

ANNALES MATHÉMATIQUES



BLAISE PASCAL

ABDELMADJID BOUDAUD

La conjecture de Dickson et classes particulières d'entiers

Volume 13, n° 1 (2006), p. 103-109.

http://ambp.cedram.org/item?id=AMBP_2006__13_1_103_0

© Annales mathématiques Blaise Pascal, 2006, tous droits réservés.

L'accès aux articles de la revue « Annales mathématiques Blaise Pascal » (<http://ambp.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://ambp.cedram.org/legal/>). 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.

*Publication éditée par les laboratoires de mathématiques
de l'université Blaise-Pascal, UMR 6620 du CNRS
Clermont-Ferrand — France*

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

La conjecture de Dickson et classes particulières d'entiers

ABDELMADJID BOUDAUD

Abstract

As a consequence of Dickson's Conjecture, we prove, for each couple of integers $q > 0$ and $k > 0$, the existence of an infinite set $L_{q,k} \subset \mathbb{N}$ such that, for each $n \in L_{q,k}$ and every integer s , $0 < |s| \leq q$, we have $n + s = |s|t_1 \dots t_k$ where $t_1 < \dots < t_k$ are prime numbers. Similarly, we prove the existence of an infinite set $M_{q,k} \subset \mathbb{N}$ such that, for each $n \in M_{q,k}$ and every integer $s \in [-q, q]$ (including 0), we have $n + s = lt_1 \dots t_k$ where $t_1 < \dots < t_k$ are prime numbers and $l \in [1, 2q + 1]$ is an integer. The nonstandard interpretation of this result suggests the following question: Is every unlimited integer equal to the sum of a limited integer and a product of two unlimited integers? We present families of integers in which each unlimited member is a product of two unlimited integers.

Résumé

En admettant la conjecture de Dickson, nous démontrons que, pour chaque couple d'entiers $q > 0$ et $k > 0$, il existe une partie infinie $L_{q,k} \subset \mathbb{N}$ telle que, pour chacun des entiers $n \in L_{q,k}$ et tout entier s tel que $0 < |s| \leq q$, on ait $n + s = |s|t_1 \dots t_k$ où $t_1 < \dots < t_k$ sont des nombres premiers. De même, pour chaque couple d'entiers $q > 0$ et $k > 0$, il existe une partie infinie $M_{q,k} \subset \mathbb{N}$ telle que, pour chacun des entiers $n \in M_{q,k}$ et tout entier s (nul ou non) de l'intervalle $[-q, q]$, on ait $n + s = lt_1 \dots t_k$ où $t_1 < \dots < t_k$ sont des nombres premiers et l'entier l appartient à l'intervalle $[1, 2q + 1]$. La lecture non standard de ce résultat nous suggère la question suivante : est-ce-que chaque entier illimité est, à un entier limité près, produit de deux entiers illimités? Suite à ceci nous présentons des familles d'entiers, dans chacune desquelles tout nombre illimité est produit de deux entiers illimités.

Mots-clés : Conjecture de Dickson, analyse non standard, nombres premiers, suites d'entiers naturels.

Classification Mathématique (1991) : Primary 11N32, 26E35 ; Secondary 11A51, 11A41, 11B83.

1. Introduction

En 1904 Dickson [1], avait annoncé sa conjecture concernant les nombres premiers, valeurs simultanées de s formes linéaires à coefficients entiers $f_i(x) = b_i x + a_i$ où $b_i > 0$ pour $1 \leq i \leq s$.

Parmi les travaux suscités par cette conjecture on peut citer ceux de Schinzel & Sierpinski [6]. Schinzel a donné une généralisation de la conjecture de Dickson où les formes linéaires sont remplacées par des polynômes. Pour notre part, et sous l'hypothèse que la conjecture de Dickson est vraie, nous démontrons l'existence de classes particulières d'entiers dont chacun des éléments a une factorisation spéciale lorsque l'on ajoute un entier s .

Nous donnons, en termes non standard ([2, 3]), une conséquence du résultat principal et des exemples de familles d'entiers dans chacune desquelles tout membre illimité est produit de deux entiers illimités.

2. Rappel

La conjecture de Dickson [5]. On l'énonce comme suit. On se donne s formes linéaires à coefficients entiers $f_i(x) = b_i x + a_i$, où $b_i > 0$ pour $1 \leq i \leq s$. On désigne par $g(x) = f_1(x) f_2(x) \dots f_s(x)$ le produit de ces s formes. On suppose que la condition suivante est satisfaite :

(D) L'ensemble des entiers $\{g(k) : k \in \mathbb{Z}\}$ n'a aucun diviseur commun > 1 .

Il existe alors une infinité d'entiers $m \in \mathbb{N}$ pour lesquels chacun des entiers $f_1(m), f_2(m), \dots, f_s(m)$ est un nombre premier.

3. Résultat principal

Théorème 3.1. *En admettant la conjecture de Dickson, pour chaque couple d'entiers $q > 0$ et $k > 0$, il existe une partie infinie $L_{q,k} \subset \mathbb{N}$ telle que, pour chacun des entiers $n \in L_{q,k}$ et tout entier s tel que $0 < |s| \leq q$, on ait*

$$n + s = |s| t_1 \dots t_k$$

où $t_1 < \dots < t_k$ sont des nombres premiers. De même, pour chaque couple d'entiers $q > 0$ et $k > 0$, il existe une partie infinie $M_{q,k} \subset \mathbb{N}$ telle

que, pour chacun des entiers $n \in M_{q,k}$ et tout entier s (nul ou non) de l'intervalle $[-q, q]$, on ait

$$n + s = lt_1 \dots t_k$$

où $t_1 < \dots < t_k$ sont des nombres premiers et l'entier l appartient à l'intervalle $[1, 2q + 1]$.

La démonstration se fait selon le schéma suivant

(1) On commence par établir l'existence d'une partie infinie $L_{q,1}$ de \mathbb{N} pour tout entier $q > 0$ en utilisant la conjecture de Dickson.

(2) On établit ensuite l'existence des parties infinies $L_{q,k}$, par récurrence sur l'entier k , en utilisant la partie $L_{q,1}$.

(3) On établit enfin l'existence des parties $M_{q,k}$ en se servant uniquement des parties infinies $L_{q,k}$

Démonstration.

Première étape.

Existence de la partie infinie $L_{q,1}$ pour tout entier $q > 0$.

Soit $q > 0$ un entier. On désigne par $2 = p_1 < p_2 < \dots < p_n < \dots$ la suite des nombres premiers. On choisit un entier suffisamment grand $r > 1$ pour que l'on ait $q < \min \{2^r, p_r\}$ et on pose $K = (p_1 p_2 p_3 \dots p_{r-1})^r$.

Tout entier $s \neq 0$ de l'intervalle $[-q, q]$ est un diviseur de K . En effet, pour un nombre premier donné p et chaque entier $k > 0$ tels que p^k divise s , on a $p^k \leq |s| \leq q < \min \{2^r, p_r\}$ donc $p < p_r$ et $k < r$ de sorte que p^k divise K .

Soit, maintenant, $h > 0$ un entier quelconque, premier avec $K p_r$

[on peut prendre simplement $h = 1$]. Enfin, pour chaque diviseur d de K , positif ou négatif (y compris ± 1 et $\pm K$), on définit la forme linéaire $f_d(x)$ comme suit :

i) $f_d(x) = d p_r h x + 1$ si $d > 0$ et

ii) $f_d(x) = |d| p_r h x - 1$ si $d < 0$.

On obtient ainsi une famille de $2(r+1)^{r-1}$ formes linéaires auxquelles on adjoint encore la forme $f_0(x) = p_1 p_2 p_3 \dots p_{r-1} h x + p_r$. Démontrons, maintenant, que la famille de ces $2(r+1)^{r-1} + 1$ formes satisfait la condition (D).

En effet, on désigne par $F(x)$ le produit de toutes les formes $f_d(x)$ (pour d diviseur de K) et on pose $g(x) = F(x) f_0(x)$. Il s'agit de montrer

que l'ensemble des entiers $\{g(k) : k \in \mathbb{Z}\}$ n'a aucun diviseur commun > 1 . On suppose que le nombre premier p divise tous les produits $F(k) f_0(k)$ pour $k \in \mathbb{Z}$. Alors p divise, en particulier, le produit $F(p) f_0(p)$, mais il ne saurait diviser aucun des $f_d(p)$, il divise donc nécessairement $f_0(p) = p_1 p_2 p_3 \dots p_{r-1} h p + p_r$ et divise donc p_r de sorte que l'on devrait avoir $p = p_r$. Ainsi, p_r diviserait en particulier le produit $F(1) f_0(1)$, ce qui n'est pas possible.

On en déduit, à l'aide de la conjecture de Dickson, qu'il existe une infinité d'entiers $m \in \mathbb{N}$ pour lesquels l'entier $f_0(m)$ ainsi que tous les entiers $f_d(m)$ sont premiers.

Soit m l'un quelconque de ces entiers et soit $n = K p_r h m$. On montre que, pour tout entier $s \neq 0$ de l'intervalle $[-q, q]$, on a

$$n + s = |s| p$$

où p est un nombre premier.

On sait déjà que s divise K donc $K = sd$ et $n + s = (sd) p_r h m + s = s(d p_r h m + 1)$. Suivant que s est positif ou négatif, d sera également positif ou négatif, de sorte que l'on aura

- i) $n + s = s(d p_r h m + 1) = |s| f_d(m)$ ou
- ii) $n + s = |s| (|d| p_r h m - 1) = |s| f_d(m)$.

Or, dans les deux cas, l'entier $f_d(m)$ est premier ce qui achève la démonstration de la première étape.

Deuxième étape.

Il s'agit d'établir l'existence des parties $L_{q,k}$ pour tout entier $k > 1$. On procède par récurrence sur l'entier k , en utilisant l'existence des parties $L_{r,1}$ **pour tout entier** $r > 0$.

On suppose établie l'existence de $L_{q,k}$ pour un entier $k > 0$ et on établit l'existence de $L_{q,k+1}$.

On observe ceci. Pour $m \in L_{n+q,1}$, $n \in L_{q,k}$ et s un entier non nul de l'intervalle $[-q, q]$, on a $n + s = |s| t_1 \dots t_k$ où $t_1 < \dots < t_k$ sont des nombres premiers. Or $0 < n + s \leq n + q$. D'où $m + (n + s) = |n + s| p = |s| t_1 \dots t_k p$ où p est un nombre premier. Il suffit alors de prendre m assez grand [par exemple $m > (n + q)^2$] pour avoir $p > t_k$.

[Vérification. Si $m > (n + q)^2$ alors $(m + (n + s))^2 = (n + s)^2 p^2 > m^2 > (n + q)^4 \geq (n + s)^4$. D'où $p^2 > (n + s)^2 = |s|^2 (t_1 \dots t_k)^2 \geq (t_1 \dots t_k)^2$, donc $p > t_1 \dots t_k$ et $p > t_k$]. On peut ainsi prendre

$$L_{q,k+1} = \left\{ m + n : m \in L_{n+q,1}, n \in L_{q,k}, m > (n + q)^2 \right\},$$

cet ensemble étant infini puisque $L_{n+q,1}$ et $L_{q,k}$ le sont.

Troisième étape.

Il suffit de reprendre l'ensemble $L_{2q+1,k}$ et de poser $M_{q,k} = L_{2q+1,k} + q + 1$. En effet, soient $n \in M_{q,k}$ et $s \in [-q, q]$. Ainsi $n = m + q + 1$ pour un entier $m \in L_{2q+1,k}$ de sorte que $n + s = m + (q + 1 + s)$. On a $(q + 1 + s) \in [1, 2q + 1]$ et $m \in L_{2q+1,k}$ donc $n + s = (q + 1 + s)t_1 \dots t_k = lt_1 \dots t_k$ où $t_1 < \dots < t_k$ sont des nombres premiers et l'entier l appartient à l'intervalle $[1, 2q + 1]$. \square

En termes non standard ([2, 3]), le théorème précédent a la conséquence suivante

Corollaire 3.2. *En admettant la conjecture de Dickson, pour chaque entier $k > 0$, il existe une partie infinie $L_{\infty,k} \subset \mathbb{N}$ telle que, pour chacun des entiers $n \in L_{\infty,k}$ et tout entier limité non nul s , on ait*

$$n + s = |s| t_1 \dots t_k$$

où $t_1 < \dots < t_k$ sont des nombres premiers. De même, pour tout entier illimité $\omega > 0$ et chaque entier $k > 0$, il existe une partie infinie $M_{\infty,k} \subset \mathbb{N}$ telle que, pour chacun des entiers $n \in M_{\infty,k}$ et tout entier limité s (nul ou non), on ait

$$n + s = lt_1 \dots t_k$$

où $t_1 < \dots < t_k$ sont des nombres premiers et l'entier l appartient à l'intervalle $[1, \omega]$.

Démonstration. $L_{\infty,k} = L_{q,k}$ où q est un entier illimité quelconque. $M_{\infty,k} = M_{q,k}$ où q est un entier illimité tel que $2q + 1 \leq \omega$. \square

4. Une question

Soit $F(n)$ la propriété externe qui dit ceci : " l'entier n est illimité, positif, mais il n'est pas produit de deux entiers illimités ". La propriété $F(n)$ est ainsi satisfaite si et seulement si n est de la forme $n = r.p$ où r est un entier limité ≥ 1 et p un nombre premier illimité.

Soit $n \in L_{\infty,1}$. L'entier n est produit de deux entiers illimités, par construction. Cependant, pour chaque entier limité $s \neq 0$, la propriété $F(n+s)$ est satisfaite.

La question se pose : existe-t-il des entiers n pour lesquels la propriété $F(n+s)$ est satisfaite pour tout entier limité s , **nul ou non ?**

Autrement dit, pour tout entier illimité n existe-t-il toujours un entier limité s tel que $n+s$ soit produit de deux entiers illimités ?

Dans la suite nous présentons des familles d'entiers, dans chacune desquelles, tout nombre illimité est produit de deux entiers illimités (pour une bibliographie concernant ces familles se référer à [4]).

Exemple 1. Nombres pseudopremiers.

Procédons par étapes.

(1) Un entier n illimité, composé, mais qui n'est pas produit de deux entiers illimités est nécessairement de la forme $n = s.p$ pour un entier limité $s > 1$ et un nombre premier illimité p .

(2) Si le nombre de diviseurs d'un entier n est illimité, alors n est produit de deux entiers illimités. [Conséquence immédiate du (1).]

(3) Soit $a > 1$ un entier limité. Tout nombre a -pseudopremier illimité n est produit de deux entiers illimités.

En effet, sinon, l'entier n serait de la forme $n = s.p$ pour un entier limité $s > 1$ et un nombre premier illimité p . Or $a^{n-1} \equiv 1 \pmod n$ donc, en particulier, $a^n \equiv a \pmod p$. D'autre part $a^p \equiv a \pmod p$ car p est premier. Ainsi $a^n = (a^p)^s = a^s \pmod p$ d'où $a^s \equiv a \pmod p$, autrement dit p divise $a^s - a$ ce qui est impossible car $a^s - a$ est limité et non nul. \square

(4) Les nombres pseudopremiers d'Euler en base a et les nombres pseudopremiers forts en base a sont des cas particuliers de nombres a -pseudopremiers, de sorte que le (3) s'applique à eux.

(5) Tout nombre de Carmichael illimité n est produit de deux entiers illimités car n est a -pseudopremier pour tout entier a premier avec n et tel que $1 < a < n$. S'il existe un nombre a limité et premier avec n , le résultat découle du (3). Sinon, le nombre des diviseurs de n est illimité et le résultat découle du (2).

Exemple 2. Tout nombre illimité n pour lequel $\sigma(n) = an - b$ où $a > 0$ est entier et $b \geq 0$ entier limité ($\sigma(n)$ désigne la somme des diviseurs positifs de n), est produit de deux entiers illimités.

Démonstration. Si l'on avait $n = sp$ où s est un entier limité et p un nombre premier illimité, on aurait

$$\sigma(n) = \sigma(sp) = \sigma(s)(p+1) = asp - b$$

donc $(as - \sigma(s))p = \sigma(s) + b$ ce qui est impossible. \square

Remerciements. Les observations de l'arbitre nous ont permis d'améliorer sensiblement la première version de cet article. Qu'il trouve ici l'expression de notre gratitude.

Références

- [1] L. E. DICKSON – « A new extension of Dirichlet's theorem on prime numbers », *Messenger* **2**, no. 38, p. 155–161.
- [2] F. DIENER et G. REEB – *Analyse non standard*, Hermann, 1989.
- [3] E. NELSON – « Internal set theory : A new approach to non standard analysis », *bull. Amer. Math. Soc.* **83** (1977), p. 1165–1198.
- [4] P. RIBENBOIM – *The little book of big primes*, Springer-Verlag, 1991.
- [5] ———, *Nombres premiers : mystères et records*, PUF, 1994, page 214.
- [6] A. SCHINZEL et W. SIERPINSKI – « Sur certaines hypothèses concernant les nombres premiers », *Acta Arith.* **4** (1958), 185–208 ; *erratum* **5** (1958), p. 259.

ABDELMADJID BOUDAUD
Département de Mathématiques
Université de M'sila
28000 M'sila
ALGÉRIE
boudaoudab@yahoo.fr