Sur l'équation $a^3 + b^3 = c^p$

Alain Kraus

TABLE DES MATIÈRES

Soit p un nombre premier ≥ 17. Cet article concerne l'équation diophantienne $a^3 + b^3 = c^p$. En supposant que la conjecture de Taniyama–Weil soit vraie, nous démontrons un critère permettant souvent de prouver que cette équation n'a pas de solution en nombres entiers non nuls a, b et c dans $\mathbb{Z}$ premiers entre eux. Nous vérifions en particulier que tel est bien le cas si p est < 10000.

Let p be a prime number ≥ 17. This paper deals with the diophantine equation $a^3 + b^3 = c^p$. If we suppose that the Taniyama–Weil conjecture is true, we get a criterion that often allows one to prove that this equation has no nonzero integer solution with a, b and c coprime. In particular, we verify that this is the case if p is < 10000.

NOTE AJOUTÉE AUX ÉPREUVES

Récemment B. Conrad, F. Diamond and R. Taylor ont démontré que toute courbe elliptique sur $\mathbb{Q}$ dont le conducteur n'est pas divisible par 27 est modulaire. Cela entraîne en particulier que la courbe $E(a,b)$ du paragraphe 4 est modulaire. Dans les énoncés des résultats obtenus dans cet article il est donc maintenant inutile de supposer que la conjecture de Taniyama–Weil est vraie.

1. INTRODUCTION

En supposant que la conjecture de Taniyama–Weil soit vraie, on se propose de faire quelques remarques sur la conjecture suivante :

Conjecture. *Soit p un nombre premier ≥ 3. L'équation*

$$a^3 + b^3 = c^p \tag{1–1}$$

n'a pas de solution a, b et c dans $\mathbb{Z}$, avec abc non nul et a, b, c premiers entre eux.

Conformément à la terminologie utilisée par H. Darmon [1993], nous dirons qu'un triplet d'entiers (a, b, c) est une solution de l'équation (1–1) si l'on a $a^3 + b^3 = c^p$, que cette solution est *propre* si l'on a $\mathrm{pgcd}(a, b, c) = 1$ et qu'elle est *non triviale* si abc est non nul.

H. Darmon et A. Granville [1995] ont démontré que l'équation (1–1) ne possède qu'un nombre fini de solutions propres.

1058-6458/1998 $0.50 per page

Si $p = 3$, l'énoncé de cette conjecture a été prouvé par Euler en 1753. Par ailleurs, Darmon et Granville [1995] ont abordé l'étude de l'équation (1–1). Ils démontrent que, si la conjecture de Taniyama–Weil est vraie, l'équation (1–1) ne possède pas de solution propre non triviale (a, b, c) si c est *pair* et si p est ≥ 17. Il semble que ce soient les seuls résultats déjà connus sur la conjecture précédente.

Signalons qu'il existe une infinité de solutions propres pour l'équation $a^3 + b^3 = c^2$ [Darmon et Granville 1995].

En supposant que la conjecture de Taniyama–Weil soit vraie, nous obtenons un énoncé permettant souvent en pratique de démontrer que l'équation (1–1) n'a pas de solution propre non triviale pour un exposant p donné. Cet énoncé permet par exemple de vérifier, en admettant la conjecture de Taniyama–Weil, qu'il en est bien ainsi, si l'on a $17 \leq p < 10000$. On peut en fait vérifier de la sorte, conjecturalement, que l'équation (1–1) n'a pas de solution propre non triviale, pour des nombres premiers p notablement plus grands que 10000 : tel est par exemple le cas pour $p = 350377$, qui est le trente millième nombre premier.

2. NOTATIONS

2A. Une formulation de la conjecture de Taniyama–Weil

Rappelons brièvement une des nombreuses formulations de la conjecture de Taniyama–Weil (voir par exemple [Serre 1996]). Soit A une courbe elliptique définie sur $\mathbb{Q}$. Soient N_A son conducteur et

$$s \mapsto \sum a_n(A) n^{-s}$$

la fonction L de Hasse–Weil de A. La courbe A est *modulaire* si la fonction, définie sur le demi-plan de Poincaré par

$$\tau \mapsto \sum a_n(A) q^n \qquad \text{avec} \quad q = e^{2\pi i \tau},$$

est une forme modulaire parabolique de poids 2 pour le sous-groupe $\Gamma_0(N_A)$ de $\mathrm{SL}_2(\mathbb{Z})$, formé des matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ telles que N_A divise c. La conjecture de Taniyama–Weil peut alors se formuler de la façon suivante :

Conjecture (Taniyama–Weil). *Toute courbe elliptique définie sur $\mathbb{Q}$ est modulaire.*

A. Wiles [1995] a démontré cette conjecture pour les courbes elliptiques sur $\mathbb{Q}$ qui sont semi-stables. F. Diamond [1996] a complété ce résultat en prouvant que les courbes elliptiques sur $\mathbb{Q}$ qui sont semi-stables en 3 et 5 sont modulaires.

2B. La courbe elliptique E

On désignera dans toute la suite par E la courbe elliptique sur $\mathbb{Q}$ d'équation

$$y^2 = x^3 + 6x - 7.$$

Il s'agit de la courbe elliptique, de conducteur 72, notée 72A dans les tables d'Antwerp [Birch et Kuyk 1975, p. 90]. Les invariants standards c_4, c_6 et Δ associés à cette équation sont (voir [Tate 1975, 1.]) :

$$c_4 = -2^5.3^2, \quad c_6 = 2^5.3^3.7 \quad \text{et} \quad \Delta = -2^4.3^7.$$

Cette équation est minimale sur $\mathbb{Q}$. Les types de réduction de E sont les suivants :

$$\begin{cases} \text{additif de type III en } 2 \\ \text{additif de type } \mathrm{I}_1^* \text{ en } 3 \\ \text{bonne réduction en dehors de } 2 \text{ et } 3. \end{cases} \tag{2–1}$$

Étant donné un nombre premier $l \geq 5$, on note $n_l(E)$ le nombre de points sur $\mathbb{F}_l$ de la courbe elliptique sur $\mathbb{F}_l$ déduite de E par réduction modulo l. On pose

$$a_l(E) = 1 + l - n_l(E). \tag{2–2}$$

(voir par exemple [Serre 1972, p. 303] pour l'interprétation de $a_l(E)$).

2C. La courbe elliptique E_ζ

Soient q un nombre premier ≥ 5 et n un entier ≥ 1 qui divise $q - 1$. Soit $\mu_n(\mathbb{F}_q)$ le sous-groupe des racines n-ièmes de l'unité du groupe $\mathbb{F}_q^*$. Le groupe $\mu_n(\mathbb{F}_q)$ est d'ordre n. On désigne par $A(n, q)$ le sous-ensemble de $\mu_n(\mathbb{F}_q)$ formé des éléments ζ satisfaisant à la condition suivante :

$$-\tfrac{1}{3} + 36\zeta \quad \text{est un carré dans } \mathbb{F}_q. \tag{2–3}$$

Considérons un élément ζ de $A(n,q)$. Soit δ_ζ le plus petit entier ≥ 0 tel que

$$\delta_\zeta^2 \text{ mod. } q = -\frac{1}{3} + 36\zeta$$

(δ_ζ existe par hypothèse). On associe à ζ l'équation de Weierstrass affine définie sur $\mathbb{F}_q$:

$$Y^2 = X^3 + \frac{1-27\zeta}{9} X + \delta_\zeta\Big(\frac{2+27\zeta}{81}\Big). \tag{2–4}$$

Le discriminant de (2–4) est $-2^4.3^3.\zeta^2$ [Tate 1975, § 1]. Il est en particulier non nul, et (2–4) représente donc une courbe elliptique E_ζ définie sur $\mathbb{F}_q$. Soit $n_q(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de E_ζ. On pose

$$a_q(\zeta) = q + 1 - n_q(\zeta). \tag{2–5}$$

3. ÉNONCÉ DES RÉSULTATS PRINCIPAUX

Le résultat principal que l'on a en vue est le suivant :

Théorème 3.1. *Soit p un nombre premier ≥ 17. Supposons que la conjecture de Taniyama–Weil soit vraie. Supposons de plus qu'il existe un entier $n \geq 1$ tel que les conditions suivantes soient réalisées* :

a) *le nombre $q = np + 1$ est premier* ;
b) *on a $a_q(E)^2 \not\equiv 4$ mod. p* ;
c) *pour tout élément ζ appartenant à $A(n,q)$, on a $a_q(\zeta)^2 \not\equiv a_q(E)^2$ mod. p.*

Alors l'équation $a^3 + b^3 = c^p$ n'a aucune solution propre non triviale.

On déduit de ce théorème les deux résultats ci-dessous :

Corollaire 3.2. *Supposons que la conjecture de Taniyama–Weil soit vraie. Soit p un nombre premier ≥ 17 tel que $q = 2p+1$ soit premier et que q soit un carré modulo 107 et modulo 109. Alors l'équation $a^3+b^3 = c^p$ n'a aucune solution propre non triviale.*

Corollaire 3.3. *Supposons que la conjecture de Taniyama–Weil soit vraie. Soit p un nombre premier vérifiant les inégalités $17 \leq p < 10000$. Alors l'équation $a^3 + b^3 = c^p$ n'a aucune solution propre non triviale.*

Remarques. 1) D'après le théorème de Dirichlet, il existe une infinité d'entiers n vérifiant la condition a) du théorème.

2) Les nombres premiers < 1000 qui satisfont aux hypothèses du corollaire 3.2 sont 41, 113, 131, 233, 509, 593, 653, 719, 761, 809. Une conjecture de Dickson [1904] implique en fait l'existence d'une infinité de tels nombres premiers (voir aussi [Ribenboim 1991, p. 180]).

3) Si la conjecture de Taniyama–Weil est vraie, le fait que l'équation $a^3+b^3 = c^p$ avec $p = 350377$ n'ait pas de solution propre non triviale, se démontre en utilisant le théorème 3.1 avec l'entier $n = 16$ (c'est le plus petit entier $n \geq 1$ possible).

4. LA COURBE ELLIPTIQUE $E(a, b)$

Soit p un nombre premier ≥ 5. Considérons une solution *propre non triviale* (a,b,c) de l'équation $a^3 + b^3 = c^p$. On supposera, ce qui n'est pas restrictif, que la condition suivante est satisfaite :

$$ac \text{ est } pair. \tag{4–1}$$

Darmon et Granville [1995] associent au triplet

$$(a,b,c)$$

une courbe elliptique définie sur $\mathbb{Q}$. Il s'agit, à $\mathbb{Q}$-isomorphisme près, de la courbe elliptique que l'on notera $E(a,b)$, d'équation

$$y^2 = x^3 + 3ab\ x + b^3 - a^3. \tag{4–2}$$

Les invariants standards $c_4(a,b)$, $c_6(a,b)$ et $\Delta(a,b)$ associés à l'équation (4–2) sont les suivants [Tate 1975, § 1] :

$$\begin{cases} c_4(a,b) = -2^4.3^2.ab, \\ c_6(a,b) = 2^5.3^3.(a^3 - b^3), \\ \Delta(a,b) = -2^4.3^3.c^{2p}. \end{cases} \tag{4–3}$$

Déterminons le conducteur $N_{E(a,b)}$ de $E(a,b)$. Désignons pour cela par $\mathcal{R}$ le produit des nombres premiers distincts de 2 et 3 qui divisent c, c'est-à-dire le plus grand entier sans facteur carré premier à 6 qui divise c. Étant donnés un entier n et un nombre premier l, on notera par ailleurs, *pour toute la suite*, $v_l(n)$ l'exposant de l dans la décomposition de n en facteurs premiers.

Lemme 4.1. a) *Supposons que c soit pair. On a*

$$N_{E(a,b)} = \begin{cases} 2.3^2.\mathcal{R} & si\ b \equiv -1 \text{ mod. } 4, \\ 2^4.3^2.\mathcal{R} & si\ b \equiv 1 \text{ mod. } 4. \end{cases}$$

b) *Supposons que c soit impair. On a*

$$N_{E(a,b)} = \begin{cases} 2^4.3^2.\mathcal{R} & si\ b \equiv -1 \text{ mod. } 4, \\ 2^3.3^2.\mathcal{R} & si\ v_2(a) = 1\ et\ b \equiv 1 \text{ mod. } 4, \\ 2^2.3^2.\mathcal{R} & si\ v_2(a) \geq 2\ et\ b \equiv 1 \text{ mod. } 4. \end{cases}$$

Démonstration. **1)** Soit l un nombre premier ≥ 5. Puisque les entiers a, b et c sont premiers entre eux, l'équation (4–2) est minimale en l et la courbe elliptique $E(a,b)$ a réduction semi-stable en l (voir formules (4–3)). On a donc

$$v_l(N_{E(a,b)}) = \begin{cases} 1 & \text{si } l \text{ divise } c, \\ 0 & \text{si } l \text{ ne divise pas } c. \end{cases} \tag{4–4}$$

2) Déterminons l'exposant de 2 dans $N_{E(a,b)}$.

2.1) Supposons que c soit *pair*. Dans ce cas ab est impair, car $\text{pgcd}(a,b,c) = 1$. On a $c^p = (a+b) \times (a^2 - ab + b^2)$ et le nombre $a^2 - ab + b^2$ est impair. Puisque p est ≥ 5, on a donc

$$a + b \equiv 0 \text{ mod. } 32. \tag{4–5}$$

Par ailleurs, on a $a^3 - b^3 = (a-b)(a^2 + ab + b^2)$. Puisque a et b sont impairs, il résulte de la congruence (4–5) que 4 ne divise pas $a - b$. On a donc

$$v_2(a - b) = v_2(a^3 - b^3) = 1. \tag{4–6}$$

2.1.1) Supposons $b \equiv -1$ mod. 4. En effectuant le changement de variables

$$\begin{cases} x = 4X + b \\ y = 8Y + 4X, \end{cases}$$

on obtient comme nouveau modèle entier pour la courbe $E(a,b)$:

$$Y^2 + XY = X^3 + \frac{3b-1}{4}X^2 + 3b\frac{a+b}{16}X + \frac{2b^3 - a^3 + 3ab^2}{64}. \tag{4–7}$$

Les invariants c_4, c_6 et Δ de cette équation sont $c_4 = -3^2.ab$,

$$c_6 = 3^3.\frac{a^3 - b^3}{2} \quad \text{et} \quad \Delta = -\frac{3^3.c^{2p}}{2^8}.$$

L'équation (4–7) définit donc un modèle minimal de $E(a,b)$. On déduit de là que, sous l'hypothèse 2.1.1), $E(a,b)$ a réduction multiplicative en 2. D'où $v_2(N_{E(a,b)}) = 1$ dans ce cas.

2.1.2) Supposons $b \equiv 1$ mod. 4. D'après les formules (4–3) et (4–6) on a les égalités $v_2(c_4(a,b))=4$, $v_2(c_6(a,b)) = 6$ et

$$v_2(\Delta(a,b)) = 2pv_2(c) + 4.$$

Avec la terminologie utilisée dans [Papadopoulos 1993], on est donc amené à décider si l'on est dans le cas 7 de Tate ou dans un cas suivant [Papadopoulos 1993, tableau IV p. 129, et p. 125]. Les invariants standards b_2, b_4, b_6 et b_8 associés à l'équation (4–2) sont :

$$\begin{aligned} b_2 &= 0, & b_4 &= 6ab, \\ b_6 &= 4(b^3 - a^3), & b_8 &= -9a^2b^2. \end{aligned} \tag{4–8}$$

D'après la proposition 4 de [Papadopoulos 1993, p. 125], appliquée, avec ses notations, avec $r = -a$, on constate que l'on est dans le cas 7 de Tate, et que le type de Néron de $E(a,b)$ en 2 est I_ν^* avec $\nu = 2pv_2(c) - 4$. D'où $v_2(N_{E(a,b)}) = 4$ dans ce cas.

2.2) Supposons que c soit *impair*. D'après la condition (4–1), a est donc pair et b est impair. On a donc $v_2(c_4(a,b)) = 4 + v_2(a) \geq 5$,

$$v_2(c_6(a,b)) = 5 \quad \text{et} \quad v_2(\Delta(a,b)) = 4.$$

2.2.1) Supposons $b \equiv -1$ mod. 4. On est dans le cas 3, 4 ou 5 de Tate [Papadopoulos 1993, tableau IV p. 129]. Afin de déterminer dans quel cas l'on se trouve, on utilise la proposition 1 p. 224 du même article : avec ses notations on peut prendre $r = 2$ et $t = 1$. Puisque le nombre $b^3 - a^3 + 6ab + 7$ n'est pas multiple de 4, on est donc dans le cas 3 de Tate. D'où $v_2(N_{E(a,b)}) = 4$ dans ce cas.

2.2.2) Supposons $b \equiv 1$ mod. 4. Il résulte de l'alinéa précédent que l'on est dans le cas 4 ou 5 de Tate. D'après la proposition 2 de [Papadopoulos 1993], appliquée avec $r = 2$, et la formule (4–8), on constate que si $v_2(a) = 1$, on est dans le cas 4 de Tate et l'on a $v_2(N_{E(a,b)}) = 3$, et que par ailleurs, si $v_2(a) \geq 2$, on est dans le cas 5 de Tate et l'on a alors $v_2(N_{E(a,b)}) = 2$.

3) Déterminons maintenant l'exposant de 3 dans $N_{E(a,b)}$.

3.1) Supposons que 3 divise c. Sous cette hypothèse 3 ne divise pas ab. D'après l'égalité (1–1), on a $a \equiv -b$ mod. 3 et 3 ne divise pas $a^3 - b^3$. On a donc $v_3(c_4(a,b)) = 2$,

$$v_3(c_6(a,b)) = 3 \quad \text{et} \quad v_3(\Delta(a,b)) = 3 + 2pv_3(c).$$

Le type de Néron de $E(a,b)$ en 3 est donc I_ν^* avec $\nu = 2pv_3(c) - 3$ [Papadopoulos 1993, tableau II p. 126]. D'où $v_3(N_{E(a,b)}) = 2$ dans ce cas.

3.2) Supposons que 3 divise ab. On a dans ce cas $v_3(c_4(a,b)) \geq 3$,

$$v_3(c_6(a,b)) = 3 \quad \text{et} \quad v_3(\Delta(a,b)) = 3.$$

On regarde alors la condition P_2 intervenant dans le tableau II [Papadopoulos 1993, p. 123] : il s'agit de décider si l'on a

$$(2^5.(a^3 - b^3))^2 + 2 \equiv -3.2^4.ab \text{ mod. } 9.$$

On constate alors que tel est bien le cas. Le type de Néron de $E(a,b)$ en 3 est donc III. D'où encore $v_3(N_{E(a,b)}) = 2$.

3.3) Supposons que 3 ne divise pas abc. On a dans ce cas $v_3(c_4(a,b)) = 2$,

$$v_3(c_6(a,b)) \geq 3 \quad \text{et} \quad v_3(\Delta(a,b)) = 3.$$

Comme 3 ne divise pas c, on a d'après l'égalité (1–1) $a \equiv b$ mod. 3 et donc $a^3 - b^3 \equiv 0$ mod. 9. D'où $v_3(c_6(a,b)) \geq 5$. Le type de Néron de $E(a,b)$ en 3 est donc III, et l'on a encore $v_3(N_{E(a,b)}) = 2$. Cela termine la démonstration du lemme 4.1 (voir formule (4–4) ci-dessus). □

5. LA REPRÉSENTATION MODULAIRE $\rho_p^{a,b}$

Considérons dans ce paragraphe un nombre premier $p \geq 17$ et (a,b,c) une solution *propre non triviale* de l'équation $a^3 + b^3 = c^p$, telle que ac soit *pair* (condition (4–1)). Soient $\bar{\mathbb{Q}}$ une clôture algébrique de $\mathbb{Q}$ et $E(a,b)[p]$ le sous-groupe des points de p-torsion de $E(a,b)(\bar{\mathbb{Q}})$. On note

$$\rho_p^{a,b} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E(a,b)[p])$$

la représentation donnant l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur $E(a,b)[p]$. J.-P. Serre [1987, § 1, p. 180] associe à $\rho_p^{a,b}$ un conducteur $N(\rho_p^{a,b})$, qui est entier ≥ 1 et premier à p. Déterminons maintenant $N(\rho_p^{a,b})$:

Lemme 5.1. a) *Supposons que c soit pair. On a*

$$N(\rho_p^{a,b}) = \begin{cases} 2.3^2 & si\ b \equiv -1 \text{ mod. } 4 \\ 2^4.3^2 & si\ b \equiv 1 \text{ mod. } 4. \end{cases}$$

b) *Supposons que c soit impair. On a*

$$N(\rho_p^{a,b}) = \begin{cases} 2^4.3^2 & si\ b \equiv -1 \text{ mod. } 4 \\ 2^3.3^2 & si\ v_2(a) = 1\ et\ b \equiv 1 \text{ mod. } 4 \\ 2^2.3^2 & si\ v_2(a) \geq 2\ et\ b \equiv 1 \text{ mod. } 4. \end{cases}$$

Démonstration. Soit l un nombre premier ≥ 5 distinct de p. La courbe $E(a,b)$ a réduction semistable en l (lemme 4.1) et l'exposant de l dans le discriminant minimal de $E(a,b)$ est multiple de p (formules (4–3)). Le lemme 5.1 est alors une conséquence directe du lemme 4.1 et de la proposition de [Kraus 1997, II]; voir aussi [Serre 1987, p. 201, (4.1.12)]. □

Lemme 5.2. *La représentation $\rho_p^{a,b}$ est irréductible.*

Démonstration. Supposons que $\rho_p^{a,b}$ soit réductible. D'après un résultat de B. Mazur, puisque p est ≥ 17, l'invariant modulaire $j(a,b)$ de $E(a,b)$ doit appartenir à $\mathbb{Z}[\frac{1}{2}]$, et si p est distinct de 17, $j(a,b)$ doit être en fait dans $\mathbb{Z}$: voir par exemple [Darmon

1993, p. 266, proposition 1.5]. Or on a l'égalité (formules (4–3))

$$j(a,b) = \frac{2^8.3^3.(ab)^3}{c^{2p}}. \tag{5–1}$$

Si p est distinct de 17, on a ainsi $c = \pm 1$ et $ab = 0$, ce qui conduit à une contradiction. Supposons maintenant $p = 17$. Nécessairement c doit alors être une puissance de 2. On a donc $(a+b)(a^2 - ab + b^2) = \pm 2^{17k}$ pour un certain entier $k \geq 0$. On peut supposer $k \geq 1$ (sinon on a encore $ab = 0$). Dans ce cas c est pair, ab est impair et $a^2 - ab + b^2$ est impair ; d'où $a^2 - ab + b^2 = 1$. Cela entraîne $ab = 0$ ou $ab = 1$, ce qui conduit de nouveau à une contradiction. D'où le lemme. □

J.-P. Serre associe par ailleurs à $\rho_p^{a,b}$ un poids k, qui est entier ≥ 2, et qui ne dépend que de la restriction de $\rho_p^{a,b}$ à un sous-groupe d'inertie en p de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ [Serre 1987, § 2, p. 182].

Lemme 5.3. *On a $k = 2$.*

Démonstration. Si p ne divise pas c, $E(a,b)$ a bonne réduction en p. Sinon $E(a,b)$ a réduction de type multiplicatif en p et l'exposant de p dans le discriminant minimal de $E(a,b)$ est multiple de p. D'où le lemme ; voir [Serre 1987, p. 191, proposition 5]. □

Identifions désormais $\bar{\mathbb{Q}}$ à un sous-corps de $\mathbb{C}$. Étant donné un entier $n \geq 1$, on note $S_2(n)$ le $\mathbb{C}$-espace vectoriel des formes modulaires paraboliques de poids 2 et de caractère trivial pour le sous-groupe de congruence $\Gamma_0(n)$ de $\mathrm{SL}_2(\mathbb{Z})$ (cf. 2A). Soit $S_2^{\mathrm{new}}(n)$ le sous-espace vectoriel de $S_2(n)$ engendré par les newforms au sens des définitions qui figurent dans [Atkin et Lehner 1970]. Soit

$$s \mapsto \sum a_n\big(E(a,b)\big) n^{-s}$$

la fonction L de Hasse–Weil de $E(a,b)$.

Proposition 5.4. *Supposons que la courbe elliptique $E(a,b)$ soit modulaire. Il existe une newform de*

$$S_2^{\mathrm{new}}\big(N(\rho_p^{a,b})\big),$$

dont le développement de Taylor à l'infini est

$$\tau \mapsto q + \sum_{n \geq 2} a_n q^n \quad \text{où } q = e^{2\pi i \tau},$$

et une place $\wp$ de $\bar{\mathbb{Q}}$ de caractéristique résiduelle p, telles que pour tout nombre premier l qui ne divise pas $pN_{E(a,b)}$, l'on ait

$$a_l \equiv a_l\big(E(a,b)\big) \bmod. \wp. \tag{5–2}$$

Démonstration. L'hypothèse faite sur $E(a,b)$ signifie que, dans la terminologie de [Serre 1996], $\rho_p^{a,b}$ est modulaire de poids 2 et de caractère trivial pour $\Gamma_0\big(N_{E(a,b)}\big)$. D'après les lemmes 5.2 et 5.3, $\rho_p^{a,b}$ est donc modulaire de poids 2 et de caractère trivial pour $\Gamma_0\big(N(\rho_p^{a,b})\big)$ [Serre 1996, Remarques 2]. Il existe donc une newform de $S_2^{\mathrm{new}}\big(N(\rho_p^{a,b})\big)$, et une place $\wp$ de $\bar{\mathbb{Q}}$ de caractéristique résiduelle p, comme indiquées dans l'énoncé de la proposition, telles que les congruences (5–2) soient satisfaites ; voir [Serre 1987, p. 196 (3.2.5), et p. 197, alinéa (5)] et [Serre 1972, p. 303, 5.2, ii)]. D'où la proposition. □

6. CONSÉQUENCES SUR L'ÉQUATION $a^3 + b^3 = c^p$

Considérons maintenant, comme dans le paragraphe 5, un nombre premier $p \geq 17$ et (a,b,c) une solution *propre non triviale* de l'équation $a^3 + b^3 = c^p$ telle que ac soit *pair*. Nous allons démontrer le résultat suivant :

Théorème 6.1. *Supposons que la conjecture de Taniyama–Weil soit vraie.*

a) *Le nombre c est impair.*

b) *On a $v_2(a) = 1$.*

c) *On a $v_3(c) \geq 1$.*

La démonstration occupera le reste de ce paragraphe. Rappelons que l'assertion a), signalée dans l'introduction, a déjà été démontrée dans [Darmon et Granville 1995] : supposons que c soit pair. On peut supposer que l'on a $b \equiv -1 \bmod. 4$. La représentation $\rho_p^{a,b}$ est alors modulaire de poids 2 pour $\Gamma_0(18)$ (lemme 5.1 et proposition 5.4). Mais il n'existe pas de newform normalisée dans $S_2(18)$. D'où l'assertion a).

Démonstration de l'assertion b). Il résulte de l'assertion a) que l'on peut supposer *désormais* que les conditions suivantes sont satisfaites :

$$a \text{ est } \textit{pair} \quad \text{et} \quad b \equiv 1 \text{ mod. } 4. \tag{6–1}$$

Considérons alors la courbe elliptique E' d'équation

$$y^2 = x^3 + 1.$$

Il s'agit de la courbe elliptique de conducteur 36, notée 36A dans les tables d'Antwerp [Birch et Kuyk 1975, p. 84]. Les types de réduction de E sont donnés dans les mêmes tables ; ils sont les suivants :

$$\begin{cases} \text{additif de type IV en 2} \\ \text{additif de type III en 3} \\ \text{bonne réduction en dehors de 2 et 3.} \end{cases}$$

La courbe E' est à multiplications complexes par le corps $\mathbb{Q}(\sqrt{-3})$. Soit $E'[p]$ le sous-groupe des points de p-torsion de $E'(\bar{\mathbb{Q}})$. On note

$$\rho'_p : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E'[p])$$

la représentation donnant l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur $E'[p]$. Décrivons le sous-groupe de $\mathrm{Aut}(E'[p])$ image de la représentation ρ'_p [Serre 1972, § 2, p. 278].

Lemme 6.2. i) *Si l'on a* $p \equiv 1$ mod. 3 *l'image de* ρ'_p *est contenue dans le normalisateur d'un sous-groupe de Cartan déployé.*

ii) *Si l'on a* $p \equiv 2$ mod. 3 *l'image de* ρ'_p *est le normalisateur d'un sous-groupe de Cartan non déployé.*

Démonstration. Si l'on a $p \equiv 1$ mod. 3, p est décomposé dans $\mathbb{Q}(\sqrt{-3})$, et donc l'image de ρ'_p est contenue dans le normalisateur d'un sous-groupe de Cartan déployé. Si l'on a $p \equiv 2$ mod. 3, p est inerte dans $\mathbb{Q}(\sqrt{-3})$, et l'image de ρ_p est contenue dans le normalisateur d'un sous-groupe de Cartan non déployé. En fait si l'on a $p \equiv 2$ mod. 3, E' a bonne réduction de hauteur 2 en p [Silverman 1986, p. 143–144], et l'étude de la restriction de ρ'_p à un sous-groupe de décomposition en p de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ montre que l'image de ρ'_p est le normalisateur tout entier d'un sous-groupe de Cartan non déployé [Serre 1972, p. 275, proposition 12]. D'où le lemme. □

Notons alors ρ_p la représentation donnant l'action de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ sur le sous-groupe des points de p-torsion de $E(\bar{\mathbb{Q}})$, où E est la courbe elliptique notée 72A dans les tables d'Antwerp (cf. paragraphe 2B).

Proposition 6.3. *Supposons que la courbe elliptique* $E(a,b)$ *soit modulaire.*

i) *Si l'on a* $v_2(a) \geq 2$, *les représentations* $\rho_p^{a,b}$ *et* ρ'_p *sont isomorphes.*

ii) *Si l'on a* $v_2(a) = 1$, *les représentations* $\rho_p^{a,b}$ *et* ρ_p *sont isomorphes.*

Démonstration. Supposons que l'on ait $v_2(a) \geq 2$. La courbe elliptique E' est modulaire, car elle est à multiplications complexes. Par ailleurs, il existe une unique newform normalisée de $S_2^{\mathrm{new}}(36)$; il s'agit donc de celle qui correspond à E'. D'après la condition (6–1), le lemme 5.1 et la proposition 5.4, les semi-simplifiées de $\rho_p^{a,b}$ et ρ'_p sont donc isomorphes (voir les congruences (5–2)). Puisque $\rho_p^{a,b}$ est irréductible (lemme 5.2) cela entraîne l'assertion i).

Supposons que l'on ait $v_2(a) = 1$. La courbe elliptique E est aussi modulaire : en effet, E est isogène à la courbe notée 72F dans les tables de [Birch et Kuyk 1975, p. 90], qui est tordue quadratique d'une courbe elliptique modulaire (celle notée 24F dans [Birch et Kuyk 1975, p. 83], qui est modulaire car la dimension de $S_2(24)$ est 1). Il existe par ailleurs une unique newform normalisée de $S_2^{\mathrm{new}}(72)$; c'est donc celle qui correspond à E. Les représentations $\rho_p^{a,b}$ et ρ_p ont donc des simplifiées isomorphes (condition (6–1), le lemme 5.1 et la proposition 5.4), et elles sont isomorphes car $\rho_p^{a,b}$ est irréductible. D'où la proposition. □

Lemme 6.4. *Supposons que* $E(a,b)$ *soit modulaire. Alors* c *n'est pas divisible par* p.

Démonstration. Soit

$$s \mapsto \sum a_n(E')n^{-s}$$

la fonction L de Hasse–Weil de E'. Supposons que p divise c. Alors $E(a,b)$ a réduction de type multiplicatif en p. Par ailleurs, les courbes E et E' ont bonne réduction en p. Il résulte de la proposition 6.3 et de [Kraus et Oesterlé 1992, proposition 3(iii)] que l'on a

$$(a_p(E)^2 - 1)(a_p(E')^2 - 1) \equiv 0 \text{ mod. } p.$$

Puisque que l'on a les inégalités $\left|a_p(E)\right| \leq 2\sqrt{p}$ et $\left|a_p(E')\right| \leq 2\sqrt{p}$ [Silverman 1986, p. 131, théorème 1.1], cela entraîne $a_p(E) = \pm 1$ ou $a_p(E') = \pm 1$. Mais cela contredit le fait que E et E' possèdent chacune un point d'ordre 2 rationnel sur $\mathbb{Q}$ (cf. formule (2–2)). D'où le lemme. □

Terminons maintenant la démonstration de l'assertion b) du théorème 6.1. Supposons pour cela que l'on ait $v_2(a) \geq 2$.

1) Supposons $p \equiv 1$ mod. 3. D'après le lemme 6.2 et la proposition 6.3, l'image de $\rho_p^{a,b}$ est contenue dans le normalisateur d'un sous-groupe de Cartan déployé. Il résulte alors de [Halberstadt et Kraus 1996, théorème 1] que le conducteur de $E(a,b)$ doit être 36. Par ailleurs toute courbe elliptique de conducteur 36 étant modulaire, la liste des courbes elliptiques de conducteur 36 qui se trouvent dans [Birch et Kuyk 1975, p. 84] est exhaustive. Il y en a quatre à $\mathbb{Q}$-isomorphisme près. Le corps des points de 2-torsion de $E(a,b)$ étant $\mathbb{Q}(\sqrt{-3})$, $E(a,b)$ est nécessairement $\mathbb{Q}$-isomorphe à la courbe 36A ou 36C (le corps des points de 2-torsion de la 36B et celui de la 36D est $\mathbb{Q}(\sqrt{3})$). L'invariant modulaire de $E(a,b)$ est donc nul. D'où $ab = 0$ (formule (5–1)), ce qui conduit à une contradiction.

2) Supposons $p \equiv 2$ mod. 3. On utilise dans ce cas les résultats obtenus par Darmon et Merel [1997]. D'après le lemme 6.2 et la proposition 6.3 l'image de $\rho_p^{a,b}$ est le normalisateur d'un sous-groupe de Cartan non déployé. Par ailleurs la courbe $E(a,b)$ possède un point d'ordre 2 sur $\mathbb{Q}$: le point de coordonnées $(x,y) = (a-b, 0)$. Il résulte alors de [Darmon et Merel 1997, théorème 8.1] que l'invariant modulaire de $E(a,b)$ appartient à $\mathbb{Z}[\frac{1}{p}]$. Cela entraîne que c est une puissance de p (cf. formule (5–1)). D'après le lemme 6.4 cela entraîne $c = \pm 1$. On déduit de là que ab est nul, ce qui n'est pas. Cela prouve l'assertion. □

Démonstration de l'assertion c). D'après l'assertion b) précédente, on a $v_2(a) = 1$ et donc les représentations $\rho_p^{a,b}$ et ρ_p sont isomorphes (proposition 6.3). Supposons que 3 ne divise pas c. Dans ce cas la courbe $E(a,b)$ a potentiellement bonne réduction en 3. Considérons alors le groupe Φ_3 défini dans [Serre 1972, p. 311], mesurant le défaut de semi-stabilité de $E(a,b)$ en 3. Il est d'ordre 4 ou 12 [Kraus 1990, p. 355–356, corollaire]. En fait le groupe Φ_3 est d'ordre 4 car le type de Néron de $E(a,b)$ en 3 est III (voir [Kraus 1990, corollaire] et la démonstration du lemme 4.1). Si I_3 est un sous-groupe d'inertie en 3 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, cela signifie que le cardinal de $\rho_p^{a,b}(I_3)$ est 4. Mais le type de Néron de E en 3 est I_1^* (voir (2–1)) et en particulier E a potentiellement réduction de type multiplicatif en 3. Il résulte alors de la théorie de la courbe de Tate que p divise l'ordre de $\rho_p(I_3)$ [Silverman 1986, p. 357]. Cet ordre est donc distinct de 4, ce qui conduit à une contradiction. D'où le résultat. □

7. DÉMONSTRATION DES RÉSULTATS PRINCIPAUX

Soient p un nombre premier ≥ 17. Considérons une solution *propre non triviale* (a,b,c) de l'équation $a^3 + b^3 = c^p$ telle que a soit *pair* (cela n'est pas restrictif car c est impair).

Démonstration du théorème 3.1.

Lemme 7.1. *On a* $v_3(a+b) = pv_3(c) - 1$ *et*

$$v_3(a^2 - ab + b^2) = 1.$$

Le seul diviseur premier commun à $a^2 - ab + b^2$ *et* $a + b$ *est* 3.

Démonstration. On a $c^p = (a+b)(a^2 - ab + b^2)$. D'après le théorème 6.1, on a $v_3(c) \geq 1$. Ainsi 3 ne divise pas ab et l'on a la congruence $a \equiv -b$ mod. 3. Or on a l'égalité $a^2 - ab + b^2 = (a+b)^2 - 3ab$. On déduit de là que $v_3(a^2 - ab + b^2) = 1$. Par ailleurs si l est un nombre premier qui divise $a+b$ et $a^2 - ab + b^2$, alors l divise $3ab$. Puisque a et b sont premiers entre eux, cela implique $l = 3$. D'où le lemme. $\square$

Posons $\lambda = pv_3(c) - 1$. D'après le lemme 7.1 il existe des entiers c_1 et c_2 premiers à 3, tels que $c = 3^{v_3(c)} c_1 c_2$, et que

$$\begin{cases} a + b = 3^\lambda c_1^p, \\ a^2 - ab + b^2 = 3c_2^p. \end{cases}$$

Autrement dit, il existe deux entiers α et β tels que l'on ait

$$\begin{cases} 3(a+b) = \alpha^p \\ a^2 - ab + b^2 = 3\beta^p, \end{cases} \tag{7–1}$$

où $\alpha = 3^{v_3(c)} c_1$ et $\beta = c_2$.

Considérons alors un entier n vérifiant les conditions de l'énoncé du théorème 3.1 (en particulier $q = np + 1$ est un nombre premier).

Lemme 7.2. *Le nombre c n'est pas divisible par q (la courbe $E(a,b)$ a donc bonne réduction en q).*

Démonstration. Supposons que q divise c. La courbe $E(a,b)$ a alors réduction de type multiplicatif en q. Par ailleurs, $E(a,b)$ est par hypothèse modulaire, et donc les représentations $\rho_p^{a,b}$ et ρ_p sont isomorphes (cf. les assertions b) et ii) du théorème 6.1 et de la proposition 6.3). Puisque E a bonne réduction en q, on a donc la congruence

$$a_q(E) \equiv \pm(q+1) \text{ mod. } p,$$

c'est-à-dire

$$a_q(E) \equiv \pm 2 \text{ mod. } p,$$

ce qui contredit la condition b) du théorème [Kraus et Oesterlé 1992, proposition 3(iii)]. $\square$

Puisque n divise $q-1$, les racines n-ièmes de l'unité sont dans $\mathbb{F}_q$. D'après le lemme 7.2, q ne divise pas $\alpha\beta$, et donc α^p mod. q et β^p mod. q sont des racines n-ièmes de l'unité dans $\mathbb{F}_q$. Notons $\bar{a}$ et $\bar{b}$ les réductions de a et b modulo q. On déduit alors des égalités (7–1) l'existence d'un couple (u,v) de racines n-ièmes de l'unité dans $\mathbb{F}_q$, tel que l'on ait

$$\begin{cases} 3(\bar{a} + \bar{b}) = u \\ \bar{a}^2 - \bar{a}\bar{b} + \bar{b}^2 = 3v. \end{cases}$$

Posons

$$\bar{a}' = \frac{\bar{a}}{u}, \quad \bar{b}' = \frac{\bar{b}}{u} \quad \text{et} \quad \zeta = \frac{v}{u^2}.$$

On obtient ainsi l'égalité

$$3\bar{b}'^2 - \bar{b}' + \tfrac{1}{9} - 3\zeta = 0.$$

On déduit de là que ζ appartient à $A(n,q)$ (voir la condition (2–3)) et que l'on a

$$(\bar{a}', \bar{b}') = \Big(\frac{1 - \delta_\zeta \text{ mod. } q}{6}, \frac{1 + \delta_\zeta \text{ mod. } q}{6}\Big)$$

ou bien

$$(\bar{a}', \bar{b}') = \Big(\frac{1 + \delta_\zeta \text{ mod. } q}{6}, \frac{1 - \delta_\zeta \text{ mod. } q}{6}\Big).$$

On vérifie alors que la courbe elliptique sur $\mathbb{F}_q$ déduite de $E(a,b)$ par réduction modulo q est la courbe elliptique sur $\mathbb{F}_q$ déduite de E_ζ par torsion quadratique par $\sqrt{\pm u}$. D'après les assertions b) et ii) du théorème 6.1 et de la proposition 6.3, on a donc

$$a_q(\zeta)^2 \equiv a_q(E)^2 \text{ mod. } p$$

(voir formule (2–5)), ce qui contredit la condition c) du théorème. On aboutit ainsi à une contradiction, ce qui prouve que le triplet (a,b,c) n'existe pas, et termine la démonstration du théorème 3.1. $\square$

Démonstration du corollaire 3.2. Vérifions que les conditions du théorème 3.1 sont réalisées avec l'entier $n = 2$. Par hypothèse $q = 2p + 1$ est premier. De l'inégalité

$$\left| a_q(E) \pm 2 \right| \leq 2(\sqrt{q} + 1) < p,$$

on déduit que la condition b) du théorème est équivalente à $a_q(E) \neq \pm 2$. Tel est bien le cas. En effet, E possède un point d'ordre 4 rationnel sur $\mathbb{Q}$: le point de coordonnées $(x,y) = (4,9)$. Ainsi 4 divise $n_q(E)$, ce qui implique $a_q(E) \neq \pm 2$ (voir formule

(2–2)). Par ailleurs si q est un carré modulo 107 et modulo 109, l'ensemble $A(2,q)$ est vide, de sorte que la condition c) du théorème est aussi satisfaite. Le corollaire est alors une conséquence directe du théorème. □

Démonstration du corollaire 3.3. Étant donné un nombre premier p compris entre 17 et 10000, on a déterminé un entier $n \geq 1$, en fait le plus petit entier $n \geq 1$ possible, tel que les conditions du théorème 3.1 soient satisfaites, ce qui prouve ainsi le corollaire. On a utilisé pour cela le logiciel PARI [Batut, Bernardi, Cohen et Olivier 1995]. Ces couples (p,n) sont donnés dans le tableau 1. □

REMERCIEMENTS

Je remercie D. Bernardi pour les nombreuses conversations que nous avons eues concernant le logiciel PARI, et H. Darmon qui m'a suggéré une amélioration de la présentation d'une version préliminaire du théorème 3.1.

BIBLIOGRAPHIE

[Atkin et Lehner 1970] A. O. L. Atkin et J. Lehner, "Hecke operators on $\Gamma_0(m)$", *Math. Ann.* **185** (1970), 134–160.

[Batut, Bernardi, Cohen et Olivier 1995] C. Batut, D. Bernardi, H. Cohen et M. Olivier, *User's Guide to Pari-GP* 1.39, Université de Bordeaux, 1995. Voir ftp://megrez.math.u-bordeaux.fr/pub/pari.

[Birch et Kuyk 1975] B. J. Birch et W. Kuyk, "Numerical tables on elliptic curves", pp. 74–150 dans *Modular functions of one variable, IV* (Antwerp, 1972), édité par B. J. Birch et W. Kuyk, Lecture Notes in Math. **476**, Springer, Berlin, 1975.

[Darmon 1993] H. Darmon, "The equations $x^n+y^n=z^2$ and $x^n+y^n=z^3$", *Internat. Math. Res. Notices* **7**:10 (1993), 263–274.

[Darmon et Granville 1995] H. Darmon et A. Granville, "On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$", *Bull. London Math. Soc.* **27**:6 (1995), 513–543.

[Darmon et Merel 1997] H. Darmon et L. Merel, "Winding quotients and some variants of Fermat's last theorem", *J. Reine Angew. Math.* **490** (1997), 81–100.

[Diamond 1996] F. Diamond, "On deformation rings and Hecke rings", *Ann. of Math.* (2) **144**:1 (1996), 137–166.

[Dickson 1904] L. E. Dickson, "A new extension of Dirichlet's theorem on prime numbers", *Messenger of Math.* **33** (1904), 155–161.

[Halberstadt et Kraus 1996] E. Halberstadt et A. Kraus, "Sur la comparaison galoisienne des points de torsion des courbes elliptiques", *C. R. Acad. Sci. Paris Sér. I Math.* **322**:4 (1996), 313–316.

[Kraus 1990] A. Kraus, "Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive", *Manuscripta Math.* **69**:4 (1990), 353–385.

[Kraus 1997] A. Kraus, "Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique", *Dissertationes Math.* **344** (1997), 39 pp.

[Kraus et Oesterlé 1992] A. Kraus et J. Oesterlé, "Sur une question de B. Mazur", *Math. Ann.* **293**:2 (1992), 259–275.

[Papadopoulos 1993] I. Papadopoulos, "Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3", *J. Number Theory* **44**:2 (1993), 119–152.

[Ribenboim 1991] P. Ribenboim, *The little book of big primes*, Springer, New York, 1991.

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331.

[Serre 1987] J.-P. Serre, "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$", *Duke Math. J.* **54**:1 (1987), 179–230.

[Serre 1996] J.-P. Serre, "Travaux de Wiles (et Taylor, ...), I", pp. 319–332 (Exp. No. 803) dans *Séminaire Bourbaki,* 1994/95, Astérisque **237**, Soc. math. France, Paris, 1996.

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., Springer, New York, 1986.

[Tate 1975] J. Tate, "Algorithm for determining the type of a singular fiber in an elliptic pencil", pp. 33–52 dans *Modular functions of one variable, IV* (Antwerp, 1972), Lecture Notes in Math. **476**, Springer, Berlin, 1975.

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551.

p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n
17	6	241	10	523	12	829	10	1153	22	1489	10	1847	6	2207	8	2557	18	2909	18	3319	10
19	10	251	2	541	18	839	12	1163	32	1493	14	1861	40	2213	12	2579	12	2917	24	3323	12
23	2	257	6	547	10	853	4	1171	6	1499	2	1867	10	2221	6	2591	18	2927	8	3329	2
29	2	263	6	557	6	857	8	1181	12	1511	2	1871	8	2237	14	2593	6	2939	2	3331	10
31	10	269	8	563	14	859	22	1187	8	1523	14	1873	6	2239	10	2609	8	2953	4	3343	22
37	4	271	10	569	12	863	6	1193	6	1531	6	1877	8	2243	32	2617	10	2957	14	3347	8
41	2	277	6	571	10	877	34	1201	10	1543	4	1879	4	2251	10	2621	6	2963	2	3359	2
43	4	281	2	577	4	881	18	1213	22	1549	4	1889	2	2267	20	2633	54	2969	2	3361	16
47	14	283	6	587	14	883	4	1217	24	1553	6	1901	2	2269	10	2647	4	2971	6	3371	20
53	2	293	2	593	2	887	6	1223	2	1559	2	1907	6	2273	2	2657	14	2999	8	3373	24
59	12	307	24	599	8	907	6	1229	2	1567	4	1913	14	2281	6	2659	10	3001	10	3389	2
61	16	311	12	601	6	911	2	1231	16	1571	8	1931	2	2287	6	2663	26	3011	32	3391	6
67	30	313	6	607	30	919	4	1237	16	1579	4	1933	12	2293	4	2671	10	3019	12	3407	6
71	8	317	26	613	10	929	8	1249	10	1583	2	1949	18	2297	14	2677	4	3023	2	3413	2
73	4	331	6	617	8	937	6	1259	14	1597	4	1951	22	2309	14	2683	4	3037	4	3433	6
79	4	337	16	619	4	941	6	1277	20	1601	2	1973	2	2311	12	2687	14	3041	8	3449	2
83	2	347	6	631	10	947	8	1279	10	1607	6	1979	20	2333	6	2689	10	3049	4	3457	4
89	24	349	10	641	2	953	2	1283	6	1609	10	1987	4	2339	2	2693	2	3061	6	3461	8
97	10	353	14	643	34	967	16	1289	2	1613	6	1993	6	2341	18	2699	2	3067	4	3463	10
101	6	359	2	647	14	971	6	1291	10	1619	8	1997	44	2347	6	2707	16	3079	24	3467	8
103	6	367	6	653	2	977	8	1297	4	1621	18	1999	10	2351	2	2711	6	3083	12	3469	4
107	8	373	4	659	2	983	14	1301	20	1627	18	2003	2	2357	6	2713	4	3089	18	3491	2
109	10	379	12	661	6	991	18	1303	16	1637	38	2011	12	2371	22	2719	10	3109	4	3499	4
113	2	383	12	673	4	997	4	1307	8	1657	16	2017	4	2377	18	2729	12	3119	8	3511	6
127	4	389	24	677	8	1009	12	1319	24	1663	4	2027	6	2381	12	2731	22	3121	16	3517	36
131	2	397	16	683	2	1013	2	1321	6	1667	8	2029	4	2383	4	2741	2	3137	8	3527	6
137	6	401	8	691	10	1019	2	1327	4	1669	10	2039	2	2389	12	2749	30	3163	4	3529	10
139	4	409	10	701	30	1021	10	1361	6	1693	6	2053	46	2393	2	2753	2	3167	36	3533	12
149	12	419	2	709	4	1031	2	1367	8	1697	8	2063	2	2399	2	2767	4	3169	34	3539	2
151	6	421	28	719	2	1033	4	1373	12	1699	12	2069	2	2411	8	2777	20	3181	6	3541	6
157	10	431	2	727	4	1039	4	1381	6	1709	12	2081	6	2417	6	2789	12	3187	16	3547	6
163	4	433	4	733	10	1049	2	1399	18	1721	20	2083	22	2423	12	2791	6	3191	30	3557	24
167	14	439	10	739	4	1051	18	1409	2	1723	10	2087	18	2437	4	2797	16	3203	6	3559	10
173	2	443	2	743	2	1061	6	1423	4	1733	2	2089	22	2441	20	2801	8	3209	14	3571	12
179	2	449	8	751	6	1063	4	1427	6	1741	22	2099	12	2447	6	2803	4	3217	16	3581	6
181	6	457	30	757	16	1069	10	1429	4	1747	16	2111	8	2459	2	2819	2	3221	38	3583	6
191	2	461	6	761	2	1087	4	1433	6	1753	4	2113	16	2467	10	2833	12	3229	4	3593	2
193	4	463	12	769	10	1091	6	1439	2	1759	18	2129	2	2473	16	2837	8	3251	6	3607	16
197	18	467	6	773	6	1093	4	1447	24	1777	4	2131	28	2477	14	2843	32	3253	10	3613	10
199	4	479	8	787	6	1097	14	1451	2	1783	22	2137	6	2503	10	2851	6	3257	6	3617	20
211	10	487	4	797	6	1103	2	1453	4	1787	6	2141	2	2521	12	2857	10	3259	4	3623	6
223	12	491	2	809	2	1109	12	1459	10	1789	10	2143	4	2531	6	2861	6	3271	22	3631	6
227	26	499	22	811	10	1117	6	1471	16	1801	12	2153	6	2539	10	2879	12	3299	2	3637	4
229	12	503	12	821	8	1123	4	1481	2	1811	2	2161	6	2543	2	2887	4	3301	16	3643	6
233	2	509	2	823	10	1129	4	1483	10	1823	14	2179	22	2549	2	2897	6	3307	4	3659	20
239	2	521	32	827	14	1151	8	1487	6	1831	6	2203	6	2551	6	2903	2	3313	34	3671	6

TABLEAU 1. Couples (p, n) qui satisfont aux conditions du théorème 3.1. Suite au verso.

p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n
3673	6	4051	16	4451	20	4861	6	5237	8	5651	18	6047	14	6421	22	6841	6	7247	8	7673	12
3677	6	4057	4	4457	26	4871	2	5261	6	5653	4	6053	2	6427	10	6857	6	7253	12	7681	12
3691	12	4073	2	4463	14	4877	14	5273	12	5657	36	6067	16	6449	2	6863	6	7283	14	7687	10
3697	24	4079	8	4481	2	4889	8	5279	2	5659	4	6073	16	6451	6	6869	14	7297	24	7691	2
3701	20	4091	6	4483	22	4903	10	5281	6	5669	14	6079	4	6469	18	6871	6	7307	14	7699	10
3709	18	4093	12	4493	6	4909	12	5297	14	5683	24	6089	14	6473	6	6883	6	7309	10	7703	6
3719	8	4099	18	4507	6	4919	2	5303	2	5689	10	6091	18	6481	10	6899	2	7321	12	7717	4
3727	24	4111	12	4513	10	4931	6	5309	8	5693	6	6101	2	6491	2	6907	6	7331	6	7723	4
3733	12	4127	6	4517	6	4933	6	5323	10	5701	22	6113	2	6521	2	6911	6	7333	4	7727	14
3739	4	4129	12	4519	4	4937	14	5333	2	5711	2	6121	10	6529	28	6917	8	7349	2	7741	6
3761	2	4133	6	4523	12	4943	2	5347	6	5717	6	6131	2	6547	4	6947	14	7351	16	7753	4
3767	8	4139	8	4547	6	4951	18	5351	20	5737	60	6133	4	6551	2	6949	10	7369	22	7757	8
3769	4	4153	6	4549	10	4957	18	5381	8	5741	2	6143	20	6553	16	6959	8	7393	4	7759	10
3779	2	4157	6	4561	6	4967	14	5387	6	5743	4	6151	10	6563	2	6961	18	7411	28	7789	34
3793	4	4159	22	4567	4	4969	12	5393	6	5749	18	6163	6	6569	8	6967	18	7417	4	7793	14
3797	6	4177	10	4583	26	4973	14	5399	2	5779	4	6173	2	6571	12	6971	12	7433	2	7817	30
3803	2	4201	16	4591	28	4987	4	5407	6	5783	14	6197	20	6577	4	6977	6	7451	12	7823	2
3821	2	4211	2	4597	6	4993	4	5413	6	5791	6	6199	10	6581	2	6983	2	7457	14	7829	8
3823	10	4217	6	4603	4	4999	4	5417	6	5801	6	6203	14	6599	14	6991	6	7459	4	7841	2
3833	60	4219	40	4621	22	5003	2	5419	24	5807	6	6211	16	6607	10	6997	6	7477	10	7853	6
3847	16	4229	14	4637	8	5009	18	5431	6	5813	36	6217	10	6619	10	7001	8	7481	6	7867	4
3851	2	4231	12	4639	22	5011	10	5437	16	5821	10	6221	12	6637	64	7013	26	7487	24	7873	12
3853	4	4241	6	4643	12	5021	8	5441	2	5827	6	6229	4	6653	24	7019	12	7489	10	7877	26
3863	2	4243	24	4649	24	5023	6	5443	4	5839	4	6247	4	6659	42	7027	4	7499	12	7879	4
3877	28	4253	20	4651	10	5039	2	5449	34	5843	6	6257	20	6661	22	7039	18	7507	4	7883	2
3881	12	4259	14	4657	6	5051	2	5471	18	5849	2	6263	2	6673	4	7043	2	7517	14	7901	2
3889	10	4261	10	4663	16	5059	10	5477	14	5851	6	6269	2	6679	4	7057	4	7523	6	7907	18
3907	4	4271	2	4673	14	5077	16	5479	22	5857	28	6271	12	6689	20	7069	4	7529	14	7919	8
3911	2	4273	4	4679	12	5081	2	5483	20	5861	8	6277	6	6691	16	7079	2	7537	36	7927	6
3917	8	4283	20	4691	8	5087	20	5501	2	5867	14	6287	14	6701	8	7103	2	7541	2	7933	6
3919	10	4289	8	4703	6	5099	14	5503	4	5869	12	6299	18	6703	4	7109	8	7547	36	7937	6
3923	6	4297	4	4721	18	5101	22	5507	24	5879	12	6301	42	6709	18	7121	2	7549	4	7949	20
3929	12	4327	10	4723	34	5107	6	5519	14	5881	12	6311	32	6719	12	7127	18	7559	12	7951	12
3931	16	4337	14	4729	4	5113	10	5521	16	5897	14	6317	20	6733	34	7129	4	7561	10	7963	10
3943	4	4339	10	4733	2	5119	4	5527	4	5903	2	6323	2	6737	6	7151	2	7573	4	7993	4
3947	14	4349	2	4751	20	5147	8	5531	8	5923	22	6329	2	6761	2	7159	12	7577	8	8009	18
3967	10	4357	18	4759	4	5153	12	5557	4	5927	8	6337	4	6763	10	7177	6	7583	12	8011	10
3989	12	4363	16	4783	12	5167	36	5563	10	5939	18	6343	4	6779	12	7187	24	7589	18	8017	4
4001	6	4373	2	4787	6	5171	2	5569	4	5953	4	6353	6	6781	12	7193	2	7591	42	8039	12
4003	6	4391	2	4789	4	5179	4	5573	12	5981	36	6359	8	6791	32	7207	24	7603	10	8053	4
4007	6	4397	14	4793	2	5189	8	5581	6	5987	6	6361	10	6793	6	7211	2	7607	30	8059	4
4013	12	4409	2	4799	8	5197	4	5591	6	6007	4	6367	4	6803	6	7213	60	7621	12	8069	2
4019	2	4421	18	4801	6	5209	22	5623	6	6011	6	6373	22	6823	6	7219	12	7639	4	8081	6
4021	18	4423	12	4813	6	5227	76	5639	2	6029	14	6379	22	6827	8	7229	14	7643	2	8087	6
4027	16	4441	6	4817	26	5231	2	5641	58	6037	24	6389	20	6829	22	7237	4	7649	2	8089	18
4049	12	4447	4	4831	10	5233	22	5647	16	6043	22	6397	4	6833	24	7243	10	7669	4	8093	2

TABLEAU 1 (suite).

p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n	p	n
8101	12	8287	4	8467	18	8669	14	8821	10	9007	10	9187	4	9371	2	9521	26	9721	16	9883	16
8111	2	8291	6	8501	12	8677	10	8831	18	9011	8	9199	58	9377	6	9533	24	9733	4	9887	18
8117	8	8293	16	8513	2	8681	12	8837	14	9013	36	9203	6	9391	10	9539	2	9739	18	9901	6
8123	14	8297	6	8521	12	8689	4	8839	48	9029	2	9209	8	9397	4	9547	4	9743	14	9907	6
8147	6	8311	12	8527	18	8693	2	8849	8	9041	18	9221	2	9403	30	9551	12	9749	12	9923	6
8161	10	8317	16	8537	20	8699	14	8861	18	9043	12	9227	44	9413	6	9587	8	9767	6	9929	8
8167	6	8329	4	8539	4	8707	10	8863	12	9049	40	9239	14	9419	2	9601	36	9769	18	9931	12
8171	26	8353	4	8543	24	8713	16	8867	8	9059	2	9241	30	9421	6	9613	4	9781	6	9941	12
8179	4	8363	12	8563	4	8719	4	8887	6	9067	4	9257	36	9431	12	9619	12	9787	10	9949	12
8191	46	8369	14	8573	6	8731	6	8893	4	9091	6	9277	6	9433	6	9623	20	9791	2	9967	4
8209	30	8377	6	8581	6	8737	4	8923	10	9103	34	9281	12	9437	30	9629	2	9803	24	9973	12
8219	14	8387	18	8597	8	8741	2	8929	18	9109	28	9283	10	9439	34	9631	6	9811	18		
8221	28	8389	10	8599	10	8747	24	8933	12	9127	16	9293	2	9461	6	9643	6	9817	34		
8231	12	8419	10	8609	20	8753	12	8941	42	9133	6	9311	8	9463	4	9649	18	9829	4		
8233	4	8423	30	8623	24	8761	6	8951	2	9137	26	9319	4	9467	38	9661	12	9833	20		
8237	14	8429	8	8627	14	8779	4	8963	20	9151	6	9323	14	9473	2	9677	8	9839	8		
8243	2	8431	6	8629	10	8783	12	8969	2	9157	4	9337	10	9479	2	9679	28	9851	6		
8263	4	8443	4	8641	18	8803	30	8971	16	9161	30	9341	8	9491	30	9689	2	9857	8		
8269	22	8447	6	8647	4	8807	8	8999	8	9173	20	9343	16	9497	6	9697	16	9859	22		
8273	2	8461	6	8663	2	8819	12	9001	10	9181	10	9349	4	9511	10	9719	14	9871	10		

TABLEAU 1 (fin).

Alain Kraus, Université de Paris VI, Institut de Mathématiques, Case 247, 4 place Jussieu 75252 Paris Cedex 05, France (kraus@math.jussieu.fr)

Received March 21, 1997; accepted May 8, 1997