Une équation diophantienne

Daniel PERRIN

Introduction

Le problème abordé ici est posé dans le numéro 541 de *Au fil des maths* (problème 541-3) :

Résoudre dans les entiers naturels l'équation (E) *:* $a^2 - b^4 = \dfrac{p!}{q!}$ *avec* $p > q + 1$.

Je dois dire que j'ai trouvé ce problème particulièrement coriace [1] et que je ne sais pas faire grand chose sur ce sujet hormis de montrer, de plusieurs manières, que l'équation a une infinité de solutions. Je me contente donc de prouver quelques résultats faciles et de proposer quelques conjectures sans doute hasardeuses [2].

Je signale que la littérature contient de nombreux articles concernant les produits d'entiers consécutifs, c'est-à-dire de la forme $p!/q!$, voir le panorama de [7], mais je n'y ai pas trouvé de référence pour l'équation (E), sauf dans le cas $b = 0$. Il faut dire qu'on ne voit pas pourquoi se limiter à un premier membre de la forme $a^2 - b^4$. *On pourrait dire ... Oh ! Dieu ! ... bien des choses en somme, En variant ... les paramètres.* En effet, une simple expérience montre par exemple qu'il y a beaucoup de solutions aux équations $a^r - b^s = p!/q!$ avec $2 \leq r, s \leq 5$.

1 Remarques préliminaires

1.1 Des solutions avec l'ordinateur

Face à une question ouverte comme celle-ci, il est utile de disposer d'une liste de "petites" solutions (s'il y en a). Le programme suivant, sur SAGE, renvoie la liste des solutions de l'équation avec $a \leq n$:

```
def APM(n):
   for a in [0..n] :
         for b in [0..sqrt(a)] :
            for p in [0..a+1] :
               for q in [0..p-2] :
                  if a^2-b^4==factorial(p)/factorial(q) :
```

1. Pour moi, résoudre signifie trouver toutes les solutions. J'en suis bien loin.

2. J'ai la réputation d'avoir la conjecture facile. Mon collègue R. Hartshorne parle des conjectures "à la Daniel".

```
print(a,b,p,q)
```

1.1 Proposition. *L'équation admet les* 31 *solutions suivantes avec* $a \leq 100$ *:* $(5,1,4,0)$, $(5,1,4,1)$, $(6,2,5,3)$, $(11,1,5,0)$, $(11,1,5,1)$, $(11,1,6,3)$, $(16,2,16,14)$, $(19,1,6,2)$, $(21,3,6,2)$, $(26,4,21,19)$, $(29,1,7,3)$, $(31,5,8,5)$, $(35,5,25,23)$, $(41,1,8,4)$, $(41,5,33,31)$, $(44,4,8,4)$, $(51,3,7,2)$, $(53,5,14,11)$, $(55,1,9,5)$, $(61,7,12,9)$, $(64,2,17,14)$, $(71,1,7,0)$, $(71,1,7,1)$, $(71,1,10,6)$, $(76,8,8,4)$, $(81,3,81,79)$, $(81,7,65,63)$, $(86,4,85,83)$, $(89,1,11,7)$, $(91,5,88,86)$, $(96,6,11,7)$.

1.2 *Remarque.* Dans la liste ci-dessus il y a plusieurs solutions de (E) avec les mêmes p, q comme $(19,1,6,2)$, $(21,3,6,2)$; $(41,1,8,4)$, $(44,4,8,4)$, $(76,8,8,4)$ ou encore $(89,1,11,7)$; $(96,6,11,7)$. Si l'on ne craint pas de s'aventurer on peut proposer une première conjecture :

1.3 Conjecture. *Il existe une infinité de paires de solutions de* (E) *avec les mêmes* p *et* q*.*

À l'appui de cette conjecture, il est facile de voir que l'équation $a^2 - b^4 = c^2 - d^4$ a une infinité de solutions [3] avec $a \neq c$, par exemple, pour $x \in \mathbf{N}^*$, $a = 8x^2+6x+3$, $b = 2x$, $c = 8x^2+10x+5$, $d = 2x+2$ qui donne $(17,2,23,4)$, $(47,4,57,6)$, etc.

1.2 Quelques remarques

La quantité $p!/q!$ est égale à $p(p-1)\cdots(q+1)$ avec $p > q+1$ et, le produit ayant au moins deux termes, elle est paire. Il s'ensuit que a et b sont de même parité et $a^2 - b^4$ multiple de 4. On note aussi que $p!/q!$ étant strictement positif, il en est de même de a.

Soit n un entier multiple de 4. S'il est de la forme $a^2 - b^4 = (a-b^2)(a+b^2)$, il s'écrit donc $n = rs$ avec $r = a - b^2$ et $s = a + b^2$, donc r, s pairs, $r \leq s$ et $s - r = 2b^2$. Inversement, si n est de la forme $n = rs$ avec r, s vérifiant ces propriétés, il s'écrit $a^2 - b^4$. Cela donne une procédure finie pour résoudre l'équation (E) grâce au programme suivant :

```
def APMD(n) :
   L=divisors(n)
   l=len(L)
   for i in [0..(l/2)-1] :
   r=L[i]
   s=n/r
```

3. Mais bien entendu, pas nécessairement avec $a^2 - b^4$ produit d'entiers consécutifs.

```
t=(s-r)/2
a=(s+r)/2
b=sqrt(t)
if floor(b)==b :
   print (a,b)
```

1.4 *Remarques.* 1) Dans la quantité $a^2-b^4=(a-b^2)(a+b^2)$ les deux termes peuvent être premiers impairs ce qui exclut que le produit soit du type $p!/q!$. Pour $b=1$ il suffit de prendre pour $a-b^2$ et $a+b^2$ une paire de nombres premiers jumeaux, mais il y a bien d'autres exemples avec $b=2,3,....$ En effet, la conjecture de Polignac affirme que, pour tout $b\in\mathbf{N}^*$, il existe une infinité de nombres premiers r,s tels que $s-r=2b^2$. En posant $2a=s+r$ on obtient, si l'on en croit cette conjecture, une infinité de nombres a^2-b^4 qui sont produits de deux nombres premiers, donc pas du type $p!/q!$.

2) Dans ce qui suit, les solutions que je trouve sont le plus souvent banales au sens où $a-b^2$ et $a+b^2$ sont des produits de termes pris parmi $p, p-1, \ldots, q+1$. Bien entendu il y en a beaucoup d'autres, obtenues en regroupant des facteurs de ces termes, comme on le voit dans les résultats de l'ordinateur.

1.3 Un fil conducteur

Si l'on note X l'ensemble des $(a,b,p,q)\in\mathbf{N}^4$ (avec $a,p>0$) solutions de (E), nous montrerons ci-dessous de multiples manières que X est infini. Une question sans doute plus pertinente est de savoir si les ensembles X_a, X_b, X_p, X_q des solutions avec a,b,p ou q fixés sont infinis [4]. On a déjà de manière évidente :

1.5 Proposition. *L'ensemble X_a (resp. X_p) des solutions avec a fixé (resp. p fixé) est fini. Précisément, si a est fixé on a $b\leq\sqrt{a}$, $q<p\leq a$ et si p est fixé on a $a\leq p!$, $b\leq\sqrt{a}$, $q<p$.*

Démonstration. Si a est fixé on a $p\leq a$. Sinon, si $p\geq a+1$ on a $p!/q!\geq p(p-1)\geq(a+1)a>a^2\geq a^2-b^4$ et c'est absurde. Si p est fixé, on a $(a+b^2)(a-b^2)=p!/q!$, donc $a\leq a+b^2\leq p!/q!\leq p!$.

1.6 *Remarque.* En revanche, pour b ou m fixés la situation est plus complexe. Nous verrons que X_b est vide pour $b=0$, non vide pour $b\geq 1$ et infini pour $b=1$ et peut-être pour $b\geq 1$ et que X_m est souvent (toujours ?) infini.

4. En fait, plutôt que q nous utiliserons le paramètre $m=p-q$ et l'ensemble X_m associé.

1.4 Quelques cas particuliers

On note qu'il ne peut y avoir de solutions de (E) avec $a = 0$ ou $p = 0$. Pour le cas $b = 0$, voir plus loin. Il reste le cas $q = 0$.

1.4.1 Le cas $q = 0$

On note que si l'on a une solution $(a, b, p, 0)$ on a aussi $(a, b, p, 1)$. Le programme APMD donne de telles solutions :

1.7 Proposition. *Pour $q = 0$ et $a \leq 10000$ l'équation admet les solutions suivantes :* $(5, 1, 4, 0)$, $(11, 1, 5, 0)$, $(71, 1, 7, 0)$ *;* $(201, 3, 8, 0)$ *;* $(204, 6, 8, 0)$ *;* $(524, 22, 8, 0)$ *;* $(684, 18, 9, 0)$ *;* $(2304, 36, 10, 0)$ *;* $(7911, 69, 11, 0)$.

1.8 *Remarques.* 0) Voici d'autres solutions avec $p \leq 16$: $(22716, 78, 12, 0)$; $(295344, 84, 14, 0)$; $(1369424, 868, 15, 0)$; $(5477696, 1736, 16, 0)$, etc.

1) On vérifie avec le programme APMD qu'il n'y a pas de solution à $a^2 - b^4 = p!$ pour $p = 6$, $p = 13$, $p = 17$.

2) On a une solution avec $b = 1$ si $p! = a^2 - 1$, donc si $p! + 1$ est un carré comme 24, 120 et 5040, mais il n'y en a pas d'autres pour $p \leq 1000$.

On peut évidemment, si l'on est optimiste, proposer la conjecture :

1.9 Conjecture. *Il y a une infinité de solutions de l'équation avec $q = 0$.*

1.4.2 Le cas $a = p$

1.10 Proposition. *Les solutions de l'équation (E) qui vérifient $a = p$ sont données par $a = p = b^4$ avec $b \geq 2$ et $q = p - 2$. Il y en a une infinité.*

Démonstration. On suppose qu'on a $p(p-1)\cdots(q+1) = p^2 - b^4$. On vérifie que $p = 2$ ou 3 ne donnent pas de solutions. Pour $p \geq 4$ on a $p^2 - 4p + 2 > 0$ donc $p(p-1)(p-2) > p^2$ et il ne peut y avoir de solutions sauf si $q = p - 2$. Dans ce cas il reste $p^2 - p = p^2 - b^4$ et on a $p = b^4$ comme annoncé.

Dans la liste ci-dessus on obtient les solutions $(16, 2, 16, 14)$ et $(81, 3, 81, 79)$.

1.11 Conjecture. *Toutes les solutions de (E) avec $a = b^4$ vérifient $a = p$.*

1.12 *Remarque.* Attention, si $a = b^4$ on a $a^2 - b^4 = b^4(b^4 - 1) := n(n-1)$, mais l'équation $n(n-1) = p(p-1)\cdots(q+1)$ a des solutions non triviales (i.e. avec $p \neq n$) par exemple $15 \times 14 = 7 \times 6 \times 5$ (mais pas d'autre pour $n \leq 1000$). Mordell a montré que cette solution est la seule dans le cas $q = p - 3$. Dans le cas général, Erdös a conjecturé qu'il y a un nombre fini de solutions à cette équation, voir [7]. Pour prouver la conjecture 1.11 il faut sans doute utiliser le fait que n est de la forme b^4.

2 Solutions à b fixé

2.1 Le cas $b = 0$

Dans ce cas, l'équation (E) devient $a^2 = p!/q! = p(p-1)\cdots(q+1)$ et c'est, à ma connaissance, le seul cas qui ait été très étudié.

2.1.1 Le résultat

Le théorème est le suivant :

2.1 Théorème. *L'équation (E) n'a pas de solution avec $b = 0$, autrement dit : un produit de $m \geq 2$ nombres entiers consécutifs n'est jamais un carré parfait.*

Ce théorème a une longue histoire. Goldbach, dans une lettre à Daniel Bernoulli de 1724, le montre pour le produit de trois nombres. Le résultat est conjecturé ensuite par de nombreux mathématiciens qui en prouvent des cas particuliers. Par exemple, Guibert, en 1862, le montre pour $m = 8, 9, 10, 11$, voir [1].

Le théorème est finalement démontré indépendamment par O. Rigge (voir [5]) en 1938 et Paul Erdös (voir [2]) en 1939. De plus, Erdös et Selfridge montrent en 1975 qu'un produit d'au moins deux entiers consécutifs n'est jamais une puissance n-ième, voir [3].

Je montre seulement ici le résultat dans quelques cas faciles.

2.1.2 Le cas $q = 0$

2.2 Proposition. *Une factorielle plus grande que 1 n'est jamais égale à un carré.*

Démonstration. Si $a^2 = p!$, soit n le plus grand nombre premier $\leq p$. On a $n \leq p < 2n$, sinon, si $2n \leq p$, le postulat de Bertrand [5] montre qu'il y a un nombre premier m avec $n < m < 2n \leq p$ et c'est absurde. Mais alors, comme $2n$ est plus grand que $p!$, le facteur n est avec l'exposant un dans $p!$ et $p!$ n'est donc pas un carré.

Dans la même veine on peut écarter [6] beaucoup de produit de nombres consécutifs :

2.3 Proposition. *S'il y a un nombre premier n entre $q+1$ et p, le produit $p(p-1)\cdots(q+1)$ n'est pas un carré.*

5. Ou théorème de Tchebychev.
6. Pour montrer 2.1, Erdös utilise ce type d'argument.

Démonstration. On prend le plus grand nombre premier n entre $q+1$ et p, on a $2n > p$ (sinon il y a un premier plus grand que n par Bertrand) et on a gagné.

2.1.3 Les cas $p-q$ égal à 2 ou 3

On commence par deux remarques :

2.4 *Remarque.* Si l'on a $a^2 = bc$ avec b, c premiers entre eux, b et c sont des carrés.

2.5 *Remarque.* La différence de deux carrés non nuls est au moins égale à 3.

Avec ces remarques on a le cas $p-q=2$, i.e. $a^2 = p(p-1)$ car p et $p-1$ sont premiers entre eux, donc des carrés et c'est impossible car $p \geq 2$. On a aussi le cas $p-q=3$, $a^2 = p(p-1)(p-2)$ car $p-1$ et $p(p-2)$ sont premiers entre eux, donc des carrés. On a donc $p = c^2+1$ et $(c^2+1)(c^2-1) = c^4-1$ est un carré, ce qui est encore impossible car $p \geq 3$ donc $c > 1$.

2.1.4 Le cas $p-q=4$

L'équation est $a^2 = p(p-1)(p-2)(p-3)$ avec $p \geq 4$. Or on a l'identité : $p(p-1)(p-2)(p-3)+1 = (p^2-3p+1)^2$. On conclut encore avec 2.5.

2.2 Le cas $b=1$

Les résultats de ce paragraphe seront revus dans l'étude de l'équation à $p-q$ fixé.

2.6 Proposition. *L'équation (E) admet une infinité de solutions qui vérifient $b=1$.*

Démonstration. On cherche des solutions avec $q = p-4$. On prend $p \geq 4$ et on a à résoudre $(a-1)(a+1) = p(p-1)(p-2)(p-3)$. Il faut trouver deux facteurs du second membre qui diffèrent de 2 et il suffit de prendre $a-1 = p(p-3)$ et $a+1 = (p-1)(p-2)$. On a donc une infinité de solutions de la forme $(p^2-3p+1, 1, p, p-4)$, cf. 2.1.4.

2.7 *Remarques.* 1) Dans la liste ci-dessus on obtient les solutions suivantes : $(5,1,4,0)$, $(11,1,5,1)$, $(19,1,6,2)$, $(29,1,7,3)$, $(41,1,8,4)$, $(55,1,9,5)$, $(71,1,10,6)$, $(89,1,11,7)$.

2) On a fabriqué des solutions avec $p-q=4$ mais il y en a d'autres, par exemple $(5,1,4,1)$ et $(11,1,6,3)$ $(p-q=3)$ ou $(71,1,7,1)$, $p-q=6$. Avec $p-q=3$ on a aussi $(419,1,57,54)$ mais pas d'autre jusqu'à $a=50000$. On peut donc proposer :

2.8 Conjecture. *L'équation diophantienne* $a^2 - 1 = p(p-1)(p-2)$ *n'a pas d'autres solutions dans* $\mathbf{N}$ *que* $(1,2)$, $(5,4)$, $(11,6)$ *et* $(419,57)$.

On notera que cette équation s'écrit $a^2 = p^3 - 3p^2 + 2p + 1$: c'est une courbe elliptique. Le logiciel Pari affirme qu'elle est de rang 1. Il y a donc une infinité de solutions rationnelles, mais un nombre fini de solutions entières en vertu du théorème de Siegel. Nul doute qu'un utilisateur de Pari plus averti que moi pourrait vérifier si cette conjecture est vraie.

2.3 Le cas $b > 1$

2.9 Proposition. *Pour* $b > 1$ *fixé, l'équation* (E) *admet au moins une solution.*

Démonstration. Il suffit de prendre $a = p = b^4$ et $q = p - 2$, voir 1.10 ou 3.1.

2.10 *Remarque.* Dans le cas b impair, $b \geq 3$ on peut aussi utiliser l'équation avec $p - q = 4$, voir §3.3.

Il reste à préciser le nombre de solutions et, éventuellement, son infinitude. Contrairement au cas $b = 1$ où l'on a une infinité de solutions avec $m = p - q = 4$ fixé, on a la proposition suivante :

2.11 Proposition. *Pour* $b > 1$ *fixé et* $m = p - q$ *fixé, l'équation* (E) *n'a qu'un nombre fini de solutions.*

Démonstration. Pour $m = 2$ on a $a^2 - b^4 = p(p-1)$ que l'on peut encore écrire $(2a)^2 - (2p-1)^2 = 4b^4 - 1$. Posons $x = 2a$ et $y = 2p - 1$, de sorte que l'équation devient $x^2 - y^2 = 4b^4 - 1$. Comme b est plus grand que 1, le second membre n'a qu'un nombre fini de diviseurs et $x - y$, $x + y$ ne peuvent prendre qu'un nombre fini de valeurs, donc aussi x, y puis a et p.

Pour $m = 3$ on a $a^2 = p(p-1)(p-2) + b^4$, c'est, en a et p, l'équation d'une courbe elliptique et le théorème de Siegel assure qu'il n'y a qu'un nombre fini de solutions entières (voir par exemple [8] p. 269).

Pour $m \geq 4$ l'équation en a, p définit une courbe algébrique de degré m. On vérifie, par un petit calcul de dérivées partielles [7], qu'elle est lisse, donc de genre ≥ 2. Le théorème de Faltings montre alors qu'elle n'a qu'un nombre fini de points entiers (et même rationnels), voir [4].

Cependant, comme il y a une infinité de m possibles, on peut espérer :

2.12 Conjecture. *Pour* $b \geq 1$ *fixé, l'équation* (E) *admet une infinité de solutions.*

7. Sans oublier les points à l'infini.

À l'appui de cette conjecture, il y a le fait que l'ordinateur fournit de nombreuses solutions. Par exemple, pour $b = 2$ et $a \leq 1000$ on a : $(6, 2, 5, 3)$; $(16, 2, 16, 14)$; $(64, 2, 17, 14)$; $(500, 2, 64, 61)$; $(524, 2, 66, 63)$; $(724, 2, 16, 11)$. On voit qu'effectivement l'écart $m = p - q$ augmente.

3 Classer selon les valeurs de $m = p - q$

3.1 Le cas $q = p - 2$: toutes les solutions

L'équation (E) s'écrit $a^2 - b^4 = p(p-1)$, avec $p \geq 2$. Ce cas est le seul où je suis parvenu à déterminer exactement toutes les solutions de l'équation.

3.1 Proposition. *Toutes les solutions (a, b, p, q) de (E) avec $q = p - 2$ sont obtenues par la procédure suivante :*

On choisit un entier $k \in \mathbf{N}$ tel que k^2 soit une puissance quatrième modulo $2k + 1$. On prend b tel que $k^2 \equiv b^4 \pmod{2k+1}$ et $b^4 \geq k^2 + 4k + 2$ et on pose $p = \dfrac{b^4 - k^2}{2k+1}$ et $a = p + k$.

3.2 *Remarques.* 1) Dans le cas $k = 0$, la procédure consiste à choisir n'importe quel entier $b > 1$ et à poser $a = p = b^4$. On obtient évidemment ainsi une infinité de solutions. De plus on voit que pour tout $b > 1$ il y a au moins une solution avec ce b.

2) Une autre manière d'avoir une infinité de solutions consiste à prendre b non multiple de 3 quelconque. On a alors $b^2 \equiv 1 \pmod 3$, donc $b^2 = 3k+1 = k + (2k + 1)$. On obtient une solution de (E) avec $p = 4k + 1$ et $a = 5k + 1$. On vérifie que cette solution est bien du type annoncé, mais c'en est un cas doublement particulier. D'abord on a $b^2 \equiv k \pmod{2k+1}$ et pas seulement $b^4 \equiv k^2$, voir 3.7.2, ensuite on résout la congruence de la manière la plus évidente en prenant $b^2 = k + (2k + 1)$ au lieu de $k + n(2k + 1)$.

Démonstration. Supposons d'abord qu'on a une solution de l'équation $a^2 - b^4 = p(p-1)$ avec $p \geq 2$. On a alors $p \leq a$. En effet, $p \geq a + 1$ donne $p(p-1) \geq a^2 + a > a^2 - b^4$ (car a est non nul), ce qui est absurde. On a donc $a = p + k$ avec $k \geq 0$ et $p^2 + 2kp + k^2 - b^4 = p^2 - p$ donc $p = \dfrac{b^4 - k^2}{2k+1}$. On voit qu'on a obtenu les formules donnant a et p et la congruence annoncée pour les solutions. L'inégalité $b^4 \geq k^2 + 4k + 2$ provient de la condition $p \geq 2$.

Inversement, si l'on se donne k vérifiant la condition de congruence, si l'on choisit b tel que $k^2 \equiv b^4 \pmod{2k+1}$ et $b^4 \geq k^2 + 4k + 2$ et si l'on pose $p = \dfrac{b^4 - k^2}{2k+1}$ et $a = p + k$, on vérifie que (a, b, p) est bien solution de l'équation.

Il reste à préciser quels sont les k et les b qui donnent des solutions. On commence par quelques rappels.

3.3 Lemme. (Lemme chinois) *Soit n un entier décomposé en produit de facteurs premiers distincts : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. L'application qui à $\overline{x} \in \mathbf{Z}/n\mathbf{Z}$ associe ses classes modulo chaque $p_i^{\alpha_i}$ est un isomorphisme d'anneaux de $\mathbf{Z}/n\mathbf{Z}$ sur $\mathbf{Z}/p_1^{\alpha_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_1^{\alpha_r}$.*

Un élément $\overline{x}$ est un carré ou une puissance quatrième, etc. dans $\mathbf{Z}/n\mathbf{Z}$ si et seulement toutes ses classes modulo les $p_i^{\alpha_i}$ le sont.

3.4 Lemme. (Hensel) *Soit p un nombre premier, α un entier et a un entier premier à p. Alors, a est un carré ou une puissance quatrième modulo p^α si et seulement si il l'est modulo p. Plus précisément, si b est une racine (carrée ou quatrième) de a modulo p il existe un unique c qui relève b et qui soit racine (carrée ou quatrième) de a modulo p^α.*

Démonstration. C'est un résultat classique que l'on prouve en relevant une racine carrée ou quatrième b de a modulo p sous la forme $b+c_1p+\cdots+c_{\alpha-1}p^{\alpha-1}$ et en calculant les c_i de proche en proche.

3.5 Lemme. *Soit p un nombre premier impair.*

1) -1 est un carré modulo p si et seulement si l'on a $p \equiv 1 \pmod 4$,

2) 2 est un carré modulo p si et seulement si l'on a $p \equiv \pm 1 \pmod 8$.

On a alors le résultat suivant :

3.6 Proposition. *Soit $k \in \mathbf{N}$. On pose $n = 2k+1$ et on le décompose en facteurs premiers : $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Les conditions suivantes sont équivalentes :*

1) k^2 est une puissance quatrième modulo n,

2) 2 ou -2 est un carré modulo chacun des p_i,

3) aucun des p_i n'est congru à 5 modulo 8.

On note $\mathscr{B}$ l'ensemble des $k \in \mathbf{N}$ vérifiant ces propriétés (les "bons" k). Alors, pour tout $k \in \mathscr{B}$, le nombre de classes modulo n de b tels que $b^4 = k^2$ est égal à $2s + 4t$ où s (resp. t) est le nombre de $p_i \equiv -1 \pmod 4$ (resp. $\equiv 1 \pmod 4$). Pour chaque classe $\overline{b}$ convenable il y a une infinité de b qui donnent une solution de l'équation (E) avec $p - a = k$ et $q = p - 2$ par la procédure de 3.1.

Démonstration. Le cas $k = 0$ est évident, voir 3.2. On suppose désormais $k \geq 1$.

Comme n est impair, 2 est inversible modulo n et tous les p_i et on a $k = -1/2$ dans $\mathbf{Z}/n\mathbf{Z}$. Dire que k^2 est une puissance quatrième dans $\mathbf{Z}/n\mathbf{Z}$ signifie que $1/4$ est une puissance quatrième, c'est équivalent à dire que $4 =$

$\frac{1}{4} \times 2^4$ est une puissance quatrième modulo n ou encore modulo tous les $p_i^{\alpha_i}$ (par 3.3) et en vertu de 3.4 que 4 est une puissance quatrième modulo tous les p_i. Comme on a $4 - x^4 = (2 - x^2)(2 + x^2)$ et que $\mathbf{Z}/p_i\mathbf{Z}$ est intègre, cela signifie que 2 ou -2 est un carré modulo p_i pour tout i. Si p_i est congru à -1 modulo 4 c'est automatique car -1 n'st pas un carré, mais si p est congru à 1 modulo 4 c'est équivalent à $p_i \equiv 1 \pmod 8$ (voir 3.5). En définitive, les k à écarter sont ceux pour lesquels n a un facteur premier $p_i \equiv 5 \pmod 8$.

Soit $k \in \mathscr{B}$ et soit b tel que $b^4 = k^2$ modulo $n = 2k+1$. On note $(b_1, \ldots, b_r)$ l'image de b dans le produit des $\mathbf{Z}/p_i^{\alpha_i}\mathbf{Z}$. Alors, pour trouver c tel que $c^4 = k^2$ modulo n, on peut remplacer b_i par $-b_i$ si $p_i \equiv -1 \pmod 4$, mais si $p_i \equiv 1 \pmod 4$ on peut remplacer b_i par ζb_i où ζ est une racine quatrième de l'unité dans $\mathbf{Z}/p_i\mathbf{Z}$.

Pour chaque classe $\overline{b}$ il y a une infinité de b dans cette classe tels que $b^4 \geq k^2 + 4k + 2$, il suffit de relever $\overline{b}$ en b et de prendre $b + jn$ avec j assez grand.

3.7 *Remarques.* 1) Les plus petits nombres premiers congrus à 5 modulo 8 sont $5, 13, 29, 37, 53, 61, 101, \ldots$ qui correspondent à $k = 2, 6, 14, 18, 26, 30, 50$. Il y a d'autres k qui donnent des nombres multiples des facteurs premiers précédents, par exemple tous les entiers dont le chiffre des unités est 2 ou 7 qui donnent des multiples de 5 comme $k = 7, 12, 17, 22, \ldots$ qui donnent $2k + 1 = 15, 25, 35, 45, \ldots$, et d'autres encore, qui donnent des multiples de $13, 29, 37, \ldots$: $k = 19, 43, 45, 55, \ldots$ qui donnent $39, 87, 91, 111, \ldots$

2) Si $n = 2k + 1$ est premier, dire qu'on a $k^2 - b^4 = 0 = (k - b^2)(k + b^2)$ modulo $(2k + 1)$ signifie que k ou $-k$ est un carré modulo n car $\mathbf{Z}/n\mathbf{Z}$ est intègre. **Attention** cela ne subsiste pas si $2k+1$ n'est pas premier, ainsi, pour $k = 10$, on a $k^2 \equiv -5 \pmod{21}$ et $-5 = 16 = 2^4 = 5^4$ est une puissance quatrième bien que ni 10 ni -10 ne soient des carrés modulo 21. Avec $b = 5$ on obtient la solution $(35, 5, 25, 23)$ avec $b \equiv 2$ il faut prendre $b = 23$ et la solution $(13331, 23, 13321, 13319)$.2)

3) Pour $k = 3$ on a $2k + 1 = 7$, -3 est un carré (mais pas 3) et les classes $\overline{b}$ convenables sont celles de 2 et -2, les b correspondants qui donnent des solutions étant alors $2 + 7m$ et $-2 + 7m$ avec $m \geq 1$ (pour vérifier $b^4 \geq k^2 + 4k + 2$). On obtient ainsi par exemple les solutions $(939, 9, 936, 934)$ et $(91, 5, 88, 86)$.

4) Pour $k = 8$ on a $2k + 1 = 17$, il y a quatre classes convenables $b = 3, 5, 12, 14$ avec, par exemple, les solutions $(9416, 20, 9408, 9406)$, $(41, 5, 33, 31)$, $(1224, 12, 1216, 1214)$, $(2264, 14, 2256, 2254)$.

3.8 *Exemples.* Voici les solutions de la liste de 1.1 qui rentrent dans ce cadre, classées selon $k = a - p$:

- $k = 0$: $(16, 2, 16, 14)$ et $(81, 3, 81, 79)$.

- $k = 1 : (6, 2, 5, 3)$, $(86, 4, 85, 83)$
- $k = 3 : (91, 5, 88, 86)$
- $k = 5 : (26, 4, 21, 19)$
- $k = 8 : (41, 5, 33, 31)$
- $k = 10 : (35, 5, 25, 23)$
- $k = 16 : (81, 7, 65, 63)$

3.9 *Remarques.* 0) Parmi les $k \leq 10$ absents dans la liste ci-dessus, certains ne donnent pas de solution à la congruence $k^2 \equiv b^4 \pmod{2k+1}$ (par exemple $k = 2$, $k = 6$, $k = 7$) mais d'autres sont valables mais n'apparaissent pas à cause de la borne mise sur les solutions (par exemple $k = 4$ qui donne $(1629, 11, 1625, 1623)$ ou $k = 9$ qui donne $(12334, 22, 12325, 12323)$).

2) Il est clair que les k qui sont des carrés de $\mathbf{N}$ fournissent des solutions de l'équation.

3) Si l'on n'impose pas $p \geq 2$, l'équation $a^2 - b^4 = p(p-1)$ admet des solutions pour $p = 1$ en prenant pour a un carré quelconque $a = b^2$.

3.2 Une infinité de solutions pour $p - q = 3$

L'équation s'écrit $(a - b^2)(a + b^2) = p(p-1)(p-2)$. Commençons par les solutions "banales" au sens de 1.4, obtenues en partageant les facteurs du deuxième membre. Il y a deux solutions :

• On cherche des solutions avec $p(p-1) = a + b^2$ et $p - 2 = a - b^2$, ce qui donne $2a = p^2 - 2$ et $2b^2 = p^2 - 2p + 2$. Cette équation du second degré en p a pour discriminant réduit $\Delta' = 2b^2 - 1$ et dire que c'est un carré c^2 revient à résoudre $c^2 - 2b^2 = -1$, équation de Pell-Fermat dont on connaît les solutions, voir [6]. En effet, cette équation revient à trouver les éléments inversibles de l'anneau $\mathbf{Z}[\sqrt{2}]$. À partir de la solution fondamentale $1 + \sqrt{2}$ on a une infinité de solutions [8] en prenant $c + b\sqrt{2} = (1+\sqrt{2})^n$ avec n impair. On en déduit $p = c + 1$ puis $a = p^2/2 - 1$.

Pour $n = 3$ cela donne $b = 5$, $c = 7$ (donc $p = 8$ et $a = 31$), puis, pour $n = 5$, $b = 29$, $p = 42$, donc $a = 881$), etc.

• La même méthode fonctionne avec $p = a - b^2$ et $(p-1)(p-2) = a + b^2$, cela donne $2a = p^2 - 2p + 2$, $p^2 - 4p + 2 - 2b^2 = 0$, le discriminant réduit $\Delta' = 2b^2 + 2$ est un carré c^2 si l'on a $c^2 - 2b^2 = 2$. À partir de la solution évidente $c = 2$, $b = 1$ on en a une infinité en posant $c + b\sqrt{2} = (2+\sqrt{2})(1+\sqrt{2})^n$ avec n pair. On a alors $p = c + 2$ et $2a = p^2 - 2p + 2$ (c et p sont pairs).

Par exemple, pour $n = 0$ on trouve $(5, 1, 4, 1)$, pour $n = 2$, $(61, 7, 12, 9)$, pour $n = 4$, $(1741, 41, 60, 57)$, etc.

En résumé on a montré :

8. On montre par récurrence que c est impair, donc p pair.

3.10 Proposition. *L'équation admet une double infinité de solutions avec $q = p - 3$, obtenues de l'une des manières suivantes :*

1) On choisit un entier n impair, $n \geq 3$, on pose $c + b\sqrt{2} = (1 + \sqrt{2})^n$, $p = 1 + c$ et $2a = p^2 - 2$.

2) On choisit un entier n pair, $n \geq 0$, on pose $c+b\sqrt{2} = (2+\sqrt{2})(1+\sqrt{2})^n$, $p = 2 + c$ et $2a = p^2 - 2p + 2$.

3.11 *Remarques.* 1) Le fait que $a - b^2$ et $a + b^2$ soient de même parité impose, dans les deux cas, que p soit pair. Cela implique aussi qu'il n'y a pas de solutions avec $a - b^2 = p - 1$ et $a + b^2 = p(p - 2)$.

2) Il y a bien d'autres solutions que celles données par la proposition, obtenues en partageant les facteurs de p, $p - 1$, $p - 2$ entre $a - b^2$ et $a + b^2$, par exemple $(11, 1, 6, 3)$; $(53, 5, 14, 11)$; $(64, 2, 17, 14)$, etc. On a d'ailleurs une infinité de solutions [9] analogues à $(11, 1, 6, 3)$ en choisissant un b quelconque ≥ 1 et en posant $p = 4b^4 + 2$ et $a = 8b^6 + 3b^2$. Dans ce cas, on partage $p-2 = 4b^4$ en $\alpha\beta$ avec $\alpha = \beta = 2b^2$ et l'on a $a+b^2 = p\alpha$ et $a-b^2 = (p-1)\beta$.

Dans le cas de $(53, 5, 14, 11)$ on partage encore $p - 2$, mais dans celui de $(64, 2, 17, 14)$ on partage $p - 1$. On obtient d'ailleurs une infinité de solutions non banales de ce type en prenant $a = b^6$ et $p = b^4 + 1$.

Bref, pour les solutions "non banales" les choses ne sont pas simples ...

3.3 Une infinité de solutions pour $p - q = 4$

L'équation s'écrit $(a - b^2)(a + b^2) = p(p - 1)(p - 2)(p - 3)$. Là encore on va se contenter des solutions "banales". Il y a deux solutions :

• On cherche des solutions avec $a-b^2 = p(p-3)$ et $a+b^2 = (p-1)(p-2)$. Cela impose $b = 1$. Ce cas a été vu en 2.6 et on a une infinité de solutions.

• Avec $a - b^2 = (p - 2)(p - 3)$ et $a + b^2 = p(p - 1)$ on obtient une infinité de solutions ainsi : on choisit b impair, $b \geq 3$, on pose $p = (b^2+3)/2$, puis $a = p^2 - 3p + 3$. On obtient par exemple les solutions $(21, 3, 6, 2)$, $(157, 5, 14, 10)$, etc. voir remarque 2.10.

3.12 *Remarque.* Il y a beaucoup de solutions non banales avec $p-q = 4$, par exemple $(44, 4, 8, 4)$, $(76, 8, 8, 4)$, etc.

3.4 Une infinité de solutions pour $p - q = 5$

On a $(a - b^2)(a + b^2) = p(p - 1)(p - 2)(p - 3)(p - 4)$. Si l'on partage le produit en $p(p - 1)(p - 2) = a + b^2$ et $(p - 3)(p - 4) = a - b^2$ il reste à

9. C'est un des rares cas où l'on dispose d'une formule donnant une infinité de solutions non banales.

résoudre $2b^2 = p^3 - 4p^2 + 9p - 12$. On tombe encore sur une courbe elliptique de rang 1 mais j'ignore si elle a des points entiers (en tous cas elle n'en en a pas avec $b, p \leq 10000$). En revanche, une autre méthode permet de montrer l'infinitude des solutions. Elle consiste à partager le terme central $p-2$ entre $a-b^2$ et $a+b^2$ en supposant que $p-2$ est un carré c^2 et en posant $a-b^2 = (p-3)(p-4)c$ et $a+b^2 = p(p-1)c$. On a alors $2b^2 = 6c^3$, donc $b^2 = 3c^3$ et on voit qu'il faut que $3c$ soit un carré. On pose donc, pour $d \geq 1$, $c = 3d^2$, $b = 9d^3$, $p = 9d^4 + 2$ et $a = c(p^2 - 4p + 6) = 243d^{10} + 6d^2$. On obtient ainsi une infinité de solutions de (E) avec $p - q = 5$. Par exemple, pour $d = 1$, on obtient $(249, 9, 11, 6)$, pour $d = 2$ on a $(248856, 72, 146, 141)$.

3.5 Une infinité de solutions pour $p - q = 6$

On a $(a-b^2)(a+b^2) = p(p-1)(p-2)(p-3)(p-4)(p-5)$. Si l'on partage le produit en $p(p-1)(p-2) = a+b^2$ et $(p-3)(p-4)(p-5) = a-b^2$ il reste à résoudre $9p^2 - 45p + 60 - 2b^2 = 0$. Mais cette équation n'a pas de solutions. En effet, sinon b serait multiple de 3 et on en déduirait que 9 divise 60, ce qui est absurde.

Pour trouver des solutions, il faut prendre $a + b^2 = p(p-1)(p-4)$ et $a - b^2 = (p-2)(p-3)(p-5)$. On obtient $5p^2 - 27p + 30 - 2b^2 = 0$ et cette équation admet pour discriminant $\Delta = 129 + 40b^2$. Dire que c'est un carré c^2 revient à résoudre une équation de Pell-Fermat : $c^2 - 40b^2 = 129$. À partir de la solution $c = 13$, $b = 1$ et des éléments inversibles on obtient une infinité de solutions $c + b\sqrt{10} = (13 + 2\sqrt{10})(19 + 6\sqrt{10})^n$. Pour que p soit entier il faut que c soit congru à 3 modulo 10 et comme on a $c \equiv 13 \times 19^n \equiv 3 \times (-1)^n \pmod{10}$, c'est le cas si n est pair. On obtient ainsi une infinité de solutions de (E), la plus petite étant $(2705955431, 2203, 1396, 1390)$.

3.6 Une infinité de solutions pour $p - q = 7$

Pour obtenir ces solutions, on suppose que $p - 3 = c^2$ est un carré et on partage $p(p-1)\cdots(p-6)$ comme suit [10] : $a + b^2 = cp(p-4)(p-5) = c(p^2 - 9p^2 + 20p)$ et $a - b^2 = c(p-1)(p-2)(p-6) = c(p^3 - 9p^2 + 20p - 12)$ on a donc $2b^2 = 12c$. Pour réaliser cela on prend $c = 6k^2$, d'où $b = 6k$, $p = c^2 + 3 = 36k^4 + 3$ et $a = 216k^6(1296k^8 - 7)$. On vérifie qu'on obtient bien une infinité de solutions avec $k \geq 1$, la plus petite étant $(278424, 6, 39, 32)$.

10. Bien entendu les choix sont faits pour que le plus possible de monômes en p s'annulent.

3.7 Une infinité de solutions pour $p - q = 8$

Cette fois, on partage le produit en $a + b^2 = p(p-3)(p-5)(p-6)$ et $a - b^2 = (p-1)(p-2)(p-4)(p-7)$ d'où $2b^2 = 16p - 56$ et $b^2 = 4(2p-7)$. Pour obtenir cela on choisit un entier $k = 2c+1$ impair et on pose $b = 2k = 4c+2$ et $p = (k^2+7)/2 = 2c^2 + 2c + 4$, d'où

$$a = 16c^8 + 64c^7 + 112c^6 + 112c^5 + 28c^4 - 56c^3 - 56c^2 - 20c + 4.$$

Pour $c \geq 1$ on obtient ainsi une infinité de solutions dont la plus petite est $(204, 6, 8, 0)$ et la suivante $(22780, 10, 16, 8)$.

3.8 Une infinité de solutions pour $p - q = 9$

La méthode est toujours la même : on pose $p - 4 = c^2$ et on partage le produit en $a + b^2 = cp(p-3)(p-6)(p-7)$ et $a - b^2 = (p-1)(p-2)(p-5)(p-8)$ la différence vaut $2b^2 = 20c^2$. En posant $c = 10k^2$ on obtient une infinité de solutions $a = 10^9 k^{18} + 15 \times 10^5 k^{10} + 240k^2$, $b = 10^2 k^3$ et $p = 100k^4 + 4$. La plus petite solution n'est pas très petite : $(998500240, 100, 104, 95)$.

3.9 Fixer $m = p - q$

On a donc une infinité de solutions pour $p - q = 2, 3, \ldots, 9$. On en trouve [11] aussi pour $p - q = 10$: $(2304, 36, 10, 0)$. En vertu de 1.7, il y a des solutions pour $q = 0$ et les $p = p - q = m$ suivants : 11, 12, 14, 15, 16 mais pas 13 ni 17. Cependant on trouve des solutions pour $14!/1!$, qui donne le cas $m = 13$ ou $18!/1!$ qui donne $m = 17$.

Par conséquent on peut hasarder deux conjectures :

3.13 Conjecture. *1) (faible) Pour tout $m \geq 2$ il existe une solution de l'équation de la forme $(a, b, p, p - m)$.*

2) (forte) Pour tout $m \geq 2$ il existe une infinité de solutions de l'équation de la forme $(a, b, p, p - m)$.

La conjecture forte est prouvée pour $m = 2, 3, 4, 5, 6, 7, 8, 9$, la faible pour $m \leq 17$.

Références

[1] Guibert A.-D., *Sur quatre produits d'entiers consécutifs*, Nouvelles annales de mathématique, 2-ième série, tome 1 (1862), p. 102-109.

11. Pour $p - q = 9$ on a aussi $(684, 18, 9, 0)$.

[2] Erdös P., *Note on the product of consecutive integers (1)*, Jour. London Math. Soc. 14 (1939), 194-198.

[3] Erdös P., Selfridge J.-L., *The product of consecutive numbers is never a power*, Illinois Jour. Math. 19 (1975), p. 292-301.

[4] Faltings G., *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349-366.

[5] Rigge O., *Über ein diophantisches Problem*, 9th Congress Math. Scand. Helsingfors, 1938, Mercator (1939), 155-160.

[6] Samuel P., *Théorie algébrique des nombres*, Hermann, 1967.

[7] Shorey T.N., *Exponential diophantine equations involving products of consecutive integers and related equations*, Number Theory edited by R.P.Bambah, V.C.Dumir and R.J.Hans-Gill, Hindustan Book Agency (1999), 463-495.

[8] Silverman J.H., *The Arithmetic of Elliptic Curves*, Springer, 2° ed., 1986.