour l'équation (F').

Bien entendu, ce n'est que sous certaines conditions que les hypothèses A et B sont vraies pour un couple (p, q) de nombres premiers, et, p étant donné, il n'est pas certain qu'il existe pour lui un tel q. La méthode de Sophie Germain - et ses développements - consiste à formuler des conditions *suffisantes* pour que ces hypothèses soient vraies pour p et q [en ce qui concerne l'hypothèse A, on peut même formuler des conditions nécessaires et suffisantes] , et à les utiliser afin de prouver, pour certains exposants p, le «premier cas du théorème de Fermat», c'est-à-dire l'absence des solutions (x, y, z) de (F') dans Z telles que $xyz \not\equiv 0 \pmod p$. Quand nous appliquerons une méthode analogue dans certains corps quadratiques imaginaires $Q(\sqrt{-m})$, et bien que pour certains d'entre eux la méthode fournisse le critère relatif à certains exposants p, ce n'est pas ce résultat par lui-même qui sera au centre de notre intérêt ; on appliquera les critères ainsi obtenus aux corps quadratiques imaginaires k, où (E) a certainement une solution (r, λ) telle que λ soit une p-unité, ce qui démontrera la non-équivalence, pour p considéré de (E) et de (F) et entraînera la divisibilité par p de h(k).

Revenant à la méthode de Sophie Germain dans le corps rationnel, on remarque d'abord que l'hypothèse A est certainement fausse, si $q \neq 2$, en étant $\not\equiv 1 \pmod p$. En effet, si $q \not\equiv 1 \pmod p$, tout élément de Φ_q est une puissance p-ième ; et si, de plus, $q \neq 2$, il existe trois éléments non-nuls de Φ_q dont la somme est nulle. D'autre part, les méthodes «élémentaires» ne donnent rien non plus, en ce qui concerne l'hypothèse B quand $q = 2$. Ainsi, seul le cas $q \equiv 1 \pmod p$ peut présenter de l'intérêt pour la méthode. Posons donc $q = up + 1$. Ainsi qu'on le verra plus loin, l'hypothèse A est encore fausse si $u \equiv 0 \pmod 3$.

Sophie Germain (selon Legendre) a démontré le critère suivant, pour que B soit vraie relativement au couple $(p, q = up + 1)$:

L'hypothèse B *est vraie pour* $(p, q = up + 1)$ *si* q *ne divise pas* $u^u - 1$.

La démonstration de Sophie Germain est essentiellement appuyée sur les égalités d'Abel du 1er cas, qui consistent dans l'affirmation suivante :

Si (x, y, z) *est une solution de* (F') *dans* Z *telle que* $xyz \not\equiv 0 \pmod p$, *il existe des entiers* u, v, w, u', v', w' *mutuellement premiers, tels que :*

$$x + y = w^p \qquad \frac{x^p + y^p}{x + y} = w'^p \qquad z = -ww'$$

$$y + z = u^p \qquad \frac{y^p + z^p}{y + z} = u'^p \qquad x = -uu'$$

$$z + x = v^p \qquad \frac{z^p + x^p}{z+x} = v'^p \qquad y = -vv'.$$

Sophie Germain a bien formulé l'hypothèse A, mais ni elle, ni Legendre n'ont étudié les conditions de sa validité, et se sont bornés à la prouver pour certains cas simples (cf. le fascicule de Mordell). C'est *Wendt* qui a donné la condition nécessaire et suffisante de sa validité pour un couple (p, up + 1) donné ; cette condition est la non-annulation (mod q) d'un certain déterminant W(u) ne dépendant que de u, et qu'on appellera le déterminant de Wendt. Ce critère ne laisse rien à désirer du point de vue logique, mais est très compliqué et difficile à manier dès que u n'est pas très petit. Krasner a trouvé un certain ensemble de déterminants $R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3)$, $[\epsilon_1^2 = \epsilon_2^2 = \epsilon_3^2 = 1 ; 0 \leq i_1, i_2, i_3 < \frac{u}{2}]$ tels que $W(u) \equiv 0 \pmod q$ équivaille à l'annulation d'un au moins des R. On voit d'ailleurs immédiatement que $u \equiv 0 \pmod 3$ entraîne l'annulation (mod q) de $R(1,1,1,0, \frac{u}{3}, \frac{2u}{3})$. Comme les R peuvent être facilement bornés en fonction de u, il a pu obtenir une condition suffisante beaucoup plus maniable. La partie principale de cette condition est, pour le couple (p, q = up + 1), l'inégalité

$$3^{\frac{u}{4}} < q = up + 1.$$

D'autre part, la condition $u^u \not\equiv 1 \pmod q$ assurant la validité de l'hypothèse B peut être remplacée, dans le corps rationnel, par le critère suivant de *Furtwängler* déduit de la méthode de Kummer :

Si (x, y, z) *est une solution de* (F') *dans* Z *telle que* $xyz \not\equiv 0 \pmod p$ *et si un certain* q *premier divise* xyz, *on a* $q^{p-1} \equiv 1 \pmod{p^2}$, *ce qui, pour* q = up + 1, *équivaut à* $u \equiv 0 \pmod p$.

Ainsi, lorsque $u \not\equiv 0 \pmod p$ et cette condition est automatiquement vérifiée si q = up + 1 premier satisfait la condition indiquée $3^{u/4} < q$, q ne peut pas diviser xyz. Malheureusement, on ne sait pas si le théorème de Furtwängler est vrai dans les corps quadratiques imaginaires, ce qui empêche de remplacer le critère de Sophie Germain par ce théorème.

Pour généraliser la méthode de Sophie Germain au cas du corps quadratique imaginaire $R = Q(\sqrt{-m})$, en supposant que $h(k) \not\equiv 0 \pmod p$ et que k ne contient aucune racine p-ième de l'unité autre que 1, il y a lieu de remplacer les solutions (x, y, z) de

$$(F') \qquad X^p + Y^p + Z^p = 0$$

dans Z, par ses solutions dans l'anneau des entiers $\mathfrak{J}$ de k, et la condition $xyz \not\equiv 0 \pmod p$ par l'hypothèse que xyz est premier à p. Ensuite, au lieu de considérer la congruence

$$x^p + y^p + z^p \equiv 0 \pmod q,$$

où q est un nombre premier, il y a lieu de considérer la même congruence (mod $\mathfrak{q}$), où $\mathfrak{q}$ est un idéal premier de $\mathfrak{J}$. Si $N(\mathfrak{q})$ désigne la «norme-absolue» de $\mathfrak{q}$, l'hypothèse A se remplace par celle de la non-existence des solutions non-triviales de (F') dans $\Phi_{N(\mathfrak{q})}$. On a vu que, pour que ceci puisse avoir lieu, on doit avoir $N(\mathfrak{q}) = 2$ ou $N(\mathfrak{q}) = up + 1$, où $u \not\equiv 0 \pmod 3$. Or, si q est le premier rationnel divisible par $\mathfrak{q}$, on a $N(\mathfrak{q}) = q$ ou q^2, selon que (q) se décompose dans $\mathfrak{J}$ en produit de deux idéaux premiers (distincts ou non) $\mathfrak{q}\,\mathfrak{q}'$ (autrement dit, q se ramifie ou se décompose dans k/Q) ou est lui-même premier dans $\mathfrak{J}$. Or, si $q \neq 3$, on a $q^2 \equiv 1 \pmod 3$, et $3^2 - 1 = 8$ ne se

divise par aucun premier impair p. Ainsi, sauf le cas p = 3, déjà liquidé par Fueter, *l'hypothèse est fausse pour* $\Phi_{N(\mathfrak{q})}$ si $N(\mathfrak{q}) = q^2$, et on peut se borner au cas où $q = N(\mathfrak{q}) = up + 1$ $\{u \not\equiv 0 \pmod 3\}$ se décompose ou se ramifie dans k/Q. d étant le discriminant de $k/Q = Q(\sqrt{-m})/Q$, ceci a lieu si et si respectivement $(\frac{d}{q})$ (symbole de Legendre) est + 1/ ou q divise d. L'étude de la validité de l'hypothèse A pour un tel q est la même que dans le cas k = Q, mais la démonstration obtenue n'entraîne la non-existence des solutions non-triviales (mod $\mathfrak{q}$) de (F'), que si $(\frac{d}{q}) =$ + 1 ou $q \mid d$.

En ce qui concerne l'hypothèse B, et bien que le résultat de Sophie Germain reste vrai tel quel en substituant $k = Q(\sqrt{-m})$ à Q, la démonstration du cas rationnel doit être modifiée plus profondément pour pouvoir s'appliquer à ce cas plus général. Généralisons d'abord les égalités d'Abel du 1er cas.

Soit (x, y, z) une solution de (F') dans $Q(\sqrt{-m})$, telle que xyz soit premier à p. Si $\mathfrak{d} = (x, y)$ est le p.g.c.d. de (x) et de (y), $z^p = -(x^p + y^p)$ montre que $(z^p) = (z)^p$ se divise par $\mathfrak{d}^p$, donc (z) se divise par $\mathfrak{d}$, et $\mathfrak{d} = (x,y)$ divise (z, x). Comme x, y,z jouent des rôles symétriques, il en résulte que

$$\mathfrak{d} = (x, y) = (y, z) = (z, x) \quad \text{et que :}$$

$$(x) = \mathfrak{d}\mathfrak{x} \quad , \quad (y) = \mathfrak{d}\mathfrak{y} \quad , \quad (z) = \mathfrak{d}\mathfrak{z}$$

où $\mathfrak{x}$, $\mathfrak{y}$, $\mathfrak{z}$ sont des idéaux premiers entre eux deux à deux.

De plus, ces idéaux et également $\mathfrak{d}$, sont premiers à p. On a

$(-z)^p = (x + y)\ \frac{x^p + y^p}{x+y}$; $x + y$ se divise par $\mathfrak{d}$ et $\frac{x^p + y^p}{x+y} = \sum (-1)^i x^{p-1-i} y^i$ se divise par $\mathfrak{d}^{p-1}$. On a donc, si $(x + y) = \mathfrak{d}\mathfrak{w}$ et $(\frac{x^p + y^p}{x + y}) = \mathfrak{d}^{p-1}\mathfrak{w}'$,

$$\mathfrak{z}^p = \mathfrak{w}\mathfrak{w}'$$

Or, on a :

$(-1)^i x^{p-1-i} y^i - x^{p-1} = -x^{p-1-i} \frac{x^i - (-y)^i}{x-(-y)} (x+y)$, et cette dernière quantité est congrue à 0 modulo $(x)^{p-1-i}(x,y)^{i-1}(x+y)$, donc aussi (mod $\mathfrak{d}^{p-1-i}\,\mathfrak{d}^{i-1}(\mathfrak{d}\mathfrak{w})$), c'est-à-dire (mod $\mathfrak{d}^{p-1}\mathfrak{w}$). Par suite $\frac{x^p + y^p}{x+y} \equiv px^{p-1} \pmod{\mathfrak{d}^{p-1}\mathfrak{w}}$.

Par suite, puisque tout diviseur commun de $\mathfrak{w}$ et $\mathfrak{w}'$ divise $(\mathfrak{d}^{p-1})^{-1}(\frac{x^p + y^p}{x+y})$ et $(\mathfrak{d}^{p-1})^{-1}\,\mathfrak{d}^{p-1}\mathfrak{w}$, il doit diviser aussi $(\mathfrak{d}^{p-1})^{-1}(px^{p-1}) = (p)\,\mathfrak{x}^{p-1}$ et $\mathfrak{z}^p = \mathfrak{w}\mathfrak{w}'$.

Or, par hypothèse, $\mathfrak{w}$ est premier à $\mathfrak{x}$ et (p). Donc le p.g.c.d. de $\mathfrak{w}$ et $\mathfrak{w}'$ est (1). Par suite, il existe des idéaux $\mathfrak{w}$ et $\mathfrak{w}'$ premiers entre eux tels que :

$$\mathfrak{z} = \mathfrak{w}\mathfrak{w}' \qquad \mathfrak{w} = \mathfrak{w}^p \qquad \mathfrak{w}' = \mathfrak{w}'^p$$

donc :

$$(x+y) = \mathfrak{h}\,\mathfrak{w}^p \quad , \left(\frac{x^p+y^p}{x+y}\right) = \mathfrak{d}^{p-1}\,\mathfrak{w}'^p \quad \mathfrak{z} = \mathfrak{w}\,\mathfrak{w}'$$

$$(y+z) = \mathfrak{d}\,\mathfrak{u}^p \quad , \left(\frac{y^p+z^p}{y+z}\right) = \mathfrak{h}^{p-1}\,\mathfrak{u}'^p \quad \mathfrak{x} = \mathfrak{u}\,\mathfrak{u}'$$

$$(z+x) = \mathfrak{h}\,\mathfrak{v}^p \quad , \left(\frac{z^p+x^p}{z+x}\right) = \mathfrak{d}^{p-1}\,\mathfrak{v}'^p \quad \mathfrak{y} = \mathfrak{v}\mathfrak{v}'$$

où $\mathfrak{v}^{(')}$ et $\mathfrak{u}^{(')}$ désignent les idéaux jouant un rôle analogue pour $\{y, z\}$ et $\{z, x\}$.

Supposons maintenant qu'un idéal premier $\mathfrak{q}$ dont la norme $q = N(\mathfrak{q})$ est un premier de la forme $up + 1$, soit tel que l'hypothèse A soit vraie pour le couple (p, q). Si $\mathfrak{q}$ divise $\mathfrak{h}$, soit, d'une part, ξ un entier de k divisible par $\mathfrak{d}$ et, d'autre part, η un entier de k divisible par $(\xi) / \mathfrak{h}$ et tel que $(\eta)\left[\frac{(\xi)}{\mathfrak{d}}\right]^{-1}$ soit premier à p et $\mathfrak{q}$.

Alors :

$$(x', y', z') = \left(\frac{\eta}{\xi}x, \frac{\eta}{\xi}y, \frac{\eta}{\xi}z\right)$$

est encore une solution de (F') dans $\mathfrak{J}$.

$$\left[\text{car } \left(\frac{\eta}{\xi}x\right) = (\eta)\left[\frac{(\xi)}{\mathfrak{d}}\right]^{-1} \quad \mathfrak{d}^{-1} \quad (\mathfrak{h}\mathfrak{x}) = \left\{(\eta)\left[\frac{(\xi)}{\mathfrak{d}}\right]^{-1}\right\}\mathfrak{x}\right.$$

est un idéal entier, et, de même, $\left(\frac{\eta}{\xi}y\right)$ et $\left.\left(\frac{\eta}{\xi}z\right)\right]$ et, si $\mathfrak{d} = (x, y) = (y, z) = (z, x)$ est premier à $\mathfrak{q}$ et si $(xyz, (p)) = 1$, alors $\mathfrak{d}' = (x', y') = (y', z') = (z', x') = (\eta)\left(\left[\frac{(\xi)}{\mathfrak{d}}\right]\right)^{-1}$ est premier à p et à $\mathfrak{q}$. Ainsi, on peut supposer qu'il existe une solution de (F') dans $\mathfrak{J}$ première à (p) et à $\mathfrak{q}$, et on va prendre comme (x, y, z) une telle solution.

Ceci étant, la congruence $x^p + y^p + z^p \equiv 0 \pmod{\mathfrak{q}}$ entraîne, puisque $\mathfrak{d}$ est premier à $\mathfrak{q}$ et puisque l'hypothèse A est vraie, que $\mathfrak{q}$ divise un, et un seul, des x, y, z.
Supposons, pour fixer les idées, que $z \equiv 0 \pmod{\mathfrak{q}}$.
Alors $\mathfrak{q}$ divise $z = \mathfrak{d}\,\mathfrak{w}\,\mathfrak{w}'$, et comme $\mathfrak{q}$ ne divise pas $\mathfrak{d}$, ou bien $\mathfrak{q}$ divise $\mathfrak{w}'$ sans diviser $\mathfrak{w}$ ou bien $\mathfrak{q}$ divise $\mathfrak{w}$. On a, d'autre part :

$$\begin{cases} y \equiv y + z \\ x \equiv x + z \end{cases} \pmod{\mathfrak{q}}$$

Supposons que θ soit un élément de $\mathfrak{J}$ divisible par $\mathfrak{w}$ et tel que $\frac{(\theta)}{\mathfrak{w}}$ soit premier à $\mathfrak{q}$.
Alors, si $\alpha = \frac{\theta^p}{x+y}$, on a $\alpha(x+y) = \theta^p$, avec $(\alpha(y+z)) = (\theta)^p \frac{(y+z)}{(x+y)} = \left(\theta\frac{\mathfrak{u}}{\mathfrak{h}}\right)^p$ et $(\alpha(z+x)) = (\theta)^p \frac{(z+x)}{(x+y)} = \left(\theta\frac{\mathfrak{v}}{\mathfrak{w}}\right)^p \cdot \left(\theta\frac{\mathfrak{u}}{\mathfrak{w}}\right)$ et $(\theta)\frac{\mathfrak{v}}{\mathfrak{w}}$ sont donc des idéaux fractionnaires de k dont la puissance p-ième est principale, et dont le numérateur et dénominateur sont premiers à $\mathfrak{q}$. Puisque $h(k) \not\equiv 0 \pmod{p}$, il existe des $\mathfrak{q}$-unités φ et ψ de k telles que

$(\theta)\frac{\upsilon}{\pi} = (\varphi), (\theta)\frac{\mathfrak{b}}{\mathfrak{w}} = (\psi)$. On a donc $\alpha(y+z) = \epsilon' \varphi^p$ et $\alpha(z+x) = \epsilon'' \psi^p$.

Et comme toute unité de k est une racine de l'unité et, par hypothèse, k ne contient aucune racine de l'unité d'exposant p, ϵ' et ϵ'' sont les puissances p-ièmes d'autres unités de k. Donc, on peut choisir φ et ψ de la forme précédente de manière que :

$$\alpha(y+z) = \varphi^p \quad , \quad \alpha(z+x) = \psi^p.$$

Supposons d'abord que $\mathfrak{q}$ divise $\mathfrak{w}'$, donc ne divise pas $\mathfrak{w}$. Alors, puisque $(\theta) = \mathfrak{w}\frac{(\theta)}{\mathfrak{w}}$ est premier à $\mathfrak{q}$, et puisque :

$(-\theta)^p + \psi^p + \varphi^p = -\alpha(x+y) + \alpha(y+z) + \alpha(z+x) = +2\alpha z \equiv 0 \pmod{\mathfrak{q}}$

$(\varphi, \psi, (-\theta))$ est une solution non-triviale de (F') (mod $\mathfrak{q}$), contrairement à l'hypothèse A.

Supposons maintenant que $\mathfrak{q}$ divise $\mathfrak{w}$. Alors :

$\frac{x^p + y^p}{x+y} \equiv px^{p-1} \pmod{(x+y)}$, donc (mod $\mathfrak{q}$). Par conséquent :

$$\alpha^{p-1}\frac{x^p + y^p}{x+y} \equiv p(\alpha x)^{p-1} \equiv p[\alpha(x+z)^{p-1}] \equiv p\psi^{p(p-1)} \pmod{\mathfrak{q}}.$$

Or, on a :

$$(\alpha)^{p-1}\frac{x^p + y^p}{x+y}\frac{(\theta)^{p(p-1)}}{(x+y)^{p-1}}\frac{(-z)^p}{(x+y)} = \left(-\frac{\theta^{p-1}z}{x+y}\right)^p.$$

Comme α et ψ sont des $\mathfrak{q}$-unités [et il en est de même pour $\frac{x^p + y^p}{x+y}$, car $(\frac{x^p + y^p}{x+y}) = \mathfrak{b}^{p-1}\mathfrak{w}'^p$ est un idéal entier premier à $\mathfrak{q}$], $\lambda = -\frac{\theta^{p-1}z}{\psi^{p-1}(x+y)}$ en est encore une.

Par suite, on a $p \equiv \lambda^p \pmod{\mathfrak{q}}$.

Comme $up \equiv 1 \pmod{\mathfrak{q}}$, i.e. $u \equiv p^{-1} \pmod{\mathfrak{q}}$, on a :

$$u \equiv \lambda^{-p} \equiv \left(-\frac{\psi^{p-1}(x+y)}{\theta^{p-1}z}\right)^p \pmod{\mathfrak{q}}.$$

Or, ceci entraîne :

$$u^u \equiv (\lambda^{-p})^u \equiv \lambda^{-up} \equiv \lambda^{q-1} \equiv 1 \pmod{\mathfrak{q}}.$$

Comme $u^u - 1 \in Z$, ceci implique la congruence $\underline{u^u \equiv 1 \pmod{q}}$.

Ainsi on a le critère de Sophie Germain.

Si l'hypothèse A *est vraie pour* $q = up + 1$, *et si* $u^u \not\equiv 1 \pmod{q}$ *l'hypothèse* B *est vraie pour le couple* (p, q).

Pour terminer, je vais rappeler (bien que ce ne soit pas nouveau) comment la validité de l'hypothèse A est étudiée par les méthodes de Wendt et de Krasner. A la base des deux méthodes se trouvent les considérations générales suivantes :

Soient : $f(T) = \sum_{i=0}^{n} a_i T^i$, $g(T) = \sum_{j=0}^{m} b_j T^j$, deux polynômes de degrés effectifs

n, m à coefficients dans un corps L et soit $\mathfrak{L}$ la clôture algébrique de L.
Soient $\alpha_1, \alpha_2, ..., \alpha_n$ et $\beta_1, ..., \beta_m$ les zéros (comptés selon leur multiplicité) de f(T) et de g(T) dans $\mathfrak{L}$. On appelle *résultant* (par rapport à T) des polynômes f(T), g(T) l'expression :

$$R[f(T),g(T)] = \pm a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) = \pm b_m^n \prod_{j=1}^{m} f(\beta_j) = a_n^m \prod_{i=1}^{n} g(\alpha_i).$$

(où $\pm$ est un signe convenablement choisi, qui ne nous intéresse pas). Si l'on considère L et $\mathfrak{L}$/L comme des Z-algèbres [en posant, pour tout $z \in Z$ et $\alpha \in \mathfrak{L}$, $z.\alpha = \alpha + \alpha \ ... + \alpha$ (z fois)] $R[f(T), g(T)]$ se représente,
en fait, comme un polynôme à coefficients entiers par rapport aux coefficients a_i et b_j des f(T) et g(T), indépendant du choix de $\mathfrak{L}$. Il est visible que f et g ont un zéro commun dans $\mathfrak{L}$ si, et seulement si $R[f(T), g(T)] = 0$.

Si f et g sont des polynômes à coefficients dans un anneau $\mathfrak{I}$, soient $\mathfrak{p}$ un idéal premier de $\mathfrak{I}$, $\overline{\mathfrak{I}} = \mathfrak{I}/\mathfrak{p}$ l'anneau quotient intègre de $\mathfrak{I}$ par $\mathfrak{p}$. Supposons, en outre, que les restes $\overline{a_n}$ et $\overline{b_m}$ des a_n et b_m ne soient pas nuls dans $\overline{\mathfrak{I}}$. Alors, $R[f(T), g(T)]$ et $R[\bar{f}(T), \bar{g}(T)]$ sont des polynômes de même forme par rapport aux coefficients homologues de f(T), g(T) et de $\bar{f}(T), \bar{g}(T)$, dont les coefficients sont des opérateurs $\in Z$. Il en résulte que $R[f(T), g(T)]$ appartient à $\mathfrak{I}$ et que $R[\bar{f}(T), \bar{g}(T)] \equiv \overline{R[f(T), g(T)]} \pmod{\mathfrak{p}}$. D'un autre côté, si f(T) est unitaire, la manière la plus simple de calculer $R[f(T), g(T)]$ est la suivante :

n étant le degré de f(T), posons

$$T^{i-1} g(T) = \sum_{j=1}^{n-1} c_{i,j} T^{j-1} \pmod{f(T)} \quad (i = 1,2,...,n).$$

Alors $R[f(T), g(T)] = \pm$ dét $(c_{i,j})$. En effet, on voit directement que si f(T) et g(T) ont un zéro commun $z \neq 0$, on a le système d'équations :

$$\sum_{j=1}^{n-1} c_{ij} Z^{j-1} = 0 \quad (i = 1,...,n),$$ ce qui entraîne dét $(c_{i,j}) = 0$. Si $f(0) = g(0) = 0$, on a $c_{ij} = 0$ pour tout i = 1,2,...,n, donc encore dét $c_{ij} = 0$. Ceci implique que dét (c_{ij}) se divise par $R[f(T), g(T)]$, et la comparaison des degrés montre leur égalité.

Soit $\psi = \psi_q$ la clôture algébrique du corps Φ_q de q éléments où $q = up + 1$. On sait que les éléments non-nuls $x \in \Phi_q$ sont caractérisés parmi ceux de Ψ par l'égalité $(x^p)^u = x^{q-1} = 1$. Supposons que (F') ait dans ϕ_q une solution non-triviale (x, y, z). Alors, si $x' = \frac{x}{z}$, $y' = \frac{y}{z}$ (1, x', y') en est une autre. Si l'on pose $\xi = x'^p$, $\eta = y'^p$, on obtient le système :

$$\begin{cases} 1 + \xi + \eta = 0 \\ \xi^u - 1 = 0 \\ \eta^u - 1 = 0 \end{cases}$$

système qui équivaut à :

$$\begin{cases} \xi^u - 1 = 0 \\ \xi^u + \sum_{1}^{u-1} \binom{u}{i} \xi^{u-i} = (\xi+1)^u - 1 = 0 \\ \eta = -(1+\xi) \end{cases}$$

Supposons que $f(T) = T^u - 1$, et $g(T) = (T+1)^u - 1$ aient un zéro commun ξ dans ψ. Alors, puisque les équations $\eta = -1-\xi$, $x'^p = \xi$, $y'^p = \eta$ sont résolubles dans ψ, on a $x'^{q-1} = (x'^p)^u = \xi^u = 1$, et $\eta'^{q-1} = (-(1+\xi))^u = 1$ (car u est pair), ce qui montre que $(1, x', y')$ est une solution de (F') dans ϕ_q.

Par suite, *si* $W(u) = R[(T^u - 1), (T+1)^u - 1]$, *l'hypothèse* A *est vraie si et seulement si* W(u) *est nul* (on y considère $T^u - 1$ et $(T+1)^u - 1$ comme des polynômes $\in \phi_q[T]$) ; ou, ce qui revient au même, si, $T^u - 1$ et $(T+1)^u - 1$ étant considérés comme polynômes dans Z(T), $W(u) \equiv 0 \pmod q$.

Or, il est visible que W(u) est la circulante : $W(u) = \det(c_{ij}) = \binom{u}{(j-i)^*}$, où $(s)^*$ désigne le plus grand reste non négatif de s (mod q). On obtient ainsi le résultat suivant :

Si $k = Q(\sqrt{-m})$ *est quadratique imaginaire, si* d *est le discriminant de* k/Q *, et si, pour le premier* p *, il existe un premier* $q = up + 1$ *tel que :*

1) q *ne divise pas* W(u) (ceci exige $u \not\equiv 0 \pmod 3$)
2) q *ne divise pas* $u^u - 1$
3) $\left(\frac{d}{q}\right) = +1$, *ou* q *divise* d,

l'équation $X^p + Y^p + Z^p = 0$ *n'a pas de solution* (x, y, z) *dans l'anneau des entiers* de k, *telle que* xyz *soit premier à* p.

En particulier, si m est de la forme indiquée plus haut, entraînant l'existence de telles solutions quand (E) $\sim$ (F), on doit avoir $h(k) \equiv 0 \pmod p$.

Le critère de Wendt est tout à fait complet, mais peu maniable à cause de la complication de la fonction W(u). M. Krasner a eu l'idée de la décomposer comme suit en facteurs plus simples. Soit ρ une racine primitive (mod q), et, $\rho' = \rho^p$. Alors ρ' est un non-reste quadratique (mod q), donc satisfait à l'équation

$$\rho^{\frac{u}{2}} = (\rho^p)^{\frac{u}{2}} = \rho^{\frac{up}{2}} = \rho^{\frac{q-1}{2}} \equiv -1 \pmod q.$$

D'autre part, il existe, visiblement, des entiers rationnels $\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3$ tels que $\epsilon_1^2 = \epsilon_2^2 = \epsilon_3^2 = 1, 0 \le i_1, i_2, i_3 < \frac{u}{2}$ de manière que, considérant ρ' comme un élément de ϕ_q, on ait, pour tous $x, y, z \in \phi_q^*$,

$$x^p = \epsilon_1 \rho'^{i_1}, y^p = \epsilon_2 \rho'^{i_2}, z^p = \epsilon_3 \rho'^{i_3}$$

Si (x, y, z) annule $x^p + y^p + z^p$, on doit avoir

$$\epsilon_1 \rho'^{i_1} + \epsilon_2 \rho'^{i_2} + \epsilon_3 \rho'^{i_3} = 0.$$

Ainsi les polynômes

$$\begin{cases} T^{\frac{u}{2}} + 1 \\ \text{et} \\ c_1 T^{i_1} + c_2 T^{i_2} + c_3 T^{i_3} \end{cases}$$

ont un zéro commun ρ'. Réciproquement, si ρ' est un zéro commun de ces deux polynômes, on a $\rho'^{u/2} = -1$, donc $\rho'^{u} = 1$, ce qui entraîne l'existence d'un $\rho \in \phi_q$ tel que $\rho' = \rho^p$, d'où il résulte, si l'on pose

$$x = \epsilon_1 \rho^{i_1}, \; y = \epsilon_2 \rho^{i_2}, \; z = \epsilon_3 \rho^{i_3} : x^p + y^p + z^p = 0.$$

Ainsi, si A est faux, pour un certain choix des (ϵ_i, i_j)

$$R_{\epsilon_1,\epsilon_2,\epsilon_3,i_1,i_2,i_3} = R\left[T^{\frac{u}{2}} + 1, \; \epsilon_1 T^{i_1} + \epsilon_2 T^{i_2} + \epsilon_3 T^{i_3}\right],$$

où les deux polynômes sont considérés comme appartenant à $\phi_q[T]$, doit être nul, et réciproquement, si un certain R_i est nul, A est faux.

Or, on peut considérer les polynômes comme éléments de $Z[T]$, auquel cas le résultat précédent devient :

L'hypothèse A est vraie si, et seulement si, pour tout choix possible des (ϵ_i, i_j), on a

$$R_{\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3} \not\equiv 0 \pmod{q}.$$

Or, sous cette forme,

$$R_{\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3} = \prod_{\eta} (\epsilon_1 \eta^{i_1} + \epsilon_2 \eta^{i_2} + \epsilon_3 \eta^{i_3}),$$

où η parcourt les racines $u^{\text{èmes}}$ de l'unité telles que $\eta^{\frac{u}{2}} \neq 1$. Chaque facteur est, dans le plan complexe, la somme de trois racines de l'unité, dont la somme ne peut être nulle que si elles forment un triangle équilatéral. Ceci n'arrive, pour un certain choix des (ϵ_i, i_j), que si $u \equiv 0 \pmod 3$, et arrive effectivement dans ce cas, ce qui montre que $W(u) = 0 \Leftrightarrow u \equiv 0 \pmod 3$.

Ce cas étant exclu, calculons $R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3)$ dans tous les cas qui peuvent se présenter.

1) Supposons que $i_1 = i_2 = i_3$.

Notons i la valeur commune de ces nombres. On a :

$\epsilon_1 T^{i_1} + \epsilon_2 T^{i_2} + \epsilon_3 T^{i_3} = (\epsilon_1 + \epsilon_2 + \epsilon_3) T^i$, et $\epsilon_1 + \epsilon_2 + \epsilon_3$ a une des quatre valeurs ± 1, ± 3. Par suite, $\prod_{\eta} (\epsilon_1 \eta^{i_1} + \epsilon_2 \eta^{i_2} + \epsilon_3 \eta^{i_3})$ (où η parcourt les zéros de $T^{\frac{u}{2}} + 1$) est égal à $(\epsilon_1 + \epsilon_2 + \epsilon_3)^{\frac{u}{2}} (\prod \eta)^i = [(-1)^i (\epsilon_1 + \epsilon_2 + \epsilon_3)]^{\frac{u}{2}}$, car $\prod_{\eta} \eta = (-1)^{\frac{u}{2}}$.

Ainsi, $R(\epsilon_1, \epsilon_2, \epsilon_3, i, i, i)$ n'a pas d'autre diviseur premier que 3, donc ne se divise pas par le premier $q > p > 3$.

2) Supposons que $i_1 = i_2 \neq i_3$, et notons i la valeur commune de i_1 et i_2.

Alors, $\epsilon_1 T^{i_1} + \epsilon_2 T^{i_2} + \epsilon_3 T^{i_3} = -\epsilon_3 T^{i}[-\epsilon_3(\epsilon_1 + \epsilon_2) - T^{i_3-i}]$ d'où

$$\prod_{\eta}(\epsilon_1 \eta^{i_1} + \epsilon_2 \eta^{i_2} + \epsilon_3 \eta^{i_3}) = (\prod_{\eta}(-\epsilon_3 \eta^{i}))(\prod_{\eta}[-\epsilon_3(\epsilon_1 + \epsilon_2) - \eta^{i_3-i}]) =$$

$$[(-1)^{i+1}\epsilon_3]^{\frac{u}{2}} \prod_{\eta}[-\epsilon_3(\epsilon_1 + \epsilon_2) - \eta^{i_3-i}] .$$

Soit Δ le p.g.c.d. de i_3-i et de u. Alors, si Δ est impair, η^{i_3-i} parcourt Δ fois les zéros de $T^{\frac{u}{2}\Delta} + 1$, et, si Δ est pair, η^{i_3-i} parcourt $\frac{\Delta}{2}$ fois les zéros de $T^{\frac{u}{\Delta}} - 1$. Par suite,

$$\prod_{\eta}[-\epsilon_3(\epsilon_1 + \epsilon_2) - \eta^{i_3-i}] = \begin{cases} [(-\epsilon_3(\epsilon_1 + \epsilon_2))^{\frac{u}{2\Delta}} + 1]^{\Delta} & \text{, si } \Delta \text{ est impair} \\ [(-\epsilon_3(\epsilon_1 + \epsilon_2))^{\frac{u}{\Delta}} - 1]^{\frac{\Delta}{2}} & \text{, si } \Delta \text{ est pair.} \end{cases}$$

Comme $-\epsilon_3(\epsilon_1 + \epsilon_2)$ ne peut prendre que les valeurs 0 ou ± 2, le produit précédent ne peut prendre que les valeurs ± 1, $[(\pm 2)^{\frac{u}{2\Delta}} + 1]^{\Delta}$, et $[(\pm 2)^{\frac{u}{\Delta}} - 1]^{\frac{\Delta}{2}}$, qui divisent toutes une puissance de $2^u - 1$. Par ailleurs, si $-\epsilon_3(\epsilon_1 + \epsilon_2) = 1$, le produit précédent est $2^{\frac{u}{2}} + 1$ quand $\Delta = 1$ et $2^{\frac{u}{2}} - 1$ quand $\Delta = 2$, ce qui montre que, par exemple,

$$\prod_{i=1}^{\frac{u}{2}-1}(\prod_{\eta}(2 - \eta^{i})) \equiv 0 \pmod{2^u - 1}.$$

Ainsi, aucun des $R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3)$ n'est divisible par q si, et seulement si $2^u \not\equiv 1 \pmod{q}$.

3) Supposons que i_1, i_2, i_3 soient tous différents.

Posons, pour $1 \leq i \leq \frac{u}{2}$:

$$T^{i-1}(\epsilon_1 T^{i_1} + \epsilon_2 T^{i_2} + \epsilon_3 T^{i_3}) \equiv \sum_{j=1}^{u/2} c_{ij} T^{j-1} \pmod{T^{\frac{u}{2}} + 1}.$$

Alors, comme on a vu,

$$R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3) = \det(c_{ij}).$$

Or, si $0 \leq i-1, i_1, i_2, i_3 < \frac{u}{2}$, on a

$$0 \leq i-1 + i_1, i-1 + i_2, i-1 + i_3 < u.$$

Par suite, $T^{i-1+i_q} \equiv -T^{i-1+i_q-\frac{u}{2}} \pmod{T^{\frac{u}{2}} + 1}$, et si $\frac{u}{2} \leq i-1 + i_q < u$, on a

$0 \leq i\text{-}1 + i_q - \frac{u}{2} < \frac{u}{2}$. Par suite :

$\sum_{j=1}^{n} c_{ij} T^{j-1} = \epsilon'_{1,i} T^{j_1(i)-1} + \epsilon'_{2,i} T^{j_2(i)-1} + \epsilon'_{3,i} T^{j_3(i)-1}$, où selon que $i\text{-}1+ i_q$ soit

$< \frac{u}{2}$ ou $\geq \frac{u}{2}$, on a respectivement :

$$\begin{cases} \epsilon'_{q,i} = \epsilon_i \\ j_q(i) = i_q + i \end{cases} \qquad \text{ou} \qquad \begin{cases} \epsilon'_{q,i} = -\epsilon_i \\ j_q(i) = i_q + i - \frac{u}{2} \end{cases}$$

Finalement, $R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3) =$ dét (c_{ij}) est le déterminant de la forme :

$$\begin{vmatrix}
0 & & & & i_1+1 & & & & i_2+1 & & & i_3+1 & & & \frac{u}{2} \\
0 & & & & 0 & \epsilon_1 & 0 & & 0 & \epsilon_2 & & 0 & \epsilon_3 & 0 & 0 \\
 & 0 & & & & \epsilon_1 & & & & \epsilon_2 & & & & & \\
 & & 0 & & & & \epsilon_1 & & & & \epsilon_2 & & & & \epsilon_3 \\
0 & & & 0 & & & & \epsilon_1 & & & & \epsilon_1 & & & \\
-\epsilon_3 & & & & 0 & & & & \epsilon_1 & & & & & & \\
0 & -\epsilon_3 & & & & 0 & & & & \epsilon_1 & & & & 0 & \epsilon_2 \\
 & & -\epsilon_3 & & & & & & & & \epsilon_1 & & & & \\
0 & & & & & & & & & & & \epsilon_1 & & & \\
-\epsilon_2 & & & & & & & & & & & & & & \\
 & -\epsilon_2 & & & & & & & & & & & & & \\
 & & -\epsilon_2 & & & & & & & & & & & & \\
 & & & -\epsilon_2 & & & & & & & & & & & \\
 & & & & 0 & -\epsilon_2 & 0 & 0 & 0 & -\epsilon_3 & 0 & 0 & 0 & 0 & 0 & \epsilon_1 \\
0 & 0 & & & 0 & 0 & -\epsilon_2 & 0 & & 0 & & -\epsilon_3 & & & 0 & 0 \\
-\epsilon_1 & 0 & & & & & & & & & & & & & \\
0 & -\epsilon_1 & & & & & & & & & & & & & \\
0 & 0 & -\epsilon_1 & & & & & & & & & & & 0 & \\
0 & 0 & 0 & -\epsilon_1 & & & & & & & & & & & \\
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & \\
 & & & & & & & & & & & & & & 0
\end{vmatrix}$$

Ce déterminant admet trois éléments non-nuls sur la première ligne :

$$c_{1,i_1+1} = \epsilon_1 \; ; \; c_{1,i_2+1} = \epsilon_2 \; ; \; c_{1,i_3+1} = \epsilon_3 .$$

Il ne diffère de la circulante que par le fait que les éléments changent leur signe en passant de la dernière colonne à la première. Or, d'après la formule d'Hadamard :

$$|\text{dét}\,(c_{ij})| \leq \prod_i \left(+ \sqrt{\sum_j |c^2_{ij}|} \right)$$

Dans le cas présent, pour tout $i = 1,2,\ldots, \frac{u}{2}$, tous les c_{ij} sont nuls sauf trois, qui ont les valeurs ± 1. Par suite, $\sum |c^2_{ij}| = 3$, et on a :

$$|R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3)| \leq \prod_{i=1}^{\frac{u}{2}} 3^{\frac{1}{2}} = 3^{\frac{u}{4}}$$

Ainsi, si $u \not\equiv 0 \pmod 3$ [ce qui exclut la valeur 0 pour tout R] et si $3^{u/4} < q$, aucun des entiers $R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3)$, où les i_1, i_2, i_3 sont tous différents, ne peut se diviser par q.

Ceci conduit au résultat suivant :

Si, pour un nombre premier p *donné, il existe un nombre premier* q *de la forme* $up + 1$ *tel que*

1) $u \not\equiv 0 \pmod 3$

2) $2^u \not\equiv 1 \pmod q$

3) $3^{u/4} < q = up + 1$

4) $u^u \not\equiv 1 \pmod q$

et si $k = Q(\sqrt{-m})$ *est quadratique imaginaire tel que* d *étant son discriminant, on ait* $(\frac{d}{q}) = +1$ *ou* q *divise* d , *l'équation* $X^p + Y^p + Z^p = 0$ *n'a pas de solution* (x,y,z) *dans l'anneau des entiers de* k , *telle que* xyz *soit premier à* p.

Il en résulte, en particulier, que si m est, en outre, de la forme indiquée au début du travail, on a, sous les conditions précédentes, $h(k) \equiv 0 \pmod p$.

Dans la seconde partie de ce travail, nous appliquerons les critères de Wendt et Krasner à la caractérisation de certains corps quadratiques imaginaires $k = Q(\sqrt{-m})$, dont le nombre des classes d'idéaux h(k) est divisible par un nombre premier $p > 3$.

§ 0 - Rappels - Notations.

L'équation d'Euler est définie par l'égalité

$$(E) : \quad R(1-R) = \wedge^p ;$$

si nous donnons à $\wedge$ une valeur rationnelle $\lambda = u/v$, où u et v sont deux entiers rationnels non-nuls et premiers entre eux, on obtient une équation aux R, qui admet pour solutions :

$$R = r = \frac{1 \pm \sqrt{1 - 4\lambda^p}}{2}$$

dans le corps quadratique $k = Q(\sqrt{1-4\lambda^p}) = Q(\sqrt{\frac{v^p - 4u^p}{v^p}})$. Celui-ci est imaginaire si $1 < 4\lambda^p$, c'est-à-dire $v^p < 4u^p$. Soit $\sqrt{-m}$ son générateur, où m désigne un certain entier naturel quadratfrei.

Posant alors $v = 2^s v' v''^2$, où v' désigne le quadratfrei impair qui divise v, l'entier m est défini, selon le cas, par l'une des trois formules suivantes :

$$m = \begin{cases} v'(4u^p - v'^p v''^{2p}), \text{ si } s = 0 \quad (1) \\ 2v'(u^p - 2^{sp-2} v'^p v''^{2p}), \text{ si } s \text{ est impair} \quad (2) \\ v'(u^p - 2^{sp-2} v'^p v''^{2p}), \text{ si } s > 0 \text{ est pair} \quad (3) \end{cases}$$

On suppose désormais que λ est une p-unité, c'est-à-dire u et v sont premiers à p. Cette condition, jointe aux considérations précédentes, assure l'équivalence entre l'existence de solutions non-triviales du premier cas à l'équation de Fermat (F') : $x^p + y^p + z^p = 0$, et l'existence de solutions non-triviales à l'équation d'Euler (E) ; sous réserve expresse, toutefois, que h(k) ne soit pas divisible par p. Comme on l'a déjà vu, les critères de Wendt et de Krasner donnent une condition nécessaire et suffisante (resp. suffisante, mais beaucoup plus maniable) pour que (F') n'admette pas de solutions non-triviales du premier cas dans l'anneau des entiers de k ; l'équivalence devient caduque, d'où l'on conclut à la divisibilité de h(k) par p. L'entier m étant donné, on en déduit immédiatement le discriminant d du corps quadratique $Q(\sqrt{-m})$:

$$d = -m \text{ (resp. } -4m, \text{ si } -m \equiv 1 \text{ (resp. } 2,3) \pmod 4).$$

Si q désigne un nombre premier tel que $q = lp + 1$ (où $l \not\equiv 0 \pmod 3$), il est clair que le symbole de Legendre $(\frac{d}{q})$ défini sous l'hypothèse «$d \not\equiv 0 \pmod q$», est égal à $(\frac{-m}{q})$. Avant d'exprimer $(\frac{d}{q})$ au moyen de l'une des formules qui définissent m, nous allons examiner *sous quelles conditions d est divisible par q*. Pour cela, nous nous placerons dans le cas (1) qui est, du point de vue de cette étude, visiblement équivalent aux deux autres. Il vient :

$$v'(4u^p - v'^p v''^{2p}) = v'(4u^p - v^p) \equiv 0 \pmod q, \text{ ce qui est équivaut à } v' \equiv 0 \pmod q$$

ou $4u^p - v^p \equiv 0 \pmod q$. Nous allons démontrer que la deuxième éventualité est impossible.

En effet, elle ne pourrait se présenter d'une façon triviale, puisque u et v sont premiers entre eux, donc non simultanément divisible par q. De plus, dans ce cas, il est impossible d'avoir $uv \equiv 0 \pmod q$. On en conclurait que la classe de 4 modulo q est une puissance p-ième d'un élément α du corps

premier ϕ_q, soit :

$$\bar{4} = \alpha^p = \alpha^{\frac{q-1}{l}}.$$ Par conséquent : car l'exposant $p = \frac{q-1}{l}$

$\bar{4}^l = \alpha^{q-1} = \bar{1}$. Ceci équivaut à $(2^l - 1)(2^l + 1) \equiv 0 \pmod q$. Or, $2^l \not\equiv -1 \pmod q$, car la congruence supposée $2^l \equiv -1 \pmod q$ implique $2^{pl} = 2^{q-1} \equiv (-1)^p \equiv -1 \pmod q$. Il en résulterait que $2^l - 1$ est congru à 0 mod q. Mais ceci est rendu impossible par les conditions de validité imposées aux critères de Krasner et Wendt ; dans l'énoncé du premier, figure explicitement la clause «$2^l - 1 \not\equiv 0 \pmod q$» qui, non respectée, annulerait l'un au moins des déterminants $R(\epsilon_1, \epsilon_2, \epsilon_3, i_1, i_2, i_3)$. Par ailleurs, l'on peut montrer que $2^l - 1$ divise la circulante de Wendt $W(l)$, ceci étant lié au fait que chacun des déterminants $R((\epsilon_j), (i_h))$ est lui-même un diviseur - selon une certaine puissance - de $W(l)$. On aurait donc :

$W(l) \equiv 0 (\text{mod } 2^l - 1)$ et $2^l - 1 \equiv 0 \pmod q$, soit $W(l) \equiv 0 \pmod q$, en contradiction avec la condition 1 du critère de Wendt.

En résumé, *la condition «$d \equiv 0 \pmod q$» est équivalente à la condition «$v' \equiv 0 \pmod q$».* *Si les autres hypothèses du critère employé sont vérifiées, il en résulte que $h(k)$ est divisible par p.* Il est entendu une fois pour toutes que nous omettrons, dans nos énoncés, d'envisager le cas où $v' \equiv 0 \pmod q$, puisque *seule la condition «$v' \not\equiv 0 \pmod q$» conduit à des résultats (moins forts)*. Nous consignons certains d'entre eux dans le paragraphe suivant.

§ 1 - Expression de $(\frac{d}{q})$ - Quelques résultats.

Si $d \not\equiv 0 \pmod q$, il vient :

$$\left(\frac{d}{q}\right) = \begin{cases} (-1)^{\frac{q-1}{2}} \left(\frac{4u^{p-v}, p_v'', 2p}{q}\right)\left(\frac{v'}{q}\right), & \text{si } s = 0 \quad (I) \\ (-1)^{\frac{(q-1)(q+5)}{8}} \left(\frac{u^p \cdot 2^{sp-2v}, p_v'', 2p}{q}\right)\left(\frac{v'}{q}\right), & \text{si } s \text{ est impair} \quad (2) \\ (-1)^{\frac{q-1}{2}} \left(\frac{u^p \cdot 2^{sp-2v}, p_v'', 2p}{q}\right)\left(\frac{v'}{p}\right), & \text{si } s > 0 \text{ est pair} \quad (3) \end{cases}$$

Il peut arriver que les entiers u *et* v *soient divisibles par* q ; comme ils ne peuvent l'être simultanément, cette circonstance se présente *si* $u \equiv 0 \pmod q$ *et* $v \not\equiv 0 \pmod q$, *ou si* $u \not\equiv 0 \pmod q$ *et* $v \equiv 0 \pmod q$.

Sous la première hypothèse, u^p disparaît des formules donnant $(\frac{d}{q})$; le symbole $(\frac{v'}{q})$ garde un sens, puisque $v \not\equiv 0 \pmod q$ implique $v' \not\equiv 0 \pmod q$. Il est clair que, dans tous les cas, $(\frac{d}{q}) = +1$ (c'est évident, si $s = 0$ et si $s > 0$ est pair ; si s est impair, il suffit de revenir à l'expression correspondante de -m modulo q : $(-2)^{sp-1} v'^p + 1 v''^{2p}$, qui est le produit de trois carrés).

Pour simplifier l'énoncé des résultats obtenus, il est entendu que le corps quadratique imaginaire $k = Q(\sqrt{-m})$ mentionné ci-dessous, est caractérisé par le paramètre rationnel $\lambda = u/v$, avec $(u,v) = 1$ et $uv \not\equiv 0 \pmod p$.

Proposition I.

Si le corps $R = Q(\sqrt{-m})$ *est quadratique imaginaire, et si, pour le nombre premier* $p > 3$ *il existe un nombre premier* $q = lp + 1$ *tel que*

1) q *ne divise pas* $W(l)$ *(ceci exige* $l \not\equiv 0 \pmod 3$*).*

2) q *ne divise pas* $l^l - 1$.

(C) 3) $u \equiv 0 \pmod q$ *et* $v \not\equiv 0 \pmod q$,

[ce qui équivaut à $(\frac{d}{q}) = +1$] *alors* $h(k) \equiv 0 \pmod p$.

Proposition II.

Si, pour un nombre premier $p > 3$ *donné, il existe un nombre premier* q *de la forme* $lp + 1$ *tel que :*

1) $l \not\equiv 0 \pmod 3$

2) $2^l \not\equiv 1 \pmod q$

3) $3^{l/4} < q = lp + 1$

4) $l^l \not\equiv 1 \pmod q$, *et si* $k = Q(\sqrt{-m})$ *est quadratique imaginaire tel que*

(C) 5) $u \equiv 0 \pmod q$ *et* $v \not\equiv 0 \pmod q$

alors $h(k) \equiv 0 \pmod p$.

Sous l'hypothèse que $u \not\equiv 0 \pmod q$ et $v \equiv 0 \pmod q$, nous allons obtenir des résultats analogues, mais d'un caractère moins trivial. Afin d'éviter des redites, nous indiquerons seulement de quelle manière il convient de modifier la condition (C) pour obtenir de nouvelles propositions I', I'', I''', I'^{v} (resp. II', II'', II''', II'^{v}). En outre, nous dirons de l'entier a qu'il est R (resp. NR), s'il est reste quadratique (resp. non-reste quadratique) modulo q.

Puisque $v = 2^s v'v''^2$ est divisible par q, cela implique $v'' \equiv 0 \pmod q$, car v' n'est pas divisible par q.

Les formules qui donnent $(\frac{d}{q})$ deviennent, dans le premier et le troisième cas :

$$\begin{cases} (\frac{d}{q})_{1,3} = (-1)^{\frac{q-1}{2}} (\frac{uv'}{q}). \text{ Mais si s est impair :} \\ (\frac{d}{q})_2 = (-1)^{\frac{(q-1)(q+5)}{8}} (\frac{uv'}{q}). \end{cases}$$

Nous sommes ramenés à déterminer la parité du nombre $\mu = \frac{(q-1)(q+5)}{8}$. Selon la répartition des valeurs de q modulo 16, il vient :

$$\mu \equiv \begin{cases} \underline{0} \pmod 2, \text{ si } q \equiv \underline{1, 3, 9, 11} \pmod{16}. \\ \underline{1} \pmod 2, \text{ si } q \equiv \underline{5, 7, 13, 15} \pmod{16}. \end{cases}$$

On peut caractériser d'une façon commune les cas (I) et (3) par la condition «$\underline{s \equiv 0 \pmod 2}$». Cela étant, voici quelles sont les quatre conditions (C) sur lesquelles s'appuient les nouvelles propositions $I^{(i)}$ (resp. $II^{(i)}$).

(C_1) : «*Si* $s \equiv 0 \pmod 2$ et $q \equiv 1 \pmod 4$, et si u et v' *sont simultanément* R *ou* NR»

(C_2) : «*Si* $s \equiv 0 \pmod 2$ et $q \equiv -1 \pmod 4$, *et si* u et v' *sont alternativement* R *et* NR».

(C_3) : «*Si* s $\equiv 1 \pmod 2$ *et* q $\equiv 1, 3, 9, 11 \pmod{16}$ *et si* u *et* v' *sont simultanément* R ou NR».

(C_4) : «*Si* s $\equiv 1 \pmod 2$ *et* q $\equiv 5, 7, 13, 15 \pmod{16}$ *et si* u *et* v' *sont alternativement* R *et* NR».

On rappelle que, dans le cadre des propositions $I^{(i)}$ (resp. $II^{(i)}$), ce sont des conditions nécessaires et suffisantes (resp. suffisantes) pour que $(\frac{d}{q}) = +1$. C'est alors que $h(k) \equiv 0 \pmod p$.

§ 2 - Théorèmes généraux.

Nous supposons à présent que uv ne soit pas divisible par q. Il en résulte que les formules (Δ) sont complètes, et l'évaluation du nombre $(\frac{d}{q})$ généralement impossible ; toutefois, l'on peut conclure à la divisibilité de h(k) par p, en appliquant les techniques précédentes à un ensemble relativement large de corps quadratiques imaginaires. *Le critère de Wendt* tire son principal intérêt de la formulation suivante :

2.1. - *Si l'on se donne une certaine valeur du nombre* $l = q-1/p$, *les résultats obtenus seront valables pour tous les corps :* $k = Q(\sqrt{-m})$, *tels que le couple* (p, q) *vérifie les conditions du critère.*

Au cours du présent travail, nous admettrons d'abord $l = 2$; puis $l = 4$. Nous nous sommes limité à ces deux valeurs, en raison de l'extrême difficulté que présente le calcul de la circulante d'ordre 8.

2.2. - Si $l = 2, W(2) = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} = 1-4 = -3$, et $2^2 - 1 = 3$. Les conditions (I) et (2) sont donc vérifiées, quel que soit le nombre premier $q = 2p + 1$, puisque $p > 3$. Abordant maintenant le calcul de $(\frac{d}{q})$, sous l'hypothèse que $v' \not\equiv 0 \pmod q$, nous verrons que les trois cas envisagés conduisent à des conclusions fort différentes.

1) - $s = 0$.

Comme $v' \not\equiv 0 \pmod q$, il est R ou NR, et $(\frac{v'}{q}) = \epsilon' = \pm 1$. Par ailleurs $(-1)^{\frac{q-1}{2}} = -1$; en effet, $p \equiv \epsilon_1 \pmod 4$ implique $q = 2p + 1 \equiv 2\ \epsilon_1 + 1 \pmod 4$, soit $q \equiv -1 \pmod 4$. Puisque $u \not\equiv 0 \pmod q$, il est R ou NR, ce qui s'exprime par $u^{\frac{q-1}{2}} = u^p \equiv \epsilon \pmod q$. Enfin, $v''^{2p} \equiv 1 \pmod q$. Il en résulte :

$$(\frac{d}{q}) = -(\frac{4\epsilon - \epsilon'}{q})\epsilon' = \begin{cases} -(\frac{3}{q}), \text{ si } (\epsilon, \epsilon') = (+1, +1) \text{ ou } (-1,-1) \\ (\frac{5}{q}), \text{ si } (\epsilon, \epsilon') = (+1, -1) \text{ ou } (-1, +1) \end{cases}$$

Or, $(\frac{3}{q}) = -(\frac{q}{3}) = -(\frac{2p+1}{3})$. Parmi les trois nombres consécutifs : 2p, 2p + 1, 2p + 2, seul le dernier est divisible par 3. Ceci implique $p \equiv -1 \pmod 3$, donc $2p + 1 \equiv -1 \pmod 3$. Par conséquent, $(\frac{3}{q}) = -(\frac{-1}{3}) = +1$. Il en résulte que $(\frac{d}{q})$ n'est jamais égal à + 1, si u et v' sont simultanément restes ou non-restes quadratiques modulo q.

Par contre, $(\frac{5}{q}) = (\frac{q}{5}) = (\frac{2p+1}{5})$. *Nous sommes ramenés à chercher la classe de p modulo 5.*

a) *Si* $p \equiv 0 \pmod 5$, ce n'est possible que pour $p = 5$.

Alors, $q = 11$, et $(\frac{11}{5}) = (\frac{1}{5}) = +1$. Le couple (5, 11) satisfait les conditions du critère, et h(k) est divisible par 5.

b) *Si* $p \equiv 1, 2,$ *ou* $3 \pmod 5$, ce qui peut aussi s'écrire $p \equiv 1$ ou $2 \epsilon \pmod 5$

$(\frac{2p+1}{5}) = (\frac{3}{5}) = (\frac{5}{3}) = (\frac{2}{3}) = -1$, ou $(\frac{2p+1}{5}) = (\frac{3}{5}) = -1$ (en fait, le cas $\epsilon = +1$ est à exclure, car $2p + 1$ est premier).

c) *Si* $p \equiv -1 \pmod 5$, $2p + 1 \equiv -1 \pmod 5$, d'où $(\frac{2p+1}{5}) = +1$.

Nous concluons donc :

$(C)_{s=0}$ «*La condition nécessaire et suffisante pour que* $(\frac{d}{q}) = +1$ *est que u et v' soient alternativement R et NR, et que* p *soit congru à* -1 *modulo 5, ou égal à 5*».

Nous donnons explicitement les couples $(p, q < 1000)$ pour lesquels les corps $Q(\sqrt{-m})$, correspondant au premier cas, admettent un nombre de classes h(k) divisible par p. Cette recherche est facilitée par la remarque suivante : p est congru à -1 modulo 2, 3, et, sauf si $p = 5$, modulo 5. Donc, $p \equiv -1 \pmod{30}$ et, pour des valeurs convenables de t :

$$\begin{cases} p = 30t - 1 \\ q = 60t - 1 \end{cases}$$

Par conséquent :

$$(p,q) = \begin{cases} (5, 11) \\ (29,59) \text{ si } t = 1 \\ (89,179) \text{ si } t = 3 \\ (179,359) \text{ si } t = 6 \\ (239,479) \text{ si } t = 8 \\ (359,719) \text{ si } t = 12 \\ (419,839) \text{ si } t = 14 \end{cases}$$

2) *s est impair*

Si $v' \not\equiv 0 \pmod q$, posons, comme précédemment $(\frac{v'}{q}) = \epsilon'$. Nous avons à déterminer la *parité du nombre* $(q-1)(q+5)/8$, *et la classe modulo q du nombre* 2^{sp-2}. Comme $p \equiv \epsilon_1 \pmod 4$, il vient :

$$\begin{cases} q-1 \equiv 2\epsilon_1 \pmod 4 \\ q+5 \equiv q+1 \equiv 2(\epsilon_1 + 1) \pmod 4, \text{ d'où} \end{cases}$$

$$(q-1)(q+5) \equiv 4\epsilon_1(\epsilon_1 + 1) \pmod{16}, \text{ i.e.}$$

$$(q-1)(q+5) \equiv \begin{cases} 8 \pmod{16}, \text{ si } \epsilon_1 = +1 \\ 0 \pmod{16}, \text{ si } \epsilon_1 = -1 \end{cases}$$

Ainsi, $(-1)^{\frac{(q-1)(q+5)}{8}} = -\epsilon_1$, si $p \equiv \epsilon_1 \pmod 4$.

Le nombre 4 admet pour inverse, modulo q, tout nombre congru à $\frac{p+1}{2}$. Enfin,

$(2p)^s \equiv (\frac{2}{q})^s = (\frac{2}{q}) = (-1)^{\frac{q^2-1}{8}}$ (mod q). Comme $q^+ 5$ est congru à $q^+ 1$ modulo 4, on a aussi

$(2p)^s = -\epsilon_1$. Par conséquent :

$$\boxed{(\frac{d}{q}) = -\epsilon_1\epsilon' \, (\frac{\epsilon + \epsilon_1\epsilon' \quad \frac{p+1}{2}}{q}) = f(\epsilon_1, \epsilon, \epsilon').}$$

Mettons en évidence certaines symétries :

$$f(-\epsilon_1, \epsilon, \epsilon') = f(\epsilon_1, \epsilon, -\epsilon')$$
$$f(\epsilon_1, -\epsilon, -\epsilon') = f(\epsilon_1, \epsilon, \epsilon')$$
$$f(\epsilon, \epsilon_1, \epsilon') = f(-\epsilon, -\epsilon_1, \epsilon')$$

Ces propriétés de f rendent très rapide la détermination de $(\frac{d}{q})$ dans tous les cas possibles :

$$f(+1,+1,+1) = f(+1,-1,-1) = f(-1,+1,-1) = f(-1,-1,+1) = -(\frac{(p+3)/2}{q})$$
$$f(+1,+1,-1) = f(+1,-1,1) = f(-1,+1,+1) = f(-1,-1,-1) = -(\frac{(p-1)/2}{q})$$

-1) Evaluation de $(\frac{(p-1)/2}{q})$.

$\frac{p-1}{2} = \frac{2p-2}{4} = \frac{2p+1-3}{4} \equiv -\frac{3}{4}$ (mod q). Par conséquent,

$(\frac{(p-1)/2}{q}) = (\frac{-3}{q}) = -(\frac{3}{q}) = -1$, et $-(\frac{(p-1)/2}{q}) = +1$.

On a donc toujours, dans les quatre cas indiqués, $h(k) \equiv 0$ (Mod p), c'est-à-dire sous les conditions suivantes :

$$\begin{cases} \text{(I), (2) : } p \equiv 1 \text{ (mod 4), et u et v' simultanément R ou NR.} \\ \text{(3), (4): } p \equiv -1 \text{ (mod 4), et u et v' alternativement R et NR.} \end{cases}$$

alors $h(k) \equiv 0$ (mod p)

-2) Evaluation de $(\frac{(p+3)/2}{q})$

$\frac{p+3}{2} = \frac{2p+6}{4} = \frac{2p+1+5}{4} \equiv \frac{5}{4}$ (mod q). Donc, $(\frac{(p+3)/2}{q}) = (\frac{5}{q}) = -1$

sous la condition nécessaire et suffisante que p soit congru à 1 ou à 3 modulo 5. Dans les quatre cas indiqués correspondants et si $p \equiv 1$ ou 3 (mod 5), h(k) est divisible par p. Plus explicitement :

$$\begin{cases} \text{(I), (2) - } \textit{Si } p \equiv 1 \text{ (mod 4) et } \equiv 1 \text{ ou 3 (mod 5), et si u et v' sont alternativement R ou NR.} \\ \text{(3), (4)- } \textit{Si } p \equiv -1 \text{ (mod 4) et } \equiv 1 \text{ ou 3 (mod 5), et si u et v' sont simultanément R ou NR.} \end{cases}$$

Alors $h(R) \equiv 0$ (mod p).

-3) *s > 0 est pair*

Sous réserve que v' ne soit pas divisible par q, il vient, avec les notations habituelles :

$$(\frac{d}{q}) = - (\frac{\epsilon - 2^{sp-2}\ \epsilon'}{q})\ \epsilon'.$$

Or, $2^{sp-2} = (2^p)^s \cdot 2^{-2} \equiv \frac{1}{4} \equiv \frac{p+1}{2} \pmod q$.

$(\frac{d}{q}) = -(\frac{[2\epsilon - (p+1)\epsilon'\ ]/2}{q})\ \epsilon'$, fonction du couple (ϵ, ϵ') qui prend les valeurs suivantes :

$$(\frac{d}{q}) = \begin{cases} -1, \text{ si } (\epsilon, \epsilon') = (+1, +1) \text{ ou } (-1, -1) \\ +1, \text{ si } (\epsilon, \epsilon') = (-1, +1) \text{ ou } (+1, -1), \\ \text{et } p = 5 \text{ ou } \equiv -1 \pmod 5. \end{cases}$$

On trouve aussi les conditions de validité identiques à celles obtenues dans le premier cas.

Supposons maintenant $I = 4$.

Le calcul de W(4) se fait aisément, si l'on tient compte de sa divisibilité par 5^3 :

$$W(4) = \begin{vmatrix} 1 & 4 & 6 & 4 \\ 4 & 6 & 4 & 1 \\ 6 & 4 & 1 & 4 \\ 4 & 1 & 4 & 6 \end{vmatrix} = 5^3 \begin{vmatrix} 1 & 2 & 2 & 4 \\ 2 & 2 & 1 & 1 \\ 2 & 1 & 1 & 4 \\ 1 & 1 & 2 & 6 \end{vmatrix} = 5^3 \cdot 3$$

De plus, $I^I - 1 = 4^4 - 1 = 3.5.17$, et $W(I)(I^I - 1) = 3^2.5^4.17$. Ainsi, la réunion des conditions (1) et (2) est équivalente à la condition «$3^2.5^4.17 \not\equiv 0 \pmod q$». Or, $p > 3$ implique $q > 17$, et cette condition est donc toujours réalisée. Il reste à rechercher les valeurs prises par $(\frac{d}{q})$, dans les différents cas possibles.

1) - $s = 0$.

$q \equiv 1 \pmod 4$ implique $(-1)^{\frac{q-1}{2}} = +1$. Quant à v', il est R ou NR, donc $(\frac{v'}{q}) = \epsilon'$.

Une première forme - approximative - de $(\frac{d}{q})$ est, dans ce cas :

$$(\frac{d}{q}) = \epsilon' (\frac{4u^p - v'^p v''^{2p}}{q})$$

Désignons par ζ une racine primitive modulo q ; on en connaît au moins une, dans ce cas : c'est 2.

Selon une notation classique, nous définissons modulo q - 1 des entiers ind u et ind v', tels que :

$u \equiv \zeta^{\text{ind } u} \pmod q$; $v' \equiv \zeta^{\text{ind } v'} \pmod q$. D'une manière analogue, soit $v'' = \zeta^{\text{ind } v''} \pmod q$. Puisque $\zeta^{2p} = \zeta^{\frac{q-1}{2}}\ \zeta \equiv -1 \pmod q$, la formule qui définit $(\frac{d}{q})$ s'écrit en général :

$$(\frac{d}{q}) = \epsilon' (\frac{4\ \zeta^{p\ \text{ind } u} - (-1)^{\text{ind } v''}\ \zeta^{p\ \text{ind } v'}}{q})$$

Par conséquent, ind v'' étant pair ou impair selon que v'' est R ou NR, il est nécessaire de définir $(\frac{d}{q})$ dans quatre éventualités :

$$\left(\frac{d}{q}\right) = \begin{cases} \left(\frac{4(-1)^{\text{ind u}/2} - (-1)^{\text{ind v''} + \text{ind v'}/2}}{q}\right) & \textit{si u et v' sont R.} \\ -\left(\frac{4(-1)^{\text{ind u}/2} - (-1)^{\text{ind v''} + (\text{ind v'}-1)/2}\ \zeta^{p}}{q}\right), & \textit{si u est R et v' NR.} \\ \left(\frac{4(-1)^{\frac{\text{ind u}-1}{2}}\ \zeta^{p} - (-1)^{\text{ind v''} + \frac{\text{ind v'}}{2}}}{q}\right), & \textit{si u est NR, et v'R.} \\ \left(\frac{4(-1)^{\frac{\text{ind u}-1}{2}} - (-1)^{\text{ind v''} + \frac{\text{ind v'}-1}{2}}}{q}\right), & \textit{si u et v' sont NR , car } \left(\frac{\zeta^{p}}{q}\right) = -1. \end{cases}$$

	mod 4 ind u	u	v'	mod 4 ind v'	v''	$(\frac{d}{q})$
	0			0	R	-1
					NR	(5/q)
	0			2	R	(5/q)
I		R	R		NR	-1
	2			0	R	(5/q)
					NR	-1
	2			2	R	-1
					NR	(5/q)
	0			1	R	$-\alpha$
					NR	$-\beta$
	0			-1	R	$-\beta$
II		R	NR		NR	$-\alpha$
	2			1	R	$-\beta$
					NR	$-\alpha$
	2			-1	R	$-\alpha$
					NR	$-\beta$
	1			0	R	$\gamma(-\beta)$
					NR	$\delta(-\alpha)$
	1			2	R	$\delta(-\alpha)$
III		NR	R		NR	$\gamma(-\beta)$
	-1			0	R	$\delta(-\alpha)$
					NR	$\gamma(-\beta)$
	-1			2	R	$\gamma(-\beta)$
					NR	$\delta(-\alpha)$
	1			1	R	(3/q) = -1
					NR	(5/q)
	1			-1	R	(5/q)
IV		NR	NR		NR	(3/q)
	-1			1	R	(5/q)
					NR	(3/q)
	-1			-1	R	(3/q) = -1
					NR	(5/q)

$$\alpha = \left(\frac{4 - \zeta^{p}}{q}\right); \quad = \left(\frac{4 + \zeta^{p}}{q}\right)$$

$$= \left(\frac{4\,\zeta^{p} - 1}{q}\right); \quad = \left(\frac{4\,\zeta^{p} + 1}{q}\right)$$

$$\alpha\,\beta = \gamma\,\delta = \left(\frac{17}{q}\right)$$

$$\left(\frac{4\,\zeta^{p} + 1}{q}\right) = \left(\frac{\zeta^{p}}{q}\right)\left(\frac{4 - \zeta^{p}}{q}\right), \text{ soit}$$

$$\begin{cases} \delta = -\alpha \\ \gamma = -\beta \end{cases}$$

Donc, aussi :

Les trente-deux résultats obtenus font l'objet du tableau.

Certains d'entre eux sont immédiatement exploitables.

En effet, soit $p \equiv \epsilon \pmod 3$; alors $q = 4p + 1 \equiv 4\epsilon + 1 \pmod 3$, ce qui implique $\epsilon = +1$. Par conséquent,

$$(\frac{3}{q}) = (\frac{q}{3}) = (\frac{p+1}{3}) = (\frac{2}{3}) = -1.$$

Evaluons maintenant $(\frac{5}{q}) = (\frac{4p+1}{5}) = (\frac{5p-p+1}{5}) = (\frac{p-1}{5})$.

Il vient :

$$(\frac{p-1}{5}) \begin{cases} +1, \text{ si } p \equiv 2 \pmod 5 \\ -1, \text{ si } p \equiv 3 \text{ ou } 4 \pmod 5), \end{cases}$$

les cas $p = 5$ et $p \equiv 1 \pmod 5$ s'excluant d'eux-mêmes.

Il est plus difficile d'obtenir les valeurs précises des nombres α , β , γ , δ . Toutefois, la remarque suivante peut en simplifier le calcul :

$$\alpha\beta = (\frac{16 - \zeta^{2p}}{q}) = (\frac{16\ \zeta^{2p-1}}{q}) = (\frac{17}{q}) = \gamma\delta \quad , \text{car } (\frac{-1}{q}) = +1.$$

La détermination du nombre $(\frac{17}{q})$ aboutit alors à la conclusion que α et β (resp. γ et δ) *sont égaux ou opposés selon que 17 est R ou NR modulo q.* Ainsi :

$$(\frac{17}{q}) = (\frac{4p+1}{17}) = (\frac{24k+5}{17}) = (\frac{7k+5}{17}) \quad , \text{car } p \equiv 1 \pmod 3 \text{ et}$$

$p \equiv 1 \pmod 2 \Rightarrow p \equiv 1 \pmod 6$, soit $q = 4(6k + 1) + 1$. C'est donc la classe de k-modulo 17 qui fixe le caractère quadratique de 17 modulo q. Il vient :

$$(\frac{17}{q}) = \begin{cases} +1 \text{ , si } k \equiv 2, 3, 4, 6, 12, 14, 15, 16, \pmod{17} \\ -1, \text{ si } k \equiv 0, 1, 5, 7, 8, 10, 11, 13, \pmod{17}. \end{cases}$$

Il en résulte que certaines classes de p modulo $6 \times 17 = 102$ jouent un rôle identique à celui de k (mod 17) :

$$(\frac{17}{q}) = \begin{cases} +1, \text{ si } p \equiv 13, 19, 25, 37, 73, 85, 91, 97 \pmod{102} \\ -1, \text{ si } p \equiv 1, 7, 31, 43, 49, 61, 67, 79 \pmod{102} \end{cases}$$

De manière qualitative, il apparaît que, dans le second cas, les résultats correspondants ont un caractère «mêlé», qui les assimile à ceux des régions I et IV ; par contre, si $(\frac{17}{q}) = +1$, les régions II et III sont à prendre ou à rejeter en bloc.

Puisque $\delta = -d$ et $\gamma = -\beta$, tout revient à déterminer le caractère quadratique du nombre β , par exemple.

Or, le nombre ζ^p est, par hypothèse, d'ordre 4 modulo q ; dans le groupe multiplicatif ϕ_q^* , l'équation :

« $x^4 - 1 = 0$ », qui équivaut à

« $(x^2 + 1)(x - 1)(x + 1) = 0$ »

fait apparaître les deux racines de -1 comme les seuls éléments d'ordre 4. La solution est théoriquement bien connue ; il suffit, lors de l'application du théorème de Wilson au nombre premier $q = 4p + 1$, de mettre en évidence le fait que $(q-1)! \equiv \left[\left(\frac{q-1}{2}\right)!\right] \pmod q$, ce qui conduit immédiatement au résultat suivant :

$$\zeta^p \equiv \pm (2p)! \pmod q.$$

Malheureusement, une telle expression de ζ^p est très vite inutilisable. *Mais nous avons vu, au début de ce paragraphe, que 2 était une racine primitive modulo q ;* par conséquent $2^{2p} \equiv -1 \equiv 4p \pmod q$, et ceci équivaut à $2^{2(p-1)} \equiv p \pmod q$. Si nous désignons par ρ une des racines carrées de p modulo q (celles-ci existent à coup sur, car $\left(\frac{p}{q}\right) = \left(\frac{4p+1}{p}\right) = \left(\frac{1}{p}\right) = +1$), nous pouvons écrire cette congruence sous la forme :

$$2^{2(p-1)} \equiv \rho^2 \pmod q, \text{ soit}$$
$$2^{p-1} \equiv \epsilon\rho \pmod q, \text{ et } 2^p \equiv \sigma = 2\,\epsilon\rho \pmod q.$$

Une dernière difficulté provient du fait que le signe de ϵ semble malaisé à prévoir. Si, pour fixer les idées, on convient de désigner par $\sqrt{p}$ l'entier naturel $\sqrt{p + \lambda q}$, où λ a la plus petite valeur - positive - admissible, une table d'indices donne immédiatement le résultat cherché. En voici quelques exemples :

a) Si $(p,q) = (7,29)$, $2^6 = 64 \equiv +\sqrt{29 + 7} \pmod{29}$, soit $2^6 \equiv +6 \pmod{29}$, donc $2^7 \equiv 12 \pmod{29}$.

Par conséquent, $2^7 + 4 \equiv 16 \pmod{29}$, et $\beta = +1$. Conformément au fait que $\left(\frac{17}{q}\right) = -1$, $\alpha = \left(\frac{2}{29}\right)^3 = -1$. Le tableau précédent indique alors quels doivent être les caractères quadratiques respectifs de u, v', et v", pour que h(k) soit divisible par 7.

b) Si $(p,q) = (13,53)$, $2^{12} \equiv 11^2 \equiv +15 \pmod{53}$, et $+15 = \sqrt{13 + 4 \times 53}$;

$\beta = \left(\frac{34}{53}\right) = \left(\frac{2}{53}\right)\left(\frac{17}{53}\right) = (-1)\times(+1) = -1$.

Dans ce cas, $-\beta = -\alpha = +1$, *et tous les corps quadratiques imaginaires $Q(\sqrt{-m})$ tels que u et v' soient alternativement R et NR (mod q) ont leur nombre de classes h(k) divisible par 13.*

2) - s est impair

Dans ce cas, $\frac{(q-1)(q+5)}{8} = p(2p+3) \equiv 1 \pmod 2$. Avec les notations habituelles $\left(\frac{v'}{q}\right) = \epsilon'$. En outre,

$$2^{sp-2} = (2^p)^{2n+1}.2^{-2} = (2^{2p})^n.2^p.\frac{1}{4} \equiv (-1)^{\frac{s-1}{2}}.2^p(3p+1) \pmod q.$$

La formule qui définit $\left(\frac{d}{q}\right)$ est donc, dans ces conditions :

$$\left(\frac{d}{q}\right) = -\epsilon'\left(\frac{2^p \text{ ind u}.(-1)^{\text{ind v"} + \frac{s-1}{2}}.2^{p\,(\text{ind v'} + 1)}(3p+1)}{q}\right)$$

Afin d'obtenir des formules plus détaillées, nous sommes amenés à envisager au moins quatre éventualités distinctes, en laissant fixée la parité du nombre

$$\text{ind } v'' + \frac{s-1}{2} \ ;$$

$$\left(\frac{d}{q}\right) = \begin{cases} -\left(\dfrac{(-1)^{\frac{\text{ind } u}{2}} - (-1)^{\text{ind } v'' + \frac{s-1+\text{ind } v'}{2}}}{q}\right) 2^{p(3p+1)}, & \text{si u et v' sont R.} \\ \left(\dfrac{(-1)^{\frac{\text{ind } u}{2}} - (-1)^{\text{ind } v'' + \frac{s+\text{ind } v'}{2}}}{q}\right) (3p+1), & \text{si u et R, et si v' est NR.} \\ -\left(\dfrac{(-1)^{\frac{\text{ind } u-1}{2}} 2^p - (-1)^{\text{ind } v'' + \frac{s-1+\text{ind } v'}{2}}}{q}\right) 2^{p(3p+1)}, & \text{si u est NR, et si v' est R.} \\ \left(\dfrac{(-1)^{\frac{\text{ind } u-1}{2}} 2^p - (-d)^{\text{ind } v'' + \frac{s+\text{ind } v'}{2}}}{q}\right) (3p+1), & \text{si u et v' sont NR.} \end{cases}$$

A priori, de tels résultats ne sont utilisables qu'à titre de «critères d'essai». Si l'on se donne le couple $(p, 4p+1)$, la valeur de p n'est plus un paramètre comme les autres, et, l'on peut alors achever la discussion.

(Remarque : Dans la troisième formule, 2^p disparaît, à condition de mettre un signe $+$ devant le reste quadratique, car $\left(\frac{2^p}{q}\right) = -1$).

A titre indicatif, nous donnerons à présent les formules qui définissent $\left(\frac{d}{q}\right)$ dans le cas où s est pair et positif.

3) - $s > 0$ pair

$$\left(\frac{d}{q}\right) \begin{cases} \left(\dfrac{(-1)^{\frac{\text{ind } u}{2}} - (-1)^{\text{ind } v'' + \frac{\text{ind } v'+s}{2}}}{q}\right) (3p+1), & \text{si u et v' sont R.} \\ -\left(\dfrac{(-1)^{\frac{\text{ind } u}{2}} - (-1)^{\text{ind } v'' + \frac{s+\text{ind } v'-1}{2}}}{q}\right) 2^{p(3p+1)}, & \text{si u est R et v' NR.} \\ \left(\dfrac{(-1)^{\frac{\text{ind } u-1}{2}} 2^p - (-1)^{\text{ind } v'' + \frac{\text{ind } v'+s}{2}}}{q}\right) (3p+1), & \text{si u est NR et si v' est R.} \\ -\left(\dfrac{(-1)^{\frac{\text{ind } u-1}{2}} 2^p - (-1)^{\text{ind } v'' + \frac{s+\text{ind } v'-1}{2}}}{q}\right) 2^{p(3p+1)}, & \text{si u et v' sont NR.} \end{cases}$$

La remarque précédente s'applique à la quatrième formule du tableau ci-dessus ; l'ensemble des résultats obtenus montre bien la complexité et la fécondité des méthodes de Wendt.

3 - **Applications du critère de Krasner.**

La méthode précédente, fondée sur la constance du rapport $\lambda = \frac{q-1}{p}$ nous a donné des résultats très complets ; en effet, les diviseurs premiers de h(k) y sont caractérisés par leurs classes de congruence selon un certain module, et on obtient ainsi une infinité de «règles de divisibilité».

Malheureusement, la richesse même de ces résultats n'autorise leur exploitation complète (resp. partielle), que si $\lambda = 2$ (resp. $\lambda = 4$). Une raison technique en est l'énormité du déterminant $W(\lambda)$, dès que λ n'est plus très petit. Une autre raison est peut-être la difficulté croissante que l'on éprouve à situer les éléments u^p, v'^p, v''^{2p}, dans le corps Φ_q ; ce sont des racines λ i-èmes, ou $\lambda/2$i-èmes de l'unité, d'autant plus nombreuses que λ est plus grand. Une valeur imposée à $(\frac{d}{q})$ correspond alors à un nombre considérable d'éventualités distinctes, ce qui nécessite la construction et l'examen de «matrices-réponses» de plus en plus complexes, et très vite inutilisables.

Nous allons voir que la méthode de Krasner pallie de tels inconvénients, ce qui lui permet de se montrer beaucoup plus féconde en propositions d'ordre concret. Son principe essentiel consiste à se donner une valeur de p, et, sous garantie des quatre conditions rappelées ci-dessous, à déterminer les corps quadratiques imaginaires $k = Q(\sqrt{-m})$, dans lesquels le nombre premier $q = \lambda p + 1$ se décompose ou se ramifie. C'est donc, dans ce cas, le rapport $\underline{p} = \frac{q-1}{\lambda}$ qui est constant ; il représente un éventuel diviseur premier de tous les h(k) convenables - Nous énoncerons :

Critère de Krasner :

Si pour un nombre premier $p > 3$ *donné, il existe un nombre premier* q *de la forme* $\lambda p + 1$, tel que :

1) $\lambda \not\equiv 0 \pmod 3$

2) $2^{\lambda} \not\equiv 1 \pmod q$

3) $3^{\lambda/4} < q = \lambda p + 1$

4) $\lambda \not\equiv 1 \pmod q$, *et si* $k = Q(\sqrt{-m})$ *est un corps quadratique imaginaire tel que*

5) $(\frac{d}{q}) = +1$, ou $d \equiv 0 \pmod q$,

alors, $h(k) \equiv 0 \pmod p$.

a) Limitation du domaine des variations de λ .

Une valeur de p étant donnée, on peut constater qu'il existe une infinité de nombres $\lambda p + 1$ composés ; en effet, d'après la condition (I), λ est congru à ± 1 modulo 3, soit $\lambda \equiv \epsilon \pmod 3$. De même, $p \equiv \epsilon' \pmod 3$. Par conséquent, $q = \lambda p + 1 \equiv \epsilon\epsilon' + 1 \pmod 3$, et, si $\epsilon\epsilon' = -1$, q *est nécessairement divisible par 3, quel que soit* λ . C'est pourquoi nous appliquerons la règle suivante :

«p *étant donné, se restreindre à l'examen des entiers* $\lambda p + 1$ *pour lesquels* $\lambda \equiv p \equiv \epsilon \pmod 3$».

Il en résulte que les nombres premiers q peuvent revêtir deux formes généralement distinctes, et deux seulement :

1) si $\lambda \equiv p \equiv 1 \pmod 3$, comme p est impair, on en déduit $p \equiv 1 \pmod 6$, soit $p = 6\mu + 1$. Par ailleurs, $\lambda \equiv 1 \pmod 3$ et $\equiv 0 \pmod 2$ impliquent $\lambda = 2k \equiv 1 \pmod 3$

i-è. $k \equiv -1 \equiv 2 \pmod 3$, donc $\lambda = 2(3\lambda + 2) = 6\lambda + 4$. Il vient alors :

$$\begin{cases} p = 6\mu + 1 \\ I = 6\lambda + 4 \end{cases} \quad \text{et } q = Ip + 1 = 36\lambda\mu + 6\lambda + 24\mu + 5.$$

2) Si $I \equiv p \equiv -1 \pmod 3$, un calcul semblable nous conduit au résultat suivant :

$$\begin{cases} p = 6\mu - 1 \\ I = 6\lambda + 2 \end{cases} \quad \text{et } q = Ip + 1 = 36\lambda\mu - 6\lambda + 12\mu - 1.$$

Il est facile de voir qu'on peut trouver des couples de paramètres (λ, μ) et (λ', μ') pour lesquels $q_{\lambda,\mu} = q_{\lambda',\mu'}$. Ceci équivaut à la résolution d'un système comportant une équation de Bezout à trois inconnues, ainsi que trois équations simples adjointes :

$$\begin{cases} 2X - Y + 6Z = +1 \text{ (rem. : p.g.c.d. } (2, -1, 6) = 1). \\ X = \mu' - 2\mu \\ Y = \lambda + \lambda' \\ Z = \lambda'\mu' - \lambda\mu \end{cases}$$

Sans chercher la solution générale d'un tel système, dépourvue d'intérêt relativement aux problèmes que nous nous posons, nous aurons l'occasion de constater une telle coïncidence.

Enfin, il est utile de résoudre, par rapport à I, l'inégalité (3) :

$3^{I/4} < Ip + 1$, qui s'écrit aussi :

$3^{I/4} - 3) < 4p.\ I/4$. Or, désignant par «L » le logarithme népérien de n, il vient :

$3^t = e^{tL3}$, et l'application : $t \to 3^t$ admet pour dérivée l'application : $t \to L3.\, e^{tL3}$.

Par conséquent, le problème est de comparer les deux intégrales définies :

$$\int_0^{I/4} L3.\, e^{tL3}\, dt \quad \text{et} \quad \int_0^{I/4} 4p\, dt, \quad \text{soit :}$$

$$\int_0^{I/4} e^{tL3}\, dt < \frac{4p}{L3} \int_0^{I/4} 1.dt$$

La fonction e^{tL3} possédant de «bonnes» propriétés (avoir des dérivées toutes positives), et puisque I est strictement inférieur à $\frac{4p}{L3}$, la plus grande valeur admissible pour I est donnée par la résolution de l'équation transcendante :

$$e^{\frac{x}{4} L3} = \frac{4p}{L3}, \text{ elle-même équivalente à l'équation :}$$

$$\frac{x}{4} L3 = L(4p/L3), \text{ ou } x = \frac{4L(4p/L3)}{L3} \quad \text{soit :}$$

$$I_{max} = E\left\{\frac{4\,L\,(4p\,/\,L3)}{L3}\right\}$$

Nous pourrions donner une expression de l_{max} au moyen des logarithmes décimaux ; toutefois, un calcul direct fait intervenir des logarithmes itérés. En pratique, il est préférable de se livrer à quelques essais sur l'inégalité (3), mise sous forme équivalente :

(3') $l/4 \log_{10} 3 < \log_{10}(lp + 1)$, ou encore :

(3'') $$\frac{l}{\log_{10}(lp+1)} < \frac{4}{\log_{10} 3} .$$

b) Etude du cas $s = 0$; b_1) Généralités.

[Nous supposons, au cours de cette étude, que $v' \not\equiv 0 \pmod q$].

Selon la première formule définissant $(\frac{d}{q})$, il vient :

$$(\frac{d}{q}) = (-1)^{\frac{q-1}{2} + \text{ind } v'} \left(\frac{g^{\text{ind } 4 + p \text{ ind } u} - g^{p(\text{ind } v' + 2 \text{ ind } v'')}}{q}\right)$$

où g désigne une racine primitive modulo q.

Si q est donné par la première des deux formules précédentes, $\frac{q-1}{2} = \frac{lp}{2} \equiv \lambda \pmod 2$.

Par contre, dans le deuxième cas, $\frac{q-1}{2} \equiv \lambda + 1 \pmod 2$. Sous forme condensée :

$$\left\| (\frac{d}{q}) = (-1)^{\frac{q-1}{2} + \text{ind } v'} \left(\frac{g^{\text{ind } 4 + p \text{ ind } u} - g^{p(\text{ind } v' + 2 \text{ ind } v'')}}{q}\right)\right.$$

(où l'on rappelle que $p \equiv l \pmod 3$).

Les nombres ind 4 + p ind u et p (ind v' + 2 ind v'') sont définis modulo q-1. Posant respectivement :

$$\underline{\text{ind } 4 + p \text{ ind } u \equiv \alpha} \pmod{(q-1)}$$
$$\underline{p(\text{ind } v' + 2 \text{ ind } v'') \equiv \beta} \pmod{(q-1)}$$

une condition nécessaire et suffisante pour que ces congruences aient un sens est que α - ind 4, d'une part, et β, d'autre part, soient divisibles par le p.g.c.d. de p et de q-1, soit pgcd (p, l p) = p. Par conséquent :

$$\alpha \equiv \text{ind } 4 + \alpha' p \pmod{(q-1)}$$
$$\beta \equiv \beta' p \pmod{(q-1)}, \text{ avec } 0 \leq \left\{\begin{matrix}\alpha' \\ \beta'\end{matrix}\right\} \leq l - 1$$

La détermination des nombres u, v', v'' - définis modulo q - pour lesquels $(\frac{d}{q}) = +1$ est rendue plus facile par la remarque suivante : le caractère quadratique du nombre $g^\alpha - g^\beta$ dépend seulement de la différence $\alpha - \beta$, lorsque la parité de β est fixée. En effet,

$$(\frac{g^\alpha - g^\beta}{q}) = (\frac{g^{\alpha - \beta + \beta} - g^\beta}{q}) = (\frac{g}{q})^\beta \left(\frac{g^{\alpha-\beta} - 1}{q}\right) = (-1)^{\beta + \text{ind}(g^{\alpha-\beta} - 1)}$$

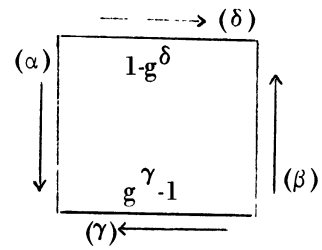
Si $l \equiv p \equiv 1 \pmod 3$, les solutions du problème seront fournies par tous les couples (α, β) tels que :

$$\beta + \text{ind}(g^{\alpha-\beta} - 1) + \lambda + \text{ind } v' \equiv 0 \pmod 2, \text{ donc tels que}$$

$$p(\text{ind}v' + 2\text{ind}v'') + \text{ind}(g^{\alpha} {}^{\beta}-1) + \lambda + \text{ind}v' \equiv 0 \pmod 2 ;$$

cela signifie que, dans ce cas, ind $(g^{\alpha - \beta} - 1)$, *doit être de même parité que* λ. De façon analogue : si $I \equiv p \equiv -1 \pmod 3$, ind $(g^{\alpha - \beta} - 1)$ *est de parité opposée à celle de* λ.

Ce qui précède suggère un algorithme simple, en vue de déterminer les couples (α, β) acceptables : on se donne un tableau à quatre entrées, orienté selon le schéma ci-dessous :



Les γ correspondent à une valeur fixée de la différence $\alpha - \beta$; les solutions sont donc fournies par toutes les colonnes du tableau d'indice «ind $(g^{\gamma} - 1)$» pair ou impair, selon le cas. On a evidemment toujours :

$\text{ind}(g^{\gamma} - 1) \equiv \gamma + \text{ind}(1 - g^{\delta}) \pmod{(q-1)}$, si $\delta + \gamma \equiv 0 \pmod{(q-1)}$.

Il est difficile de donner des résultats plus précis, sans avoir fixé au préalable une valeur de p. *Nous supposons, dans ce qui suit, que p est égal à 5.*

b_2) Applications numériques : p = 5.

Les trois premières valeurs de I, à priori admissibles, sont :

$$I = \begin{cases} 8 = 6.1 + 2 \\ 14 = 6.2 + 2 \\ 20 = 6.3 + 2 \end{cases}$$; les valeurs de q associées sont

respectivement : 41, 71, 101. Or, l'inégalité (3') s'écrit dans ce cas, tous calculs faits :

$$(3\lambda + 1) . 0{,}23856 < \log(30\lambda + 11).$$

Pour $\lambda = 2$, on a bien :

$$7 \times 0{,}23856 = 1{,}66992 < 1{,}85126 = \log 71.$$

Par contre, pour $\lambda = 3$, *l'inégalité est renversée :*

$$2{,}38560 > 2{,}00432 = \log 101.$$

L'inégalité (3) laisse donc «filtrer» les deux couples :

$$(I, q) = \begin{cases} \underline{(8,41)} \\ \underline{(14,71)} \end{cases}$$

Il nous reste à examiner, pour chacun d'eux, l'expression :

$$(2^{I} - 1)(I^{I} - 1).$$

Dans le premier cas : $(2^8-1)(8^8-1) = (2^8-1)(2^{24}-1) = (2^{12}+1)(2^4-1)(2^{12}-1)(2^4+1)$

$= 15 \times 17 \times 63 \times 65 (2^{12} + 1) = A(2^{12} + 1)$, où $A \not\equiv 0 \pmod{41}$.

Enfin, $(2^4)^3 + 1 = (2^4+1)(2^8 - 2^4 + 1) = (2^4+1).241 \not\equiv 0 \pmod{41}$.

Dans le second cas : $(2^7-1)(2^7+1) \not\equiv 0 \pmod{71}$, et $14^{14} \equiv 7^{7\times 14} \equiv 7^{28} \equiv 5 \pmod{71}$, donc $14^{14}-1 \equiv 4 \pmod{71}$, ce qui démontre le résultat.

Nous étudierons d'abord l'expression de $(\frac{d}{q})$, lorsque $\underline{(p, I, q) = (5, 8, 41)}$.

Une racine primitive modulo 41 (la plus petite) est $g = 6$. Dans les calculs, cette valeur numérique n'intervient pas, puisque seule la correspondance indicielle «$x \not\equiv 0 \leftrightarrow g^{\text{ind } x}$» est utilisable. Les tables d'indices sont celles du petit livre de Vinogradov «Eléments of Number Theory».

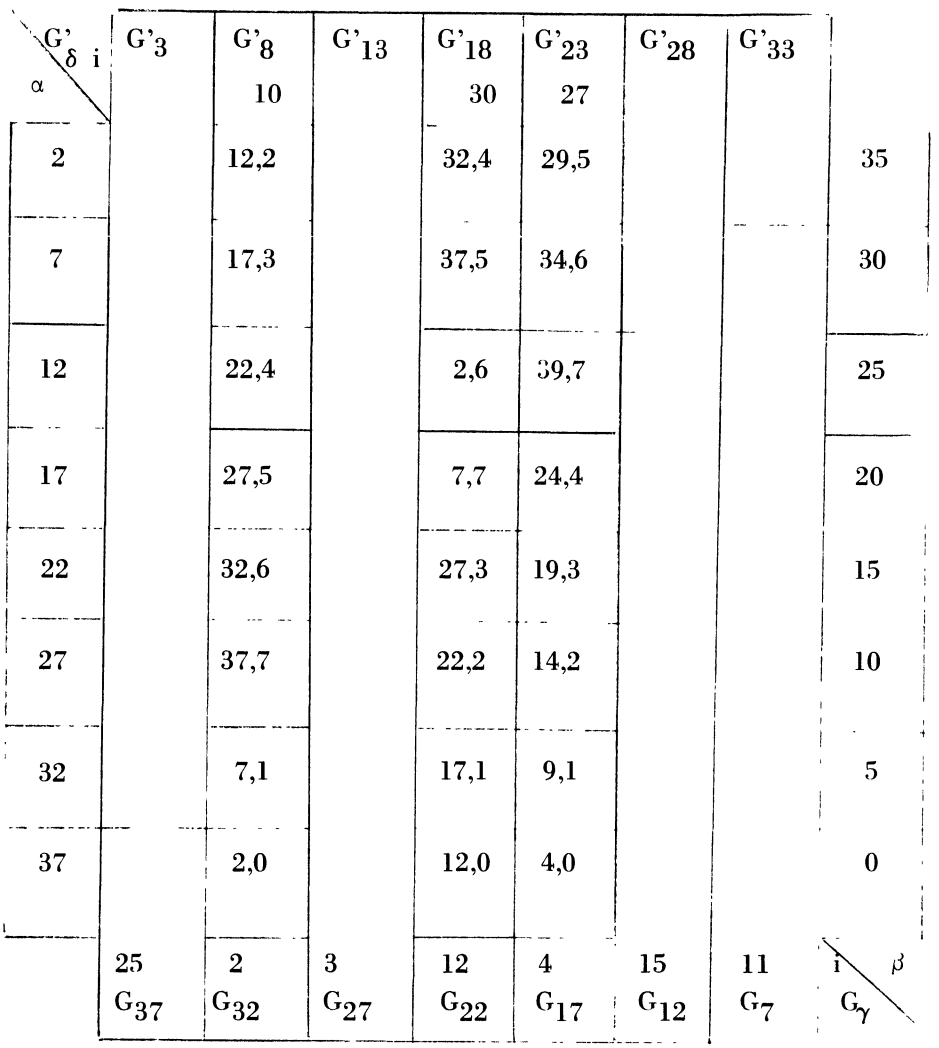
$\text{ind } 4 \equiv 12 \pmod{40}$. Par conséquent, si l'on se donne les α par une suite *croissante* de restes modulo 41 - ce qui n'est pas nécessairement le cas de la suite $\{\text{ind } 4 + \alpha \cdot p\}$, il vient :

$$\begin{cases} \alpha \equiv 2, 7, 12, 17, 22, 27, 32, 37 \pmod{41}. \\ \beta \equiv 0, 5, 10, 15, 20, 25, 30, 35 \pmod{41}. \end{cases}$$

$-5 \equiv -1 \pmod 3$. Il convient donc de retenir les colonnes du tableau correspondant à «$\text{ind}(g^\gamma - 1) \equiv 0 \pmod 2$» puisque $\lambda = 1$.

Pour éviter de détruire l'aspect symétrique du tableau, on a muni ce dernier d'une «colonne flottante», associée à la suite de nombres : $g^2-1, g^7-g^5, \ldots, g^{37}-g^{35}$; cette colonne est donc caractérisée par $\text{ind}(g^2-1) = \text{ind } 35 \equiv 21 \pmod{40}$, qui ne convient pas : nous nous abstiendrons, par conséquent, d'y inscrire les résultats obtenus (cette remarque vaut pour toutes les colonnes qui ne sont pas des solutions).

Pour des raisons de commodité typographique, nous désignerons par $\underline{G_\gamma}$ (resp. $\underline{G'_\delta}$) les nombres $g^\gamma - 1$ (resp. $\underline{1 - g^\delta}$).



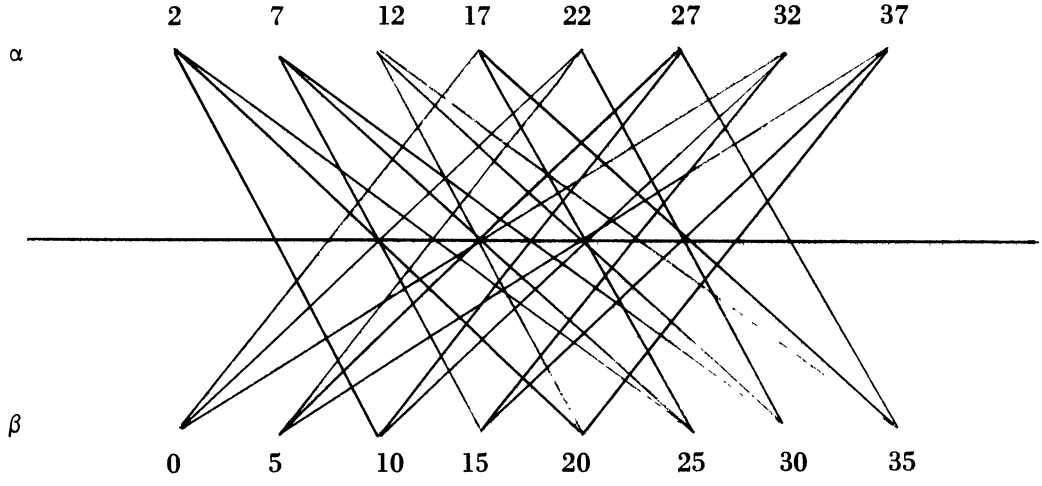
Dans les carrés intérieurs figurent les sommes $\alpha + i\,(G'_\delta)$ ou les sommes $\beta + i\,(G_\gamma)$.

A chacune d'elles est associée la valeur de $\beta' = \beta/5$ qui lui correspond.

Le rôle de la ligne brisée, qui progresse parallèlement à la direction de la première bissectrice, est de séparer graphiquement toute colonne-solution en deux sous-colonnes de la façon suivante :

$\alpha - \beta$ étant défini modulo 40, il en résulte, pour fixer les idées, que, lors d'une progression $\alpha - \beta$ = 2-10, 7-15, ..., 27-35, le terme suivant sera 32-40, i-é. 32-0, et finalement 37-5.

Ceci est bien illustré par la représentation en réseaux des solutions.



β'	0	1	2	3	4	5	6	7
0	θ		θ		θ		θ	
1		θ		θ		θ		θ
2			θ		θ		θ	
3				θ		θ		θ
4					θ		θ	
5						θ		θ
6							θ	
7								θ

Ind v'

Il est désormais facile d'obtenir explicitement les générateurs m de tous les corps quadratiques imaginaires $k = Q(\sqrt{-m})$, pour lesquels h(k) est congru à 0 modulo 5.

En effet, puisque nous étudions le cas «s = 0», il vient :

$$m = v'(4u^p - v'^p v''^{2p}) = v'(g^{\alpha} - g^{\beta});$$

$$m = v'\, g^{\beta}\,(g^{\alpha - \beta} - 1) = v'\, g^{\beta}\, G_{\gamma}\ , \text{ où l'on a posé } \gamma = \alpha - \beta. \text{ Ainsi :}$$

$$m \equiv g^{\operatorname{ind} G_{\gamma}} \cdot g^{\beta + \operatorname{ind} v'} \pmod{41}.$$

Il est raisonnable d'indéxer les solutions d'une même colonne par β' ou par β, ce qui revient au même. Par conséquent, la formule ci-dessus se lit directement (partie inférieure du tableau) tant que

est inférieur à $37 - \gamma$. Nous écrirons

$$m \equiv \begin{cases} g^{\text{ind } G_\gamma} \cdot g^{\text{ind v'} + 5\,\beta'} & \text{si } 0 \leq \beta \leq 37 - \gamma \\ g^{\text{ind } G_\gamma - \gamma} \cdot g^{\text{ind v'} + 5\,\beta'} & \text{si } 37 - \gamma < \beta \leq 35. \end{cases} \pmod{41}$$

Ici, 37 (resp. 35) représente le plus grand reste inférieur à 40 de l'indice α (resp. β).

En vue d'achever la détermination de m, il est nécessaire de résoudre par rapport à ind v' (mod 8) l'équation :

$$\text{ind v'} + 2 \text{ ind v''} \equiv \beta' \pmod 8.$$

Les résultats ont été reportés au bas de la page. Nous les explicitons ici (le paramètre est β ').

$$\text{ind v'} \equiv \begin{cases} 0 & \text{si } \beta' \equiv 0 \pmod 8 \\ 1 & \text{si } \beta' \equiv 1 \pmod 8 \\ 0,2 & \text{si } \beta' \equiv 2 \pmod 8 \\ 1,3 & \text{si } \beta' \equiv 3 \pmod 8 \\ 0,2,4 & \text{si } \beta' \equiv 4 \pmod 8 \\ 1,3,5 & \text{si } \beta' \equiv 5 \pmod 8 \\ 0,2,4,6 & \text{si } \beta' \equiv 6 \pmod 8 \\ 1,3,5,7 & \text{si } \beta' \equiv 7 \pmod 8 \end{cases} \pmod 8$$

Enfin, nous rappellerons que les valeurs numériques obtenues définissent des classes de congruence modulo 41 ; il convient d'y choisir les entiers naturels qui sont quadratfrei, car eux seuls sont les générateurs cherchés.

A titre d'exemple, nous résolvons complètement le problème relatif à la colonne

$G_{17} = g^{17} - 1.$

Ind $G_{17} = 4$. Donc, nous obtiendrons tous les indices de m correspondant à la prmière formule en ajoutant 4 aux nombres de la suite (0,6, < 10, 12 > , <16, 18> , < 20, 22, 24 >), ce qui donne :

(4, 10, <14, 16> ,< 20, 22 >, <24, 26, 28 >). De même

(< 13,15,17 > , <17,19,21,23 > , < 23,25,27,29 >) représente les indices de m correspondant à la deuxième formule (dans ce cas, il faut ajouter 27 - ou retrancher - 13 à la suite «ind v' + 5 β '»). Finalement :

$\underline{m \equiv 2,3,5,12,14,18,21,22,24,25,26_2,30_2,31,34,35,40} \pmod{41}$.

N.B. : «26_2» et «30_2» signifient que 26 et 30 apparaîssent deux fois dans la recherche des restes de m modulo 41.

$\underline{\text{Si (p, I , q)} = (5, 14, 71)}$, les solutions doivent être cherchées dans les colonnes dont l'indice est *impair,* car $14 = 6.\underline{2} + 2$. Nous indiquerons de quelle façon varient les paramètres α et β :

$\alpha \equiv 2,7,12,17,22,27,32,37,42,47,52,57,62,67 \pmod{70}$

$\beta \equiv 0,5,10,15,20,25,30,35,40,45,50,55,60,65 \pmod{70}$.

Dans ce cas, nous trouvons quatre G_γ d'indice impair ; ce sont, respectivement :

$$\begin{cases} G_7 \to i(G_7) = 39 \\ G_{37} \to i(G_{37}) = 27 \\ G_{42} \to i(G_{42}) = 19 \\ G_{47} \to i(G_{47}) = 63 \end{cases}$$

Pour avoir toutes les solutions, il suffit d'appliquer la formule démontrée plus haut, en posant cette fois :

$$\begin{cases} \alpha_m = 67 \\ \beta_m = 65., \text{ soit} \end{cases}$$

$$m \pmod{71} \equiv \begin{cases} g^{\text{ind } G_\gamma + \text{ ind } v' + \beta} & \text{si } 0 \leq \beta \leq 67 - \\ g^{(\text{ind } G_\gamma - \gamma) + \text{ ind } v' +} & \text{si } 67 - \gamma < \beta \leq 65. \end{cases}$$

On a toujours $\beta \equiv 5\beta' \pmod{70}$; il convient donc de remarquer que β' est maintenant défini *modulo 14.*

c) s impair, ou s pair > 0.

Rien d'essentiel n'est changé à ce qui précède ; en effet, $2^{sp-2} \equiv g^{(sp-2)\text{ind } 2}$, ce qui revient à donner une définition un peu différente des indices α et β déjà utilisés. Il vient :

$$\begin{cases} \alpha \equiv p \text{ ind } u \pmod{(q-1)}, \text{ soit } \alpha \equiv 0 \pmod{p}. \\ \beta \equiv (sp-2) \text{ ind } 2 + p(\text{ind } v' + 2 \text{ ind } v'') \pmod{(q-1)}, \text{ i.e. :} \end{cases}$$

$2 \text{ ind } 2 + p(s \text{ ind } 2 + \text{ind } v' + 2 \text{ ind } v'') \pmod{(q-1)}$, ce qui implique :

$\beta + 2 \text{ ind } 2 \equiv 0 \pmod{p}$. Ainsi,

$$\begin{cases} \alpha \equiv 0 \pmod{p} \\ \beta \equiv -2 \text{ ind } 2 \pmod{p} \end{cases}$$

Enfin, si q est de la première forme, il est congru à $2\lambda + 1$ modulo 4, donc

$$\frac{(q-1)(q+5)}{8} \equiv \frac{\lambda(\lambda+3)}{2} \pmod 2, \text{ soit}$$

$$\frac{(q-1)(q+5)}{8} \equiv \begin{cases} 0 \pmod 2, \text{ si } \lambda \equiv 0 \text{ ou } -1 \pmod 4 \\ 1 \pmod 2, \text{ si } \lambda \equiv 1 \text{ ou } 2 \pmod 4. \end{cases}$$

Si q est de la deuxième forme, il est congru à $-2\lambda - 1$ modulo 4, ce qui entraîne :

$$\frac{(q-1)(q+5)}{8} \equiv \begin{cases} 0 \pmod 2, \text{ si } \lambda \equiv 2 \text{ ou } -1 \pmod 4 \\ 1 \pmod 2, \text{ si } \lambda \equiv 0 \text{ ou } 1 \pmod 4. \end{cases}$$