Séminaire Delange-Pisot-Poitou. Théorie des nombres

Jean Lagrange

Nombres congruents et courbes elliptiques

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 16, n° 1 (1974-1975), exp. n° 16, p. 1-17

<http://www.numdam.org/item?id=SDPP_1974-1975__16_1_A11_0>

© Séminaire Delange-Pisot-Poitou. Théorie des nombres
(Secrétariat mathématique, Paris), 1974-1975, tous droits réservés.

L'accès aux archives de la collection « Séminaire Delange-Pisot-Poitou. Théorie des nombres » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

Numdam
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
16e année, 1974/75, n° 16, 17 p.

10 mars 1975

NOMBRES CONGRUENTS ET COURBES ELLIPTIQUES

par Jean LAGRANGE

1. Nombres congruents.

Soit n un entier positif "quadratfrei", on dit que n est un nombre congruent s'il existe une fraction A/B, telle que les fractions $(A/B)^2 + n$ et $(A/B)^2 - n$ soient des carrés. Ainsi Léonard de Pise (FIBONACCI) donne en 1220 :

$$\left(\frac{41}{12}\right)^2 + 5 = \left(\frac{49}{12}\right)^2 , \quad \left(\frac{41}{12}\right)^2 - 5 = \left(\frac{31}{12}\right)^2 .$$

n est donc un nombre congruent si le système diophantien :

$$(1) \quad \begin{cases} A^2 + nB^2 = C^2 \\ A^2 - nB^2 = D^2 \end{cases}$$

a une solution non triviale (i. e. avec $B \neq 0$). Les inconnues A, B, C, D appartiennent à $\mathbb{Z}$, mais on peut toujours les supposer positives. La solution est dite primitive si A et B sont premiers entre eux.

Si n est un nombre congruent, le système (1) a une infinité de solutions primitives ; en effet, si A, B, C, D est une solution primitive, on vérifie facilement que :

$$(2) \quad \begin{cases} A_1 = A^4 + n^2 B^4 \\ B_1 = 2ABCD \\ C_1 = 2A^4 - D^4 \\ D_1 = 2A^4 - C^4 \end{cases}$$

est une autre solution primitive avec $|B_1| > |B|$.

D'après FERMAT, les nombres 1 et 2 ne sont pas congruents car les équations $A^4 - B^4 = C^2 D^2$ et $A^4 - 4B^4 = C^2 D^2$ n'ont que des solutions triviales.

Dans cet exposé, on va surtout chercher des familles de nombres non congruents. p, q, r désigneront toujours des nombres premiers impairs distincts.

GENOCCHI (1855) montre que les nombres suivants ne sont pas congruents :

$n = p$ avec $p = 3 \pmod 8$

$n = pq$ avec $p = 3 \pmod 8$, $q = 3 \pmod 8$

$n = 2p$ avec $p = -3 \pmod 8$

$n = 2pq$ avec $p = -3 \pmod 8$, $q = -3 \pmod 8$.

BASTIEN (1913) donne les nombres non congruents suivants :

$n = p$, avec $p = 1 \pmod 8$, et la condition suivante : décomposant p en une somme de deux carrés, $p = a^2 + 4b^2$, la somme $a + 2b$ est un non-résidu quadratique de p ; soit, en utilisant le symbole de Legendre, $((a + 2b)/p) = -1$.

$n = 2p$ avec $p = -7 \pmod{16}$.

On trouvera les références des résultats cités ci-dessus ainsi que bien d'autres dans DICKSON ([8], chap. XVI).

Parmi les familles apparemment nouvelles que nous allons donner la plus simple est :

$$n = 2pq \text{ , avec } p = 3 \pmod 8 \text{ , } q = 3 \pmod 8 .$$

A l'opposé, signalons le résultat de HEEGNER [9] et BIRCH [4] : le nombre $n = 2p$ avec $p = -1 \pmod 4$ est congruent.

2. Lien avec les courbes elliptiques.

Le système (1) est équivalent à :

$$\begin{cases} A^2 = \left(\frac{C + D}{2}\right)^2 + \left(\frac{C - D}{2}\right)^2 \\ nB^2 = \frac{C^2 - D^2}{2} \end{cases}$$

La solution générale de la première équation est :

$$\begin{cases} \frac{C + D}{2} = \alpha^2 - \beta^2 \\ \frac{C - D}{2} = 2\alpha\beta \\ A = \alpha^2 + \beta^2 \end{cases}$$

où α et β sont deux entiers premiers entre eux, de parités différentes.

B est nécessairement pair, on pose $B = 2\gamma$, et on a :

$$n\gamma^2 = \alpha\beta(\alpha^2 - \beta^2) . \tag{3}$$

Réciproquement, α et β étant deux entiers premiers entre eux, de parités différentes, le nombre $\alpha\beta(\alpha^2 - \beta^2)$ débarassé de ses facteurs carrés donne un nombre congruent. C'est l'équation (3) qui a été utilisée par ALTER, CURTZ et KUBOTA [1] pour construire une table de nombres congruents (voir aussi [2]).

Posant

$$\frac{\alpha}{\beta} = \frac{X}{nZ} \text{ , } \frac{\gamma}{\beta^2} = \frac{Y}{n^2 Z} \quad (1)$$

on obtient $Y^2 Z = X(X^2 - n^2 Z^2)$.

C'est l'équation d'une courbe elliptique Γ . On est donc ramené à l'étude des points rationnels d'une courbe elliptique. n est un nombre congruent si, et seu-

---

(1) Pour éviter de surcharger les notations toutes les équations sont écrites sous forme homogène ou quasi homogène, les inconnues ou coordonnées sont donc des entiers.

lement si, Γ possède un point rationnel avec $XYZ \neq 0$. Les égalités (2) s'écrivent alors

$$\frac{X_1}{Z_1} = \left(\frac{X^2 + n^2 Z^2}{2XZ}\right)^2$$

$$\frac{Y_1}{Z_1} = \frac{1}{8Y^3 Z^3}(X^2 + n^2 Z^2)(X^4 - 6n^2 X^2 Z^2 + n^4 Z^4) .$$

On reconnaît la multiplication par 2 dans le groupe des points rationnels de Γ . Il en résulte que n est un nombre congruent si, et seulement si, le rang g de Γ est strictement positif. Les seuls points d'ordre fini de Γ sont les points d'ordre 2 .

3. La méthode de BIRCH et SWINNERTON-DYER.

Pour calculer le rang g de Γ , nous utiliserons la méthode donnée dans [5] (Voir également TATE [11]). Rappelons brièvement cette méthode.

Le fait que n^2 soit un carré n'intervenant pas, on prendra pour Γ :

$$Y^2 Z = X(X^2 - DZ^2) .$$

On associe à Γ la courbe $\overline{\Gamma}$: $Y^2 Z = X(X^2 + 4DZ^2)$. Les courbes Γ et $\overline{\Gamma}$ sont isogènes, c'est-à-dire que la multiplication par 2 dans Γ se décompose en deux homomorphismes φ et ψ :

$$\Gamma \xrightarrow{\varphi} \overline{\Gamma} \xrightarrow{\psi} \Gamma \; ; \quad 2 = \psi \circ \varphi .$$

On utilise ensuite l'isomorphisme α : $\Gamma \xrightarrow{\alpha} \mathbb{Q}^*/\mathbb{Q}^{*2}$ défini par :

$\alpha(X , Y , Z) = X/Z \pmod{\mathbb{Q}^{*2}}$ pour $X \neq 0$,

$\alpha(0 , 0 , 1) = D \pmod{\mathbb{Q}^{*2}}$,

$\alpha(0 , 1 , 0) = 1 \pmod{\mathbb{Q}^{*2}}$,

et on démontre que $\operatorname{Ker} \alpha = \operatorname{Im} \psi$, d'où

$$\Gamma/\operatorname{Im} \psi = \Gamma/\operatorname{Ker} \alpha \simeq \alpha\Gamma .$$

g désignant le rang de Γ , on en déduit la formule $2^{g+2} = [\alpha\Gamma].[\alpha\overline{\Gamma}]$ ([ ] désigne le cardinal).

Posant $[\alpha\Gamma] = 2^{\lambda'}$, $[\alpha\overline{\Gamma}] = 2^{\overline{\lambda}'}$, on a par conséquent :

$$g + 2 = \lambda' + \overline{\lambda}' .$$

Tout revient à calculer λ' et $\overline{\lambda}'$. Pour cela on utilise un isomorphisme entre $\alpha\Gamma$ et les diviseurs d (définis mod $\mathbb{Q}^{*2}$) de D tels que l'équation

$$z^2 = dx^4 - (D/d)y^4$$

soit résoluble dans $\mathbb{Z}$.

Le calcul de λ' et $\overline{\lambda}'$ est difficile, et comme il est plus facile de résoudre

localement cette équation, on considère le groupe G défini de la façon suivante ([2])

$G \subset \mathbb{Q}^*/\mathbb{Q}^{*2}$

$G = (d\ ;\ d$ divise D, et $z^2 = dx^4 - (D/d)y^4$ est partout localement résoluble).

On définit de même $\overline{G}$, et on pose :

$$[G] = 2^{\lambda}\ ,\quad [\overline{G}] = 2^{\overline{\lambda}}\ .$$

On a alors $g + 2 \leqslant \lambda + \overline{\lambda}$. Le nombre $\lambda + \overline{\lambda}$ est appelé le nombre de la première descente.

Si D est un multiple de 4 (c'est-à-dire si n est pair), il est plus commode de prendre pour $\overline{\Gamma}$: $Y^2 Z = X(X^2 + (D/4)Z^2)$.

4. Pratique de la méthode.

On considère les équations :

(4) $z^2 = dx^4 - (n^2/d)y^4$; $d|n$ $(d \in \mathbb{Z})$

(5) $z^2 = dx^4 + (4n^2/d)y^4$; $d|2n$ $(d \in \mathbb{N})$ pour n impair

(5') $z^2 = dx^4 + (n^2/4d)y^4$; $d|(n/2)$ $(d \in \mathbb{N})$ pour n pair

et on examine leur résolubilité dans $\mathbb{R}$ et dans tous les $\mathbb{Q}_p$ (en fait, il suffit de prendre $p = 2$ et $p|n$) pour obtenir un élément d de G (avec (4)) ou de $\overline{G}$ (avec (5) ou (5')). Si l'équation considérée a une solution dans $\mathbb{Z}$, on obtient un élément de $\alpha\Gamma$ ou $\alpha\overline{\Gamma}$.

L'équation (4) a une solution dans $\mathbb{Z}$ pour $d = \pm 1$ et $d = \pm n$, de sorte que $\lambda' \geqslant 2$. (5) et (5') ont une solution pour $d = 1$ (ce qui donne $\overline{\lambda'} \geqslant 0$), on a bien $\lambda' + \overline{\lambda'} \geqslant 2$.

$\nu(n)$ désignant le nombre des diviseurs premiers impairs de n, on en déduit la majoration de g donnée par WIMAN [12] : $g \leqslant 2\nu(n)$.

En effet, le nombre des diviseurs positifs impairs de n est $2^{\nu(n)}$, et le nombre des valeurs de d possible pour (4) est $2^{\nu(n)+1}$ si n est impair, et $2^{\nu(n)+2}$ si n est pair, le nombre des valeurs de d pour (5) est $2^{\nu(n)+1}$, et pour (5') $2^{\nu(n)}$.

5. Une conjecture.

ALTER, CURTZ et KUBOTA [1] font la conjecture suivante.

Si $n = 5, 6, 7 \pmod 8$, alors n est congruent.

([2]) Ici x, y, z ne sont donc pas des entiers, mais comme nous remplacerons la résolution dans $\mathbb{Q}_p$ par une résolution modulo une puissance de p, la seule exception est celle où x, y, z appartiennent à $\mathbb{R}$; la résolution dans $\mathbb{R}$ fournit simplement le signe de d.

Nous montrons que cette conjecture est une conséquence de la conjecture bien connue :

g est de la parité du nombre de la première descente.

En effet, on sait (voir BIRCH et STEPHENS [6]) que pour D non divisible par 4 ou par une puissance quatrième, on a :

$$(-1)^{\lambda+\overline{\lambda}} = w_\infty w_2 \prod_{p^2 \| D} w_p$$

avec

$w_\infty = \mathrm{sg}\, n(-D)$

$w_2 = -1$ pour $D = 1, 3, 11, 13 \pmod{16}$, $w_2 = 1$ autrement

$w_p = -1$ pour $p = -1 \pmod 4$, $w_p = 1$ autrement.

L'application de cette formule à $D = n^2$ pour n impair, et $D = (-n^2)/4$ pour n pair donne la conjecture suivante :

g est pair pour $n = 1, 2, 3 \pmod 8$,, et impair pour $n = 5, 6, 7 \pmod 8$.

La conjecture de [1] en résulte immédiatement.

6. La deuxième descente.

Elle consiste à remarquer que si on pose

$$(6) \quad \begin{cases} x^2 = \xi \\ y^2 = \eta \end{cases}$$

l'équation (4) (par exemple) s'écrit alors :

$$(7) \qquad z^2 = d\xi^2 - (n^2/d)\eta^2 .$$

D'après un théorème de Legendre, si (4), donc (7), est partout localement résoluble, alors (7) est résoluble dans $\mathbb{Z}$. On en écrit la solution générale (elle dépend de deux paramètres homogènes), et on cherche des conditions pour que (6) soit partout localement résoluble.

7. Le cas $n = p$.

On a seulement à considérer les équations (5) avec $d = 2, p, 2p$. Remplaçant respectivement z par $2z, pz, 2pz$, on obtient les équations :

$$(2z^2 = x^4 + p^2 y^4) \Longrightarrow (p = \pm 1 \pmod 8)$$

$$(pz^2 = x^4 + 4y^4) \Longrightarrow (p = 1 \pmod 4)$$

$$(2pz^2 = x^4 + y^4) \Longrightarrow (p = 1 \pmod 8) .$$

Les implications données s'obtiennent en utilisant les parités de x, y, z ainsi que le module 8 ou 16, c'est-à-dire, en effectuant la résolution dans $\mathbb{Q}_2$. On vérifie ensuite que les équations sont partout localement résolubles. On a

$g = 0$ pour $p = 3 \pmod 8$; c'est le résultat de Genocchi donné au §1.

$g \leqslant 1$ pour $p = -1$ ou $-3 \pmod 8$; le nombre de la première descente est 1.

$g \leqslant 2$ pour $p = 1 \pmod 8$; le nombre de la première descente est 2.

On effectue ensuite la deuxième descente pour $p = 1 \mod 8$.

(a) $2z^2 = x^4 + p^2 y^4$. - Il existe des entiers u et v tels que :

$$\begin{cases} x^2 = u^2 + 2uv - v^2 \\ py^2 = u^2 - 2uv - v^2 \end{cases}$$

La résolution dans $\mathbb{Q}_2$ montre que v est pair et n impair. On résoud ensuite mod p ; la deuxième équation donne :

$u/v = 1 + \sqrt{2} \pmod p$ ($\sqrt{2}$ a un sens mod p , car $p = 1 \mod 8$).

Portant dans la première équation, on obtient :

$$\left(\frac{x}{v}\right)^2 = 4(1 + \sqrt{2}) \pmod p .$$

D'où la condition nécessaire $((1 + \sqrt{2})/p = 1$.

On vérifie que cette condition est suffisante pour la résolution dans $\mathbb{Q}_p$; mais cela est sans intérêt ici car on ne cherche que des conditions nécessaires pour la résolution dans $\mathbb{Z}$.

(b) $pz^2 = x^4 + 4y^4$. - On décompose p en somme de deux carrés, $p = a^2 + 4b^2$, et pour un choix convenable des signes de a et b, il existe des entiers u et v tels que :

$$\begin{cases} x^2 = a(u^2 - v^2) - 4buv \\ y^2 = b(u^2 - v^2) + auv \end{cases}$$

Pour que le système soit résoluble dans $\mathbb{Q}_2$ il faut et il suffit que

$$a + 2b = \pm 1 \pmod 8 ;$$

dans $\mathbb{Q}_p$ la condition est $((a + 2b)/p) = 1$. On sait que ces deux conditions sont équivalentes.

(c) $2pz^2 = x^4 + y^4$. - On utilise la même méthode qu'au (b). Il existe des entiers u et v tels que :

$$\begin{cases} x^2 = (a + 2b)(u^2 - v^2) - 2(a - 2b)uv \\ y^2 = (a - 2b)(u^2 - v^2) + 2(a + 2b)uv \end{cases}$$

On obtient les mêmes conditions

$$a + 2b = \pm 1 \pmod 8 \quad \text{et} \quad \left(\frac{a + 2b}{p}\right) = 1 .$$

D'après un théorème de CASSELS [7], les conditions données en (a), (b), (c) doivent être équivalentes, et en effet un théorème de BARRUCAND et COHN [3] affirme que si $p = 1 \pmod 8$, on a

$$\left(\frac{1+\sqrt{2}}{p}\right) = \left(\frac{1+i}{p}\right) = \left(\frac{-4}{p}\right)_8 \qquad (i^2 = -1 \mod p)$$

d'autre part, si $p = c^2 + 8d^2$, on a

$$\left(\left(\frac{-4}{p}\right)_8 = 1\right) \Longleftrightarrow (d \text{ pair}) .$$

Définissant i par $a = 2ib \pmod p$, on a

$$\left(\frac{1+i}{p}\right) = \left(\frac{a+2b}{p}\right) .$$

(On sait que $\left(\frac{2b}{p}\right) = 1$.)

On a ainsi démontré le théorème de Bastien donné au §1 :

si $p = 1 \pmod 8$ avec $p = a^2 + 4b^2$ et $\left(\frac{a+2b}{p}\right) = -1$, alors p est non congruent.

On a les énoncés équivalents suivants :

si $p = 1 \pmod 8$ avec $p = c^2 + 8d^2$ et d impair, alors p est non congruent.

si $p = 1 \pmod 8$ avec $\left(\frac{-4}{p}\right)_8 = -1$, alors p est non congruent.

Remarque. - La condition $(-4/p)_8 = 1$ peut s'obtenir rapidement à partir de l'équation $x^4 + 4y^4 = pz^2$ par le raisonnement suivant : soit ω un nombre premier impair qui divise x , on a $(p/\omega) = 1$, d'où $(\omega/p) = 1$ et $(x/p) = 1$. De même, comme $(2/p) = 1$, on a $(y/p) = 1$. x et y sont donc des carrés modulo p , et on a $(-4/p)_8 = 1$.

8. Le cas $n = 2p$.

On a seulement à considérer l'équation (4) avec $d = p$, et l'équation (5') avec $d = p$. Remplaçant z par pz , on obtient les équations :

$$(pz^2 = x^4 - 4y^4) \Longrightarrow (p = 1 , -1 , 3 \pmod 8)$$
$$(pz^2 = x^4 + y^4) \Longrightarrow (p = 1 \pmod 8) .$$

Les implications données s'obtiennent rapidement en remarquant pour la première que $(2/p)$ ou $(-2/p) = 1$, pour la seconde que $(-1/p)_4 = 1$. On vérifie ensuite que les équations sont partout localement résolubles. On a donc :

$g = 0$ pour $p = -3 \pmod 8$; c'est le résultat de Genocchi donné au §1.

$g \leqslant 1$ pour $p = -1$ ou $3 \pmod 8$; le nombre de la première descente est 1 .

$g \leqslant 2$ pour $p = 1 \pmod 8$; le nombre de la première descente est 2 .

Il faut effectuer ensuite la deuxième descente pour $p = 1 \pmod 8$, mais on n'obtient aucune condition supplémentaire.

Cependant la condition de Bastien, $p = 1 \pmod{16}$, est facile à obtenir :

(a) $pz^2 = x^4 + y^4$. - x et y sont de parités différentes, donc

$$x^4 + y^4 = 1 \pmod{16} .$$

Si $\overline{\omega}$, premier impair, divise z , on a $(-1/\overline{\omega})_4 = 1$, donc $\overline{\omega} = 1 \pmod 8$ et $z = 1 \pmod 8$. Il en résulte $z^2 = 1 \pmod{16}$ et $p = 1 \pmod{16}$.

On peut également faire le raisonnement de la remarque précédente, et montrer que $(-1/p)_8 = 1$.

(b) $pz^2 = x^4 - 4y^4$. - $p = 1 \pmod 8$ implique x et z impairs, y pair. Deux cas sont à considérer :

(α) p divise $x^2 + 2y^2$. On a alors :

$$\begin{cases} x^2 + 2y^2 = pu^2 \\ x^2 - 2y^2 = v^2 \\ z = uv \end{cases}$$

La solution générale de la deuxième équation est

$$\begin{cases} x = \lambda^2 + 2\mu^2 \\ y = 2\lambda\mu \\ v = \lambda^2 - 2\mu^2 \end{cases}$$

d'où

$$pu^2 = \lambda^4 + 12\lambda^2\mu^2 + 4\mu^4 = (\lambda^2 - 2\mu^2)^2 + 16\lambda^2\mu^2 = (\lambda^2 + 6\mu^2)^2 - 32\mu^4 .$$

Il en résulte que, pour tout diviseur premier $\overline{\omega}$ de u , on a $(-1/\overline{\omega})_4 = 1$, comme $\lambda^4 + 12\lambda^2\mu^2 + 4\mu^4 = 1 \pmod{16}$, quelle que soit la parité de μ , on peut faire le même raisonnement que précédemment.

(β) p divise $x^2 - 2y^2$. On a alors :

$$\begin{cases} x^2 - 2y^2 = pu^2 \\ x^2 + 2y^2 = v^2 \\ z = uv \end{cases}$$

Si $\overline{\omega}$, premier impair, divise u , on a $(2/\overline{\omega}) = 1$, donc

$$\overline{\omega} = \pm 1 \pmod 8 \quad \text{et} \quad u = \pm 1 \pmod 8 .$$

La solution générale de la deuxième équation est

$$\begin{cases} x = \lambda^2 - 2\mu^2 \\ y = 2\lambda\mu \\ v = \lambda^2 + 2\mu^2 \end{cases}$$

d'où

$$pu^2 = \lambda^4 - 12\lambda^2\mu^2 + 4\mu^4 = (\lambda^2 + 4\lambda\mu + 2\mu^2)(\lambda^2 - 4\lambda\mu + 2\mu^2) .$$

Les diviseurs de u étant congrus à $\pm 1 \mod 8$, μ est impair et on a

$$\lambda^4 - 12\lambda^2\mu^2 + 4\mu^4 = 1 \pmod{16} ;$$

le même raisonnement s'applique.

On a ainsi démontré le théorème de Bastien donné au §1 : si $p = -7 \pmod{16}$, alors p est non congruent.

Une forme équivalente est :

Si $p = 1 \pmod 8$ avec $(-1/p)_8 = -1$, alors p est non congruent.

9. Le cas $n = pq$.

On trouvera ci-dessous le tableau donnant les résultats de la première descente. Les calculs n'offrent aucune difficulté. Le nombre de la première descente est dans la dernière colonne. Lorsque ce nombre est zéro, on obtient un nombre non congruent.

Lorsque ce nombre est 2, la deuxième descente peut ramener ce nombre à zéro. On trouvera au paragraphe 14 les résultats. Il est impossible de donner ici tous les calculs ; à titre d'exemple nous allons traiter un des cas.

$n=pq$ (8)	p (8)	q (8)	$(\frac{p}{q})$	Eléments de G	λ	Eléments de $\overline{G}$	$\overline{\lambda}$	$g\leqslant$
1	1	1	1	±1 , $\pm p$, $\pm q$, $\pm n$	3	1 , 2 , p , q , 2p , 2q , n , 2n	3	4
			- 1	±1 , $\pm n$	2	1 , 2 , n , 2n	2	2
	- 3	- 3	1	±1 , $\pm n$	2	1 , p , q , n	2	2
			- 1	±1 , $\pm n$	2	1 , 2p , 2q , n	2	2
	- 1	- 1		±1 , $\pm p$, $\pm q$, $\pm n$	3	1 , 2	1	2
	3	3		±1 , $\pm n$	2	1	0	0
3	1	3	1	±1 , $\pm p$, $\pm q$, $\pm n$	3	1 , p	1	2
			- 1	±1 , $\pm n$	2	1	0	0
	- 3	- 1	1	±1 , $\pm p$, $\pm q$, $\pm n$	3	1 , p	1	2
			- 1	±1 , $\pm n$	2	1	0	0
- 3	1	- 3	1	±1 , $\pm p$, $\pm q$, $\pm n$	3	1 , p , q , n	2	3
			- 1	±1 , $\pm n$	2	1 , n	1	1
	- 1	3		±1 , $\pm p$, $\pm q$, $\pm n$	3	1	0	1
- 1	1	- 1	1	±1 , $\pm p$, $\pm q$, $\pm n$	3	1 , 2 , p , 2p	2	3
			- 1	±1 , $\pm n$	2	1 , 2	1	1
	- 3	3	1	±1 , $\pm n$	2	1 , p	1	1
			- 1	±1 , $\pm n$	2	1 , 2p	1	1

10. La deuxième descente pour $p \in \overline{G}$ avec $(p/q) = 1$.

Remplaçant z par pz , on doit étudier l'équation

$$pz^2 = x^4 + 4q^2 y^4 ,$$

d'où $p = 1 \pmod 4$. Si $(x , q) = q$, on remplace x par xq , et z par zq , on obtient l'équation

$$pz^2 = q^2 x^4 + 4y^4 .$$

On va étudier simultanément ces deux équations ; dans les deux cas, on a

$$(x , q) = (y , q) = 1 .$$

On aura besoin du résultat suivant :

si $p = a^2 + 4b^2$ ou encore $2p = (a + 2b)^2 + (a - 2b)^2$, on a

$$\left(\left(\frac{a + 2b}{p}\right) = 1\right) \Longleftrightarrow (a + 2b = \pm 1 \pmod 8) .$$

En effet, si $\overline{\omega}$ premier impair divise $a + 2b$, on a $(2p/\overline{\omega}) = 1$, d'où

$$\left(\frac{\overline{\omega}}{p}\right) = \left(\frac{p}{\overline{\omega}}\right) = \left(\frac{2}{\overline{\omega}}\right) = \begin{cases} 1 & \text{si } \overline{\omega} = \pm 1 \pmod 8 \\ -1 & \text{si } \overline{\omega} = \pm 3 \pmod 8 \end{cases}$$

(a) $pz^2 = x^4 + 4q^2 y^4$	(b) $pz^2 = q^2 x^4 + 4y^4$

Pour un choix convenable de a et b , il existe des entiers u et v tels que

$\begin{cases} x^2 = a(u^2 - v^2) - 4buv \\ qy^2 = b(u^2 - v^2) + auv \end{cases}$	$\begin{cases} qx^2 = a(u^2 - v^2) - 4buv \\ y^2 = b(u^2 - v^2) + auv \end{cases}$

On étudie la résolution dans $\mathbb{Q}_2$ (en fait, mod 8), on obtient

si $p=1 \pmod 8$, $a+2b = \pm 1 \pmod 8$	si $p=1 \pmod 8$, $a+2b = \pm q \pmod 8$
si $p=-3 \pmod 8$, $a+2b=\pm(q+2) \pmod 8$	si $p=-3 \pmod 8$, $a+2b=\pm(1+2q) \pmod 8$

On obtient ainsi la condition suivante :

si $p = 1 \pmod 8$ et $q = \pm 1 \pmod 8$, $(-4/p)_8 = 1$.

si $p = 1 \pmod 8$ et $q = \pm 3 \pmod 8$, l'équation à considérer est obtenue par le signe de $(-4/p)_8$;

si $p = -3 \pmod 8$ et $q = \pm 1 \pmod 8$, $a + 2b$ est déterminé (au signe près) ;

si $p = -3 \pmod 8$ et $q = \pm 3 \pmod 8$, aucune condition.

On étudie ensuite la résolution dans $\mathbb{Q}_p$ (en fait, mod p) . On pose $a = 2ib \pmod p$, et on obtient :

$\begin{cases} x^2 = a(u + iv)^2 \pmod p \\ qy^2 = b(u + iv)^2 \pmod p \end{cases}$	$\begin{cases} qx^2 = a(u + iv)^2 \pmod p \\ y^2 = b(u + iv)^2 \pmod p \end{cases}$

Comme on a toujours $(a/p) = (b/p) = 1$, on n'obtient aucune condition.

Enfin on étudie la résolution dans $\mathbb{Q}_q$ (en fait, mod q), $\sqrt{p}$ est définie, et on a :

$$\frac{u}{v} = \frac{-a + \sqrt{p}}{2b} \pmod q \qquad \left(\frac{x}{v}\right)^2 = \frac{2p(a - \sqrt{p})}{4b^2} \pmod q$$

$$\frac{u}{v} = \frac{2b + \sqrt{p}}{a} \pmod q \qquad \left(\frac{y}{v}\right)^2 = \frac{b(2b + \sqrt{p})}{a^2} \pmod q$$

d'où la condition :

$$\left(\frac{2(a - \sqrt{p})}{q}\right) = 1 \qquad \left(\frac{2b + \sqrt{p}}{q}\right) = 1$$

Si $q = -1 \pmod 4$, le choix de $\sqrt{p}$ permet de satisfaire à la condition,

Si $q = 1 \pmod 4$, on obtient la condition unique $((2(a - \sqrt{p}))/q) = 1$.

D'après Emma LEHMER [10] cette condition est équivalente à $(p/q)_4 = (q/p)_4$.

Résumé de la deuxième descente :

$p = 1 \pmod 8$ et $q = 1 \pmod 8 \Longrightarrow (-4/p)_8 = 1$ et $(p/q)_4 = (q/p)_4$

$p = 1 \pmod 8$ et $q = -1 \pmod 8 \Longrightarrow (-4/p)_8 = 1$

$p = 1 \pmod 8$ et $q = -3 \pmod 8 \Longrightarrow (p/q)_4 = (q/p)_4$

$p = 1 \pmod 8$ et $q = 3 \pmod 8 \Longrightarrow$ aucune condition

$p = -3 \pmod 8$ et $q = 1 \pmod 4 \Longrightarrow (p/q)_4 = (q/p)_4$

$p = -3 \pmod 8$ et $q = -1 \pmod 4 \Longrightarrow$ aucune condition.

On peut obtenir des conditions un peu plus fines en utilisant le raisonnement de la remarque du paragraphe 7. On démontre que $(x/p) = (y/p) = 1$; dans les deux cas (a) et (b), on a $qx^2 y^2 = ab(u + iv)^4 \pmod p$, d'où $(q/p)_4 = (ab/p)_4$.

La relation $(a + 2b)^2 = p + 4ab$ donne $(ab/p)_4 = (2/p).((a + 2b)/p)$. On a donc la condition $(q/p)_4 = (2/p).((a + 2b)/p)$ qu'on peut écrire

si $p = 1 \pmod 8$: $\left(\frac{a + 2b}{p}\right) = \left(\frac{-4}{p}\right)_8$, d'où $\left(\frac{q}{p}\right)_4 = \left(\frac{-4}{p}\right)_8$

si $p = -3 \pmod 8$ et $q = 1 \pmod 8$: $((a + 2b)/p) = -1$, d'où $(q/p)_4 = 1$

si $p = -3 \pmod 8$ et $q = -1 \pmod 8$: $\left(\frac{a + 2b}{p}\right) = 1$, d'où $\left(\frac{q}{p}\right)_4 = -1$

Résumé général :

$p = 1 \pmod 8$ et $q = 1 \pmod 8 \Longrightarrow (-4/p)_8 = (p/q)_4 = (q/p)_4 = 1$

$p = 1 \pmod 8$ et $q = -3 \pmod 8 \Longrightarrow (-4/p)_8 = (p/q)_4 = (q/p)_4$

$p = 1 \pmod 8$ et $q = -1 \pmod 8 \Longrightarrow (-4/p)_8 = (q/p)_4 = 1$

$p = 1 \pmod 8$ et $q = 3 \pmod 8 \Longrightarrow (-4/p)_8 = (q/p)_4$

$p = -3 \pmod 8$ et $q = 1 \pmod 8 \Longrightarrow (p/q)_4 = (q/p)_4 = 1$

$p = -3 \pmod 8$ et $q = -3 \pmod 8 \Longrightarrow (p/q)_4 = (q/p)_4$

$p = -3 \pmod 8$ et $q = -1 \pmod 8 \Longrightarrow (q/p)_4 = -1$

$p = -3 \pmod 8$ et $q = 3 \pmod 8$ $\Longrightarrow$ aucune condition.

11. Le cas $n = 2pq$

On trouvera ci-dessous le tableau donnant les résultats de la première descente. Tout ce qui a été dit au paragraphe 9 s'applique ici. Nous traiterons seulement deux cas pour la deuxième descente.

$\frac{n}{2}=pq$ (8)	p (8)	p (8)	$(\frac{p}{q})$	Eléments de G	λ	Eléments de $\overline{G}$	$\overline{\lambda}$	$g \leq$
1	1	1	1	$\pm1,\pm2,\pm p,\pm q,\pm 2p,\pm 2q,\pm\frac{n}{2},\pm n$	4	$1,p,q,\frac{n}{2}$	2	4
			- 1	$\pm1,\pm2,\pm\frac{n}{2},\pm n$	3	$1,\frac{n}{2}$	1	2
	- 3	- 3		$\pm1,\pm n$	2	1	0	2
	- 1	- 1		$\pm1,\pm2,\pm p,\pm q,\pm 2p,\pm 2q,\pm\frac{n}{2},\pm n$	4	1	0	2
	3	3		$\pm1,\pm2,\pm p,\pm q,\pm 2p,\pm 2q,\pm\frac{n}{2},\pm n$	4	1	0	2
- 3	1	- 3	1	$\pm1,\pm p,\pm q,\pm n$	3	1,p	1	2
			- 1	$\pm1,\pm n$	2	1	0	0
	- 1	3		$\pm1,\pm2,\pm p,\pm q,\pm 2p,\pm 2q,\pm\frac{n}{2},\pm n$	4	1	0	2
3	1	3	1	$\pm1,\pm2,\pm p,\pm q,\pm 2p,\pm 2q,\pm\frac{n}{2},\pm n$	4	1,p	1	3
			- 1	$\pm1,\pm2,\pm\frac{n}{2},\pm n$	3	1	0	1
	- 3	- 1	1	$\pm1,\pm q,\pm 2p,\pm n$	3	1	0	1
			- 1	$\pm1,\pm p,\pm 2q,\pm n$	3	1	0	1
- 1	1	- 1	1	$\pm1,\pm2,\pm p,\pm q,\pm 2p,\pm 2q,\pm\frac{n}{2},\pm n$	4	1,p	1	3
			- 1	$\pm1,\pm2,\pm\frac{n}{2},\pm n$	3	1	0	1
	- 3	3	1	$\pm1,\pm q,\pm 2p,\pm n$	3	1	0	1
			- 1	$\pm1,\pm p,\pm 2q,\pm n$	3	1	0	1

12. La deuxième descente pour $p = 3 \pmod 8$, $q = 3 \pmod 8$.

(a) $pq \in G$. - Remplaçant z par pqz , on doit étudier l'équation :

$$pqz^2 = x^4 - 4y^4$$

avec x impair , y pair . Comme $(2/p) = (2/q) = -1$, $(-2/p) = (-2/q) = 1$, on a p et q divisent $x^2 + 2y^2$. On en déduit l'existence d'entiers u et v tels que

$$\begin{cases} x^2 - 2y^2 = u^2 \\ x^2 + 2y^2 = pqv^2 \\ z = uv \end{cases}$$

La solution générale de la première équation est :

$$\begin{cases} x = \lambda^2 + 2\mu^2 \\ y = 2\lambda\mu \\ u = \lambda^2 - 2\mu^2 \end{cases}$$

d'où

$$pqv^2 = \lambda^4 + 12\lambda^2\mu^2 + 4\mu^4 = (\lambda^2 - 2\mu^2)^2 + 16\lambda^2\mu^2 .$$

On en déduit $(-1/p) = (-1/q) = 1$. Contradiction.

(b) $p \in G$. - On suppose $(p/q) = 1$. La première descente montre que l'équation à étudier peut s'écrire :

$$pz^2 = -q^2x^4 + 4y^4 \quad \text{avec} \quad x \text{ et } y \text{ impairs}, \quad (y , q) = 1 .$$

On en déduit que $2y^2 + qx^2$ ou $2y^2 - qx^2$ est un carré, mais c'est impossible modulo 8 .

(c) $q \in G$. - On a alors $(q/p) = -1$, et l'équation à étudier s'écrit :

$$qz^2 = -x^4 + 4p^2y^4 \quad \text{avec} \quad x \text{ et } y \text{ impairs}, \quad (x , p) = 1 .$$

Un raisonnement identique montre que l'équation est impossible.

On a donc $g = 0$.

13. La deuxième descente pour $p = -1 \pmod 8$, $q = 3 \pmod 8$, $(p/q) = 1$.

(a) $pq \in G$. - Remplaçant z par pqz , on doit étudier l'équation :

$$pqz^2 = x^4 - 4y^4 \quad \text{avec} \quad x \text{ et } y \text{ impairs.}$$

Comme $(2/p) = (-2/q) = 1$, $(-2/p) = (2/q) = -1$, il existe des entiers u et v tels que

$$\begin{cases} x^2 - 2y^2 = pu^2 \\ x^2 + 2y^2 = qv^2 \\ z = uv . \end{cases}$$

Modulo p , on a :

$$x^2 = 2y^2 , \quad qv^2 = 4y^2 ,$$

d'où $(q/p) = 1$. Contradiction.

(b) $p \in G$. - La première descente montre que l'équation à étudier peut s'écrire

$$pz^2 = -q^2x^4 + 4y^4 \quad \text{avec} \quad x \text{ impair}, \quad y \text{ pair}, \quad (y , q) = 1 .$$

On en déduit que $2y^2 + qx^2$ ou $2y^2 - qx^2$ est un carré, mais c'est impossible modulo 8 .

(c) $q \in G$. - L'équation à étudier s'écrit :

$$qz^2 = -x^4 + 4p^2y^4 \quad \text{avec} \quad x \text{ et } y \text{ impairs}, \quad (x , p) = 1 .$$

Un raisonnement identique montre que l'équation est impossible.

On a donc $g = 0$.

Remarque. - Si on suppose $(p/q) = -1$, la deuxième descente ne donne aucune condition.

14. Les résultats.

Nous donnons ci-dessous les familles de nombres non congruents obtenus à partir des méthodes précédentes. La deuxième descente (et parfois un peu plus) a été faite pour les nombres produits de deux facteurs premiers impairs au plus lorsque le nombre de la première descente est 2 ; seule la première descente (à une exception près) a été faite pour les nombres produits de trois facteurs premiers impairs.

Les valeurs de p , q , r sont prises modulo 8 . Sont non congruents les nombres suivants :

$n = p$

$p = 3$

$p = 1$ avec $(-4/p)_8 = -1$ (ou $p = c^2 + 8d^2$ avec d impair)

$n = 2p$

$p = -3$

$p = 1$ avec $(-1/p)_8 = -1$ (ou $p = -7 \pmod{16}$)

$n = pq$

$p = 3$, $q = 3$

$p = 1$, $q = 1$ avec $\left(\frac{p}{q}\right) = -1$ et $\left(\frac{-4}{p}\right)_8 = -\left(\frac{-4}{q}\right)_8$ (ou $pq = c^2 + 8d^2$ avec d impair)

$p = -3$, $q = -3$ avec $(p/q) = 1$ et $(p/q)_4 = -(q/p)_4$

$p = -3$, $q = -3$ avec $(p/q) = -1$ et $((AB' + BA')/p) = 1$

$2p = A^2 + B^2$, $A = \pm 1 \pmod 8$, $B = \pm 3 \pmod 8$

$2q = A'^2 + B'^2$, $A' = \pm 1 \pmod 8$, $B' = \pm 3 \pmod 8$

$p = -1$, $q = -1$ avec $((EF' + FE')/p) = -1$

$p = E^2 - 2F^2$, $E > 0$, $F = 1 \pmod 4$

$q = E'^2 - 2F'^2$, $E' > 0$, $F' = 1 \pmod 4$

$p = 1$, $q = 3$ avec $(p/q) = -1$

$p = 1$, $q = 3$ avec $(p/q) = 1$ et $(q/p)_4 = -(-4/p)_8$

$p = -3$, $q = -1$, avec $(p/q) = -1$

$p = -3$, $q = -1$, avec $(p/q) = 1$ et $(q/p)_4 = 1$

$n = 2pq$

$p = -3$, $q = -3$

$p = 3$, $q = 3$

$p = 1$, $q = 1$, avec $\left(\frac{p}{q}\right) = -1$ et $\left(\frac{-1}{p}\right)_8 = -\left(\frac{-1}{q}\right)_8$ (ou $pq = -7 \pmod{16}$)

$p = -1$, $q = -1$, avec $(p/q) = 1$ et $q = 7 \pmod{16}$

$p = 1$, $q = -3$, avec $(p/q) = -1$

$p = 1$, $q = -3$, avec $(q/p)_4 = -(-1/p)_8$

$p = -1$, $q = 3$, avec $(p/q) = 1$

$n = pqr$

$p = -1$, $q = 3$, $r = -3$, avec $(p/r) = -1$

$p = 1$, $q = 3$, $r = 3$, avec $(p/q) = -(p/r)$

$p = 1$, $q = 1$, $r = 1$, avec la condition III ci-après et $pqr = c^2 + 8d^2$ avec d impair

$p = -1$, $q = -1$, $r = 3$, avec $(p/q) = (q/r) = (r/p)$

$p = 1$, $q = 1$, $r = 3$, avec la condition III ci-après

$p = 1$, $q = -1$, $r = -3$, avec la condition III ci-après

$p = 3$, $q = -3$, $r = -3$, avec la condition III ci-après

$p = 3$, $q = 3$, $r = 3$, avec la condition I ci-après

$n = 2pqr$

$p = 1$, $q = 3$, $r = 3$, avec $(p/q) = -(p/r)$

$p = 1$, $q = -3$, $r = -3$, avec $(p/q) = -(p/r)$

$p = -1$, $q = 3$, $r = -3$, avec $(p/q) = (p/r)$

$p = 1$, $q = 1$, $r = 1$, avec la condition III ci-après et $pqr = -7 \pmod{16}$

$p = -1$, $q = -1$, $r = -3$, avec $(p/q) = (p/r) = -(q/r)$

$p = 1$, $q = 1$, $r = -3$, avec la condition III ci-après

$p = 1$, $q = -1$, $r = 3$, avec la condition III ci-après

$p = 3$, $q = 3$, $r = -3$, avec la condition I ci-après

$p = -3$, $q = -3$, $r = -3$, avec la condition II ci-après

Condition I : $(p/q) = (p/r)$ ou $(q/r) = (q/p)$ ou $(r/p) = (r/q)$

Condition II : $(p/q) = (p/r) = 1$ ou $(q/r) = (q/p) = 1$ ou $(r/p) = (r/q) = 1$

Condition III : $(p/q) = (p/r) = -1$ ou $(q/r) = (q/p) = -1$ ou $(r/p) = (r/q) = -1$

15. Résultats numériques.

On prend $n < 1000$. Il y a 608 nombres "quadratfrei" qui se répartissent ainsi suivant le module 8 .

n mod 8	1	2	3	5	6	7
nombre des entiers QF	98	101	101	102	103	103

Sur les 300 nombres congrus à 1 , 2 , 3 (mod 8) les critères précédents donnent 227 nombres non congruents. Ils sont rassemblés dans la table ci-dessous.

Nombres non congruents

1	2	3	10	11	17	19	26	33	35
42	43	51	57	58	59	66	67	73	74
82	83	89	91	97	105	106	107	114	115
122	123	129	130	131	139	146	155	163	170
177	178	179	185	186	187	193	195	201	202
203	209	211	217	218	227	233	235	241	249
251	258	259	266	267	273	274	281	283	290
298	305	307	314	321	322	329	331	339	345
346	347	354	355	362	370	377	379	385	393
394	401	402	403	411	417	418	419	427	433
435	443	449	451	458	466	467	473	474	481
483	489	491	497	498	499	506	515	523	530
537	538	545	547	553	554	555	562	563	570
571	579	586	587	595	601	610	611	617	618
619	626	633	634	635	641	642	643	649	659
665	667	673	681	682	683	690	691	697	698
699	705	707	713	714	715	730	737	739	745
746	753	754	755	762	763	769	770	771	778
779	785	786	787	794	795	803	811	817	818
826	827	834	835	842	843	849	851	858	859
865	874	883	899	906	907	913	914	921	922
923	929	930	937	946	947	955	962	969	970
971	977	978	979	986	993	994			

BIBLIOGRAPHIE

[1] ALTER (R.), CURTZ (T. B.) and KUBOTA (K. K.). - Remarks and results on congruent numbers, "Proceedings of the 3rd southeastern conference on combinatorics, graph theory and computing [1972. Boca Raton]", p. 27-35. - Boca Raton, Florida Atlantic University, 1972.

[2] ALTER (R.) and CURTZ (T. B.). - A note on congruent numbers, Math. of comput., t. 28, 1974, p. 303-305.

[3] BARRUCAND (P.) and COHN (H.). - Note on primes of type $x^2 + 32y^2$, class number, and residuacity, J. reine angew. Math., t. 238, 1969, p. 67-70.

[4] BIRCH (B. J.). - Diophantine analysis and modular functions, "Algebraic geometry, Bombay Colloquium, 1968", p. 35-42. - Bombay, Tata Institute ; London, Oxford University Press, 1969 (Tata Institute of fundamental Research. Studies in Mathematics, 4).

[5] BIRCH (B. J.) and SWINNERTON-DYER (H. P. F.). - Notes on elliptic curves, II, J. reine angew. Math., t. 218, 1965, p. 79-108.

[6] BIRCH (B. J.) and STEPHENS (N. M.). - The parity of the rank of the Mordell-Weil group, Topology, t. 5, 1966, p. 295-299.

[7] CASSELS (J. W. S.). - Arithmetic on curves of genus 1, VIII, J. reine angew. Math., t. 217, 1965, p. 180-199.

[8] DIKSON (L. E.). - History of the theory of numbers, vol. 2. - New York, Chelsea publishing Company, 1952 (reprinted).

[9] HEEGNER (K.). - Diophantische Analysis and Modulfunktionen, Math. Z., t. 56, 1952, p. 227-253.

[10] LEHMER (E.). - On the quadratic character of some quadratic surds, J. reine angew. Math., t. 250, 1971, p. 42-48.

[11] TATE (J.). - Rational points on elliptic curves, Philips lectures, Haverford College, 1961.

[12] WIMAN (A.). - Uber rationale Punkte auf Kurven $y^2 = x(x^2 - c^2)$, Acta Math., Uppsala, t. 77, 1945, p. 281-320.

(Texte reçu le 21 avril 1975)

Jean LAGRANGE
Faculté des Sciences, Mathématiques
Moulin de la Housse
Boîte postale 347
51062 REIMS CEDEX