

# SUR QUELQUES PROBLÈMES NON RÉSOLUS D'ARITHMÉTIQUE

Autor(en): **Sierpinski, W.**

Objektyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **5 (1959)**

Heft 4: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **22.09.2024**

Persistenter Link: <https://doi.org/10.5169/seals-35492>

## **Nutzungsbedingungen**

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

## **Haftungsausschluss**

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

# SUR QUELQUES PROBLÈMES NON RÉSOLUS D'ARITHMÉTIQUE <sup>1)</sup>

par W. SIERPINSKI, Varsovie

(Reçu le 2 novembre 1959)

On pourrait penser qu'il n'y a pas dans l'arithmétique de problèmes dont l'énoncé est simple et qui ne sont pas encore résolus, et pour lesquels on ne connaît aucune voie par laquelle on puisse obtenir une solution après avoir effectué les calculs nécessaires, abstraction faite de leur longueur.

Il en est cependant tout autrement. Comme exemple, je donnerai ici un problème qui nous a été posé il y a quelques années, par un étudiant de l'Université de Varsovie, Werner MNICH. Il demanda s'il existe trois nombres rationnels dont la somme ainsi que le produit sont égaux à 1. Ce problème appartient évidemment à l'arithmétique élémentaire, mais, malgré les efforts des mathématiciens les plus éminents, il reste encore non résolu.

Dans l'énoncé original de M. MNICH, le problème concerne les nombres rationnels, mais il est facile de le transformer en problèmes équivalents concernant les entiers.

Le problème de MNICH est, s'il existe trois nombres rationnels  $u, v, w$ , tels que

$$u + v + w = uov = 1 . \quad (1)$$

Supposons que de tels nombres rationnels  $u, v, w$  existent.  $m$  étant leur dénominateur naturel commun, on peut les représenter sous la forme  $u = \frac{x}{m}, v = \frac{y}{m}, w = \frac{z}{m}$ , où  $x, y$  et  $z$  sont des entiers. Les équations (1) donnent alors

$$x + y + z = m \quad \text{et} \quad xyz = m^3 ,$$

ce qui donne tout de suite

$$(x + y + z)^3 = xyz . \quad (2)$$

---

<sup>1)</sup> Cet article paraîtra en anglais dans le volume consacré à la mémoire de J. GINSBURG.

La version française est augmentée de quelques détails.

Ainsi, s'il existe trois nombres rationnels satisfaisant aux équations (1), il existe aussi trois entiers non nuls, satisfaisant à l'équation (2), puisque  $xyz = m^3 > 0$ .

D'autre part, supposons qu'il existe trois entiers non nuls,  $x, y, z$ , satisfaisant à l'équation (2). D'après (2), si les nombres  $x, y, z$  sont non nuls, le nombre  $m = x + y + z$  est non nul et, d'après (2) on trouve  $m^3 = xyz \neq 0$  et, en posant  $u = \frac{x}{m}$ ,  $v = \frac{y}{m}$ ,  $w = \frac{z}{m}$  nous aurons trois nombres rationnels. D'après  $x + y + z = m$  et (2) on vérifie sans peine que les nombres  $u, v$  et  $w$  satisfont aux équations (1).

Ainsi le problème de savoir s'il existe trois nombres rationnels dont la somme et le produit sont égaux à 1 est équivalent au problème s'il existe trois entiers non nuls et tels que le cube de leur somme est égal à leur produit. Cette dernière question concerne seulement les entiers.

On pourrait aussi démontrer que le problème de MNICH équivaut au problème s'il existe trois entiers non nuls,  $x, y, z$ , tels que  $x^3 + y^3 + z^3 = xyz$ .

M. MNICH a aussi transformé son problème en d'autres équivalents, notamment en le problème s'il existe des entiers  $a, b$  et  $c$  tels que

$$\frac{a}{b} + \frac{b}{c} + \frac{c}{a} = 1. \quad (3)$$

S'il existe des nombres rationnels  $u, v, w$  satisfaisant à l'équation (1), on a  $u = \frac{k}{l}$ ,  $v = \frac{r}{s}$ , où  $k$  et  $r$  sont des entiers non nuls et  $l$  et  $s$  sont des nombres naturels, et, d'après (1), on trouve  $w = \frac{1}{uv} = \frac{ls}{kr}$  et, comme  $u + v + w = 1$ , on trouve  $\frac{kr}{l^r} + \frac{lr}{ls} + \frac{ls}{kr} = 1$ . En posant  $a = kr$ ,  $b = lr$ ,  $c = ls$  nous obtenons les entiers  $a, b$  et  $c$  satisfaisant à l'équation (3).

D'autre part, si  $a, b$  et  $c$  sont des entiers satisfaisant à l'équation (3), alors, en posant  $u = \frac{a}{b}$ ,  $v = \frac{b}{c}$ ,  $w = \frac{c}{a}$ , on obtient évidemment des nombres rationnels satisfaisant à l'équation (1).

M. MNICH a enfin transformé son problème en le suivant qui lui est équivalent:

Existe-t-il un nombre rationnel  $r$  tel que toutes les racines de l'équation

$$x^3 - x^2 + rx - 1 = 0 \quad (4)$$

sont rationnelles ?

On démontre sans peine cette équivalence. D'après les relations bien connues entre les racines d'un polynôme et ses coefficients, si  $x_1, x_2$  et  $x_3$  sont des racines du polynôme  $x^3 - x^2 + rx - 1$ , on a

$$x_1 + x_2 + x_3 = 1 \quad \text{et} \quad x_1 x_2 x_3 = 1 \quad (5)$$

D'autre part, si les nombres rationnels  $x_1, x_2$  et  $x_3$  satisfont aux équations (5), le nombre  $r = x_1 x_2 + x_2 x_3 + x_3 x_1$  est rationnel et on a pour tout  $x$

$$(x - x_1)(x - x_2)(x - x_3) = x^3 - x^2 + rx - 1$$

et on en conclut que  $x_1, x_2$  et  $x_3$  sont les seules racines de l'équation (4).

Le problème de MNICH est de trouver *trois* nombres rationnels dont la somme et le produit sont égaux à 1. Il se pose le problème de savoir s'il en est de même pour deux ou pour quatre nombres rationnels.

Existe-t-il deux nombres rationnels  $u$  et  $v$  tels que

$$u + v = uv = 1 ?$$

La réponse est négative. S'il existait de tels nombres  $u$  et  $v$ , on aurait  $u + \frac{1}{u} = 1$ , donc  $u^2 + 1 = u$ , d'où l'on conclut que  $u > 0$ , et on a  $(u - 1)^2 = u^2 - 2u + 1 = -u < 0$ , ce qui est impossible. Or, comme l'a démontré un élève de l'Université de Varsovie, André SCHINZEL, la réponse au problème de savoir s'il existe quatre nombres rationnels  $u, v, w, t$  tels que

$$u + v + w + t = uvwt = 1 \quad (6)$$

est positive. Il a prouvé que les équations (6) ont une infinité de solutions en nombres rationnels  $u, v, w, t$ . En effet, on vérifie sans peine que les nombres

$$u = \frac{n^2}{n^2 - 1}, \quad v = -\frac{1}{n^2 - 1}, \quad w = \frac{n^2 - 1}{n}, \quad t = -\frac{n^2 - 1}{n},$$

où  $n$  est un nombre naturel  $> 1$ , satisfont aux équations (6).

M. A. SCHINZEL a démontré aussi que, pour tout nombre

naturel  $s > 3$  il existe une infinité de systèmes de  $s$  nombres rationnels dont la somme et le produit sont égaux à 1.

Il est à remarquer que M. A. SCHINZEL a démontré que pour tout nombre naturel  $s$  l'équation

$$x_1 + x_2 + \dots + x_s = x_1 x_2 \dots x_s \quad (7)$$

a au moins une solution en nombres naturels  $x_1, x_2, \dots, x_s$ . Pour  $s = 2$  on a la solution  $x_1 = x_2 = 2$ . Pour obtenir une solution pour  $s > 2$ , il suffit de poser  $x_1 = x_2 = \dots = x_{s-2} = 1, x_{s-1} = 2, x_s = s$ . M. SCHINZEL a posé la question de savoir si le nombre de toutes les solutions de l'équation (7) en nombres naturels  $x_1, x_2, \dots, x_s$  croît indéfiniment avec  $s$ . Je ne sais même pas comment on pourrait démontrer que, pour  $s$  suffisamment grand, le nombre de ces solutions est  $> 1$ .

Nous avons vu que, dans l'état actuel de la science, nous ne savons pas répondre à la question de savoir si l'équation (2) qui est du troisième degré avec trois inconnues, a une solution en entiers non nuls. On connaît aussi plusieurs autres équations très simples du troisième degré avec trois inconnues dont nous ne savons pas trouver toutes les solutions en nombres entiers. Telle est, par exemple, l'équation

$$x^3 + y^3 + z^3 = 3. \quad (8)$$

Nous connaissons ici quatre solutions en nombres entiers, notamment  $x = y = z = 1$ ;  $x = y = 4, z = -5$ ;  $x = 4, y = -5, z = 4$ ;  $x = -5, y = z = 4$ . Mais nous ne savons pas s'il existe d'autres solutions de notre équation en nombres entiers, et même nous ne savons pas si le nombre de telles solutions est fini ou non. On ne connaît aucune méthode pour résoudre ce problème. Nous ne savons donc pas trouver toutes les décompositions du nombre 3 en une somme de trois cubes de nombres entiers et nous ne savons pas si le nombre de telles décompositions est fini ou non.

Il est à remarquer que s'il s'agissait de trouver toutes les décompositions d'un nombre naturel donné  $m$  en une somme de deux cubes, ou, en d'autres termes, de trouver toutes les solutions en nombres entiers  $x$  et  $y$  de l'équation  $x^3 + y^3 = m$ , on sait que le nombre de ces solutions est toujours fini et on connaît une méthode qui permettrait de les trouver toutes, si l'on effectue des calculs nécessaires.

D'autre part, il y a des équations du troisième degré à deux inconnues dont nous ne savons pas trouver toutes les solutions en nombres entiers. Telle est, par exemple, l'équation

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

On a démontré que le nombre de toutes les solutions de cette équation en nombres entiers  $x$  et  $y$  est fini, mais on ne sait pas quel est ce nombre.

Les problèmes non résolus d'arithmétique peuvent être divisés en deux espèces. Les problèmes de première espèce sont ceux où l'on connaît une voie qui peut conduire à la solution définitive du problème considéré, et la seule difficulté est que nous ne sommes pas actuellement en mesure d'effectuer les calculs nécessaires, à cause de leur longueur, même à l'aide des plus grandes machines à calculer. Tous les autres problèmes non résolus constituent la seconde espèce. Ce sont donc les problèmes où nous ne connaissons aucune voie pour les résoudre, même abstraction faite de la longueur des calculs nécessaires.

Un problème de la première espèce est, par exemple, le problème de trouver tous les diviseurs naturels du nombre  $2^{101} - 1$  qui a 31 chiffres décimaux. Pour trouver tous les diviseurs naturels de ce nombre, il suffirait de le diviser par les nombres naturels 1, 2, 3, ... ne dépassant pas le nombre  $\sqrt{2^{101} - 1}$  et de prendre en considération les diviseurs complémentaires. Pour réduire le nombre de preuves, on pourrait aussi utiliser ici le théorème d'après lequel tout diviseur naturel du nombre  $2^{101} - 1$  est de la forme  $202k + 1$ , où  $k$  est un entier non négatif. Mais toutefois les calculs excèdent nos possibilités. Deux diviseurs de notre nombre sont connus: 1 et  $2^{101} - 1$ . Or il est intéressant qu'on a démontré l'existence d'autres diviseurs naturels de notre nombre, tout au moins de deux autres, mais nous ne connaissons aucune décomposition de notre nombre en un produit de deux entiers  $> 1$ , quoiqu'on sache qu'une telle décomposition existe. Cependant pour le nombre  $2^{101}$  qui est un entier qui suit  $2^{101} - 1$ , nous connaissons tous ses diviseurs naturels, qui sont au nombre de 102: ce sont les 102 termes initiaux de la progression géométrique 1, 2, 4, 8, ...,  $2^{100}$ ,  $2^{101}$ . Ainsi les difficultés pour étudier les propriétés de deux entiers consécutifs peuvent être différentes.

Un autre exemple de problèmes de la première espèce est de trouver un nombre premier ayant mille chiffres. D'après le postulat de Bertrand, démontré par Tchebycheff, on démontre qu'il existe au moins trois nombres premiers ayant chacun un millier de chiffres, mais on n'a encore trouvé aucun de ces nombres. Le plus grand nombre premier connu,  $2^{2317} - 1$  a 969 chiffres.

Un nombre naturel étant donné, le problème de savoir s'il est premier ou non, s'il n'est pas résolu, est toujours un problème de la première espèce. Pour le résoudre, la méthode d'essais par divisions suffirait, mais le nombre des divisions nécessaires peut être très grand. Par exemple le problème de savoir si le nombre  $F_{13} = 2^{2^{13}} + 1$  qui a 2467 chiffres est premier ou non est un problème de première espèce.  $F_{13}$  est le plus petit nombre de Fermat  $F_n = 2^{2^n} + 1$  dont nous ne savons s'il est premier ou non.

Comme on sait, P. FERMAT supposait que tous les nombres  $F_n$ , où  $n = 1, 2, \dots$ , sont premiers. Tels sont les nombres  $F_n$  pour  $n = 1, 2, 3$  et  $4$ , mais, comme on l'a démontré plus tard, les nombres  $F_n$  sont composés pour  $5 \leq n \leq 12$ . A présent nous connaissons 35 nombres  $F_n$  composés dont le plus grand est le nombre  $F_{1945}$  qui a le facteur premier  $5 \cdot 2^{1947} + 1$ . Cependant le problème de savoir s'il existe une infinité de nombres  $F_n$  composés est un problème de seconde espèce. Il en est de même du problème de savoir s'il existe une infinité de nombres de Fermat premiers.

Un exemple d'un problème de première espèce est de trouver une décomposition du nombre 100 en une somme d'un nombre fini de fractions distinctes de la forme  $\frac{1}{n}$ , où  $n$  est un entier positif. (On appelle parfois ces fractions, fractions primaires.) On connaît une méthode qui fournirait une telle décomposition après certains calculs, mais à cause de la longueur de ces calculs il est actuellement impossible de la trouver. On a prouvé que dans chaque décomposition du nombre 100 en une somme d'un nombre fini de fractions distinctes  $\frac{1}{n}$ , où  $n$  est un nombre naturel, le nombre de termes a au moins 30 chiffres.

Il est arrivé qu'un problème de première espèce soit ensuite

résolu. Tel fut le cas du problème de savoir si les nombres  $F_{10}$  et  $F_{16}$  sont premiers. Il y a quelques années on a démontré qu'ils sont composés et on a trouvé pour chacun de ces nombres le plus petit facteur premier. Le développement complet en facteurs premiers de chacun de ces nombres reste cependant comme problème de première espèce.

Il y a aussi eu des cas où un problème de seconde espèce a été résolu. Il y a quelques années il en fut ainsi du problème de savoir s'il existe des entiers  $n > 1$  pour lesquels le nombre  $n \cdot 2^n + 1$  est premier. Les nombres de cette forme sont appelés *nombres de Cullen*. Récemment on a trouvé le plus petit de tels nombres premiers, à savoir pour  $n = 141$ .

Il est aussi arrivé qu'un problème de seconde espèce soit devenu problème de première espèce. Il en fut ainsi du problème de savoir si tout nombre impair  $> 7$  est une somme de trois nombres premiers impairs. Ce problème était de seconde espèce jusqu'au moment où J. Winogradow a démontré que tout nombre impair  $> a = 3^{3^{16}}$  est une somme de trois nombres premiers impairs. Pour un nombre impair donné, le problème de savoir s'il est ou non une somme de trois nombres premiers impairs est évidemment de première espèce. Il suffirait donc de vérifier si tout nombre impair  $> 7$  et  $\leq a$  est une somme de trois nombres premiers impairs.

Le problème de savoir s'il existe une progression arithmétique formée de cent nombres premiers distincts est de seconde espèce. La plus longue progression connue, formée de nombres premiers distincts est celle qui a douze termes, dont le premier est 23143 et dont la différence est 30030; elle a été trouvée par W. A. GOLUBIEFF.

On a démontré l'existence d'une infinité des progressions arithmétiques croissantes formées de trois nombres premiers, mais nous ne savons pas s'il en est de même pour les progressions formées de trois nombres premiers consécutifs  $p_n, p_{n+1}, p_{n+2}$  (où  $p_n$  désigne le  $n$ -ième nombre premier), par exemple 47, 53, 59.

Un autre exemple de problèmes de seconde espèce est s'il existe, sauf les nombres 2, 5 et 257, un nombre premier de la forme  $n^n + 1$ , où  $n$  est un nombre naturel.

Nous ne savons pas non plus s'il existe, sauf les nombres 2 et 17, des nombres premiers de la forme  $n^{n^n} + 1$ , où  $n$  est un nombre naturel. On peut démontrer que si un tel nombre premier existe, il a plus d'un milliard de milliards de chiffres, notamment qu'il est  $> 10^{10^{19}}$ . Si l'on risquait l'hypothèse que de tels nombres premiers n'existent pas, il en résulterait tout de suite l'existence d'une infinité de nombres de Fermat composés: en effet, tels seraient tous les nombres  $F_n$ , où  $n = m + 2^{m+2^m}$  et  $m = 1, 2, \dots$ , puisqu'on aurait alors  $F_n = k^{k^k} + 1$ , où  $k = 2^{2^m}$ .

De seconde espèce est aussi le problème de savoir s'il existe une infinité de nombres premiers de Mersenne:  $M_n = 2^n - 1$ . Actuellement on connaît 18 de ces nombres qui sont premiers et dont le plus grand est  $M_{3217}$ . De seconde espèce est aussi le problème de savoir s'il existe une infinité de nombres premiers  $p$  pour lesquels le nombre  $2^p - 1$  est composé. Nous ne savons pas non plus s'il existe une infinité de nombres naturels  $n$  pour lesquels le nombre  $2^n - 1$  n'est pas divisible par le carré d'un nombre naturel  $> 1$ .

De seconde espèce sont encore les problèmes suivants:

Existe-t-il une infinité de nombres premiers dont tous les chiffres décimaux sont égaux à 1 ?

Existe-t-il une infinité de nombres premiers de la forme  $x^2 + 1$ , où  $x$  est un entier ?

Existe-t-il une infinité de nombres premiers de la forme  $n! + 1$ , où  $n$  est un nombre naturel ? Nous ne savons pas si le nombre  $27! + 1$  est un nombre premier, mais ce problème est évidemment de première espèce. Or on démontre sans peine qu'il existe une infinité de nombres composés de la forme  $n! + 1$ .

Existe-t-il au moins un nombre pair  $> 2$  qui ne soit pas une somme de deux nombres premiers ?

En 1742 Ch. GOLDBACH a exprimé l'hypothèse que la réponse à cette question est négative. On a énoncé même une hypothèse plus forte, c'est que tout nombre pair  $> 6$  est une somme de deux nombres premiers distincts.

Peut-on représenter tout nombre pair comme une différence de deux nombres premiers d'une infinité de manières ? Nous ne savons même pas si le nombre 2 peut être représenté d'une

infinité de manières comme différence de deux nombres premiers, en d'autres termes, s'il existe une infinité de nombres premiers jumeaux. Nous ne savons pas non plus si tout nombre pair est la différence de deux nombres premiers.

N'existe-t-il, pour tout nombre naturel  $m$ , qu'un nombre fini de systèmes de nombres premiers  $p$  et  $q > p$ , où  $q - p < m$  ? Ce problème est équivalent au problème de savoir si la différence entre deux nombres premiers consécutifs croît indéfiniment avec ces nombres.

Est-il vrai que, pour tout nombre naturel  $n > 1$ , il existe entre  $n^2$  et  $n^2 + n$  au moins un nombre premier ?

Existe-t-il une infinité de nombres naturels  $n$ , tels que les nombres  $n$  et  $n + 1$  ont le même nombre de diviseurs naturels, respectivement la même somme de tous leurs diviseurs naturels ?

Existe-t-il une infinité de nombres premiers  $p$  tels que pour tout nombre naturel  $n < p - 1$  le reste de la division du nombre  $2^n$  par  $p$  est distinct de 1 ?

Existe-t-il une infinité des nombres naturels composés  $n$  tels que pour tout entier  $a$  le nombre  $a^n - a$  est divisible par  $n$  ? Il est à remarquer qu'on sait démontrer que, pour tout entier  $a$  il existe une infinité de nombres naturels  $n$  tels que le nombre  $a^n - a$  est divisible par  $n$ . Or, on ne sait pas s'il existe une infinité de nombres naturels composés  $n$  tels que les nombres  $2^n - 2$  et  $3^n - 3$  sont divisibles par  $n$ .

Existe-t-il une infinité de nombres naturels  $n$  tels que le nombre  $2^n - 2$  est divisible par  $n^2$  ?

Existe-t-il un nombre naturel impair  $n$  dont la somme de tous les diviseurs naturels est égale à  $2n$  ?

Existe-t-il un nombre naturel  $n$  dont la somme de tous les diviseurs naturels est égale à  $2n + 1$  ?

Deux nombres naturels distincts  $m$  et  $n$  sont appelés *amiables* si la somme de tous les diviseurs naturels de chacun est égale à  $m + n$ . Par exemple les nombres 220 et 284 sont amiables.

Existe-t-il une infinité de paires de nombres amiables ?

Existe-t-il une paire de nombres amiables dont l'un soit pair et l'autre impair ?

Existe-t-il un nombre composé  $n$  qui divise le nombre  $1^{n-1} + 2^{n-1} + \dots + (n-1)^{n-1} + 1$  ? En 1950 G. GIUGA a

exprimé l'hypothèse que la réponse à ce problème est négative. Il a vérifié cette hypothèse pour tous les  $n < 10^{1000}$ .

Existe-t-il un nombre naturel  $n > 7$  pour lequel le nombre  $n! + 1$  soit un carré ? On connaît trois de ces nombres  $\leq 7$ , notamment 4, 5 et 7.

Plusieurs problèmes de seconde espèce concernent la solution des équations en nombres entiers. Par exemple :

Existe-t-il au moins une solution de l'équation

$$x^3 + y^3 + z^3 = 30$$

en entiers  $x, y, z$  ?

Existe-t-il une solution en nombres naturels  $x_1, x_2, \dots, x_7$  du système de quatre équations du second degré à sept inconnues :

$$\begin{aligned} x_1^2 + x_2^2 &= x_4^2, & x_1^2 + x_3^2 &= x_5^2, & x_2^2 + x_3^2 &= x_6^2, \\ x_1^2 + x_2^2 + x_3^2 &= x_7^2 ? \end{aligned}$$

Le sens géométrique de ce problème est le suivant : Existe-t-il un parallélépipède rectangulaire tel que les longueurs de ses côtés, de ses diagonales et de sa diagonale intérieure s'expriment par des nombres naturels ?

Existe-t-il une infinité de nombres naturels  $a$  pour lesquels l'équation

$$a^2 = x^2 + y(y + 1)$$

n'a pas de solutions en nombres naturels  $x, y$  ? Récemment M. A. BIRMAN a démontré que ce problème équivaut au problème de savoir s'il existe une infinité de nombres premiers de la forme  $n^2 + 1$ , où  $n$  est un nombre naturel. Il a démontré aussi que le problème de savoir s'il existe une infinité de nombres naturels  $a > 1$  pour lesquels l'équation

$$a^2 = x^2 - y(y + 1)$$

n'a pas de solutions en nombres naturels  $x, y$  sauf la solution triviale  $x = a^2, y = a^2 - 1$ , est équivalent au problème de savoir s'il existe une infinité de nombres premiers jumeaux.

Existe-t-il pour tout nombre naturel  $n > 1$ , des nombres naturels  $x, y, z$ , tels que

$$\frac{5}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} ?$$

Mon hypothèse que la réponse en est positive fut vérifiée en 1958 par G. PALAMA pour tous les nombres naturels  $n$  tels que  $1 < n < 922321$ . Un problème analogue pour les nombres  $\frac{4}{n}$  fut posé, il y a plusieurs années, par P. ERDÖS.

Est-il vrai que l'équation  $x^4 + y^4 + z^4 = t^4$  n'a pas de solutions en nombres naturels  $x, y, z, t$ , ce qui était une hypothèse d'EULER ?

Est-t-il vrai que tout nombre naturel est une somme de quatre cubes de nombres entiers ?

Il y a quelques années, j'ai énoncé une hypothèse plus forte, à savoir que tout nombre entier peut être représenté d'une infinité de manières sous la forme  $x^3 + y^3 - z^3 - t^3$ , où  $x, y, z$  et  $t$  sont des nombres naturels. Cette hypothèse fut vérifiée pour tous les nombres naturels  $\leq 350$ , sauf 148 et 284, et aussi pour une infinité d'autres. Or il est facile de démontrer que tout entier peut être représenté d'une infinité de manières comme une somme de cinq cubes des nombres entiers. Cela résulte tout de suite de la remarque que, d'après l'identité  $6k = (k + 1)^3 + (k - 1)^3 + (-k)^3 + (-k)^3$ , tout entier divisible par 6 est une somme de quatre cubes d'entiers et que, pour  $t$  et  $n$  entiers, chacun des nombres  $6t + r - (6n + r)^3$ , où  $r = 0, 1, 2, 3, 4, 5$ , est divisible par 6.

Est-il possible de représenter comme une somme de trois cubes de nombres entiers tout nombre naturel qui, divisé par 9, donne un reste distinct de 4 et de 5 ?

Est-il possible de représenter tout nombre naturel sous la forme  $x^3 + y^3 + 2z^3$ , où  $x, y$  et  $z$  sont des entiers ? Le plus petit nombre naturel dont on ne sait pas s'il est de cette forme est 76; le suivant est 99.

Existe-t-il des nombres naturels  $n, x, y, z$  tels que  $n > 2$  et  $x^n + y^n = z^n$  ?

P. FERMAT affirmait, sans avoir donné de démonstration, qu'il n'existe pas de tels nombres. Cela est à présent démontré pour tous les exposants  $n$  tels que  $2 < n \leq 4002$ , et pour une infinité d'autres  $n$ . La démonstration pour  $n = 3$  est difficile; elle est plus simple pour  $n = 4$ .

Existe-t-il, sauf  $8 = 2^3$  et  $9 = 3^2$ , deux nombres naturels successifs dont chacun soit une puissance d'un nombre naturel

avec un exposant  $> 1$  ? CATALAN a exprimé l'hypothèse qu'il n'y a pas de tels nombres.

Existe-t-il trois nombres naturels successifs dont chacun soit une puissance d'un nombre naturel avec un exposant  $> 1$  ? On démontre sans peine qu'il n'existe pas quatre de ces nombres naturels successifs.

Est-il vrai que pour tout nombre naturel  $m$  il existe seulement un nombre fini de systèmes d'entiers  $> 1$ ,  $x, y, z, t$  satisfaisant aux inégalités  $0 < x^y - z^t < m$  ? En 1945 S. PILLAI a exprimé une hypothèse qui est équivalente avec celle que la réponse à ce problème est positive.

Soit  $n$  un nombre naturel  $> 10$  dans le système décimal. Est-il toujours possible de remplacer deux de ses chiffres par d'autres chiffres de sorte qu'on obtienne un nombre premier ? Il est à remarquer qu'il n'est pas toujours possible de changer un seul chiffre d'un nombre naturel de sorte qu'on obtienne un nombre premier. On peut démontrer que 200 est le plus petit nombre dont on n'obtient jamais un nombre premier, en changeant un seul chiffre.

Existe-t-il trois entiers impairs  $> 1$ ,  $x, y, z$  tels que  $x^x y^y = z^z$  ?

Est-il vrai que si  $x, y$  et  $z$  sont des nombres naturels  $> 1$  tels que  $x^x y^y = z^z$ , alors  $x$  et  $y$  ont les mêmes diviseurs premiers ? Ce problème fut posé par A. SCHINZEL.

On a démontré que tout nombre rationnel positif dont le dénominateur est impair est une somme d'un nombre fini de fractions distinctes, de la forme  $\frac{1}{n}$ , où  $n$  est un nombre naturel impair. Or nous ne savons pas si le procédé suivant, proposé par S. STEIN en 1955 amène toujours à une telle décomposition.

Etant donné un nombre rationnel positif  $r$  avec un dénominateur impair, déterminons le plus petit nombre naturel impair  $n_1$ , tel que  $r \geq \frac{1}{n_1}$ . En supposant que nous avons déjà déterminé les nombres  $n_1, n_2, \dots, n_k$ , déterminons le plus petit nombre naturel impair  $n_{k+1}$ , tel que  $r - \frac{1}{n_1} - \frac{1}{n_2} \dots - \frac{1}{n_k} \geq \frac{1}{n_{k+1}}$ . Le problème posé par S. STEIN est de savoir si, en procédant ainsi, on arrive toujours après un nombre fini  $s$  de pas, à l'égalité  $r - \frac{1}{n_1} - \frac{1}{n_2} \dots - \frac{1}{n_{s-1}} = \frac{1}{n_s}$ , qui donnerait la décomposition

cherchée du nombre  $r$  en une somme d'un nombre fini de fractions distinctes  $\frac{1}{n}$ , où  $n$  désigne des nombres naturels impairs.

Il y a quelques années, j'ai posé le problème suivant:  $n$  étant un nombre naturel  $> 1$ , rangeons les nombres  $1, 2, 3, \dots, n^2$  en  $n$  lignes,  $n$  nombres dans chaque ligne:

$$\begin{array}{l} 1, 2, 3, \dots, n \\ n + 1, n + 2, \dots, 2n \\ 2n + 1, \dots, 3n \\ \dots \dots \dots \dots \dots \dots \dots \\ (n - 1)n + 1, \dots, n^2. \end{array}$$

Est-il vrai qu'on trouvera toujours au moins un nombre premier dans chaque ligne ?

La première ligne contient évidemment (pour  $n > 1$ ) le nombre premier 2. La proposition que la deuxième ligne contient toujours (pour  $n > 1$ ) au moins un nombre premier équivaut au théorème qui a été démontré il y a plus d'un siècle par TSCHEBYCHEFF, notamment que pour  $n > 1$  il existe au moins un nombre premier entre  $n$  et  $2n$ . On peut aussi démontrer que, pour  $n \geq 9$ , chacune des neuf premières lignes de notre table contient au moins un nombre premier.

André SCHINZEL a vérifié à l'aide des tables de Western que pour  $n \leq 3000$  la réponse à notre problème est positive.

Il est à remarquer que de l'hypothèse que chacune des deux dernières lignes de notre table contient au moins un nombre premier, il résulte tout de suite qu'entre deux carrés consécutifs de nombres naturels ils existe toujours au moins deux nombres premiers. Or, on n'a pas encore démontré cela. Une autre conséquence facile de l'hypothèse dont nous parlons est qu'entre deux cubes successifs de nombres naturels il existe toujours au moins deux nombres premiers. Or il est à remarquer qu'en 1947 W. H. MILLS a démontré que pour les nombres naturels  $n$  suffisamment grands il existe entre  $n^3$  et  $(n + 1)^3$  au moins un nombre premier.

A. SCHINZEL a exprimé l'hypothèse que si  $k$  est un nombre  $< n$  et premier avec  $n$ , la  $k$ -ième colonne de notre table contient au moins un nombre premier. M. GORZELEWSKI a vérifié que cela est vrai pour  $n \leq 100$ .

De l'hypothèse que (pour  $n > 1$ ) toute ligne de la table (1) contient au moins un nombre premier, on déduit sans peine qu'entre deux nombres triangulaires consécutifs il existe toujours au moins un nombre premier, en d'autres termes, si l'on écrit successivement les nombres naturels en lignes,  $n$  nombres dans la  $n$ -ième ligne

1  
2, 3  
4, 5, 6  
7, 8, 9, 10  
11, 12, 13, 14, 15  
.....

alors chaque ligne à partir de la deuxième contient au moins un nombre premier. On ne sait pas si cela est vrai.

A. SCHINZEL a énoncé récemment une hypothèse plus forte que l'hypothèse sur la table dont nous avons parlé. C'est l'hypothèse suivante:

Si  $x$  est un nombre réel  $\geq 117$ , il existe au moins un nombre premier entre  $x$  et  $x + \sqrt{x}$ .

A. SCHINZEL a vérifié son hypothèse pour tous les nombres  $x$  tels que  $117 \leq x < 10^7$ . Il est à remarquer que LEGENDRE a exprimé l'hypothèse que pour les nombres  $x$  suffisamment grands, il existe au moins un nombre premier entre  $x$  et  $x + \sqrt{x}$ .

Une autre hypothèse de A. SCHINZEL est que pour tout nombre réel  $x \geq 8$  il existe au moins un nombre premier entre  $x$  et  $x + (\log x)^2$ . Si l'on désigne par  $p_n$  le  $n$ -ième nombre premier, et si l'on pose ici, pour  $n > 4$ ,  $x = p_n$ , on obtient l'inégalité  $p_{n+1} - p_n < (\log p_n)^2$ , qui est plus forte que l'hypothèse de H. CRAMER sur la différence  $p_{n+1} - p_n$  de l'année 1937, énoncée à la page 24 du volume 2 du journal *Acta Arithmetica* paraissant en Pologne.

En 1957 A. SCHINZEL a énoncé encore une autre hypothèse sur les nombres premiers (qui a paru dans le volume IV des *Acta Arithmetica*).

Soit  $s$  un nombre naturel donné et soient  $f_1(x), f_2(x), \dots, f_s(x)$  des polynômes en  $x$  aux coefficients entiers où le coefficient de la plus grande puissance de  $x$  est positif. Nous dirons que les polynômes  $f_1(x), \dots, f_s(x)$  satisfont à la condition S s'ils sont

irréductibles et s'il n'existe aucun entier  $> 1$  qui, pour tout  $x$  entier, soit un diviseur du produit  $f_1(x) f_2(x) \dots f_s(x)$ .

L'hypothèse H de A. SCHINZEL est la suivante:

H. Soit  $s$  un nombre naturel et  $f_1(x), f_2(x), \dots, f_s(x)$  une suite de polynômes aux coefficients entiers, où le coefficient de la plus grande puissance de  $x$  est positif. Si ces polynômes satisfont à la condition S, il existe une infinité de nombres naturels  $x$  pour lesquels chacun des nombres  $f_1(x), f_2(x), \dots, f_s(x)$  est premier.

De l'hypothèse H de A. SCHINZEL résultent sans peine plusieurs conséquences, par exemple celle que tout nombre entier peut être d'une infinité de manières représenté comme différence de deux nombres premiers consécutifs. Une autre conséquence de l'hypothèse H est qu'il existe des progressions arithmétiques aussi longues que l'on veut, formées des nombres premiers consécutifs. Une autre conséquence est celle qu'il existe pour tout nombre naturel  $m$  une infinité de nombres naturels  $x$  pour lesquels le nombre  $x^2 + m$  est premier.

Voici encore deux problèmes non résolus:

Est-il vrai que dans le développement décimal du nombre  $\sqrt{2}$  le chiffre 1 se trouve une infinité de fois ?

Est-il vrai que dans le développement décimal du nombre  $\pi$  la suite formée de chiffres consécutifs 123456789 se trouve au moins une fois ?

Il y a beaucoup d'autres problèmes non résolus d'arithmétique. Leur nombre augmente toujours, puisqu'on pose plus rapidement les nouveaux problèmes qu'on ne résout les anciens parmi lesquels il y a des problèmes posés il y a quelques centaines d'années et encore non résolus.<sup>1)</sup> Or notre connaissance de l'arithmétique consiste non seulement à savoir ce qui est déjà établi, mais aussi à savoir quels sont les problèmes importants qui ne sont pas encore résolus.

<sup>1)</sup> Lorsque j'ai dit cela à ma conférence à l'Université de Rennes, le professeur Antoine a dit qu'alors il y aurait des problèmes qui ne seraient jamais résolus. J'ai répondu que cela pouvait naturellement arriver, mais que si l'humanité existait un temps infini, il pourrait aussi arriver cette situation paradoxale que le nombre des problèmes non résolus croisse indéfiniment et que néanmoins chaque problème soit résolu en son temps. En effet, imaginons qu'on pose chaque année dix problèmes, tous numérotés au moyen des nombres naturels consécutifs et qu'on résolve chaque année un seul problème: celui des problèmes posés jusqu'à ce moment qui a le numéro le plus petit. (Par exemple, après dix années seront posés les problèmes 1, 2, 3, ..., 100 et résolus les problèmes, 1, 2, ..., 10). Le problème numéro  $n$  sera donc résolu après  $n$  années.