L'hypothèse analogue pour k impair ne serait pas justifiée. Il est vrai que l'équation $\varphi(x+1) = \varphi(x)$ a pour $x \leqslant 10000$, 18 solutions 1, 3, 15, 104, 164, 194, 255, 495, 584, 975, 2204, 2625, 2834, 3255, 3705, 5186, 5187 (cf. [1]), mais l'équation $\varphi(x+3) = \varphi(x)$ a pour $x \leqslant 10000$ les seules solutions $x = 3$ et $x = 5$, alors que l'équation $\varphi(x+2) = \varphi(x)$ a 80 solutions pour $x \leqslant 10000$.

Travaux cités

[1] L. Moser, *Some equations involving Euler's totient function*, The American Math. Monthly 56 (1949), p. 21-22.

[2] W. Sierpiński, *Sur une propriété de la fonction* $\varphi(n)$, Publ. Math., Debrecen, 4 (1956), p. 184-185.

Reçu par la Rédaction le 17. 5. 1957

Sur certaines hypothèses concernant les nombres premiers

par

A. Schinzel et W. Sierpiński (Warszawa)

La répartition des nombres premiers parmi les nombres naturels n'est pas encore suffisamment étudiée: c'est pourquoi depuis les temps les plus anciens on a énoncé diverses hypothèses concernant les nombres premiers. Plusieurs de ces hypothèses se sont montrées fausses; quelques unes d'elles ne sont pas encore mises en défaut, et il y en a qui sont vérifiées pour tous les nombres ne dépassant pas un nombre très grand.

Une de plus anciennes hypothèses sur les nombres premiers, ayant au moins 25 siècles, était celle des Chinois: un nombre naturel $n > 1$ est premier si et seulement si le nombre $2^n - 2$ est divisible par n. La nécessité de cette condition a été démontrée il y a quelques centaines d'années. En 1681 Leibniz a essayé de démontrer qu'elle est suffisante, mais sa démonstration était basée sur un raisonnement faux, et en 1819 on a trouvé que l'hypothèse des Chinois était fausse, puisque le nombre $2^{341} - 2$ (qui a 103 chiffres) est divisible par 341, bien que le nombre $341 = 11 \cdot 31$ ne soit pas premier. Ensuite on a démontré (de nos temps) qu'il existe une infinité de nombres composés n pour lesquels le nombre $2^n - 2$ est divisible par n, impairs aussi bien que pairs. (Le plus petit de ces nombres pairs est le nombre $n = 161038 = 2 \cdot 73 \cdot 1103$ trouvé en 1950 par D. H. Lehmer).

P. Fermat supposait premiers tous les nombres $F_n = 2^{2^n} + 1$, où $n = 0, 1, 2, \ldots$ Cela est vrai pour $n = 0, 1, 2, 3$ et 4, mais, comme l'a trouvé L. Euler en 1772, le nombre F_5 (qui a 10 chiffres) est composé, car il est divisible par 641. Maintenant nous connaissons 29 nombres F_n composés, pour $n = 5, 6, 7, 8, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 39, 55, 63, 73, 117, 125, 144, 150, 207, 226, 228, 268, 284, 316, 452$.

On peut donc énoncer l'hypothèse qu'il existe une infinité de nombres F_n composés. On a même énoncé l'hypothèse plus forte: les nombres F_n premiers sont en nombre fini. Ce sont peut-être seulement ceux que connaissait Fermat, à savoir les nombres F_n pour $n \leqslant 4$.

Le plus petit nombre F_n dont nous ne sachions pas s'il est premier ou non est F_{13}. Le plus grand nombre F_n composé connu est F_{45}, dont le plus petit diviseur premier est le nombre $27 \cdot 2^{455}+1$ (voir [14]).

Le fait que le nombre F_{16} est composé met en défaut l'hypothèse que tous les nombres de la suite infinie

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ 2^{2^{2^{2^2}}}+1,\ \ldots$$

sont premiers, puisque F_{16} est le cinquième terme de cette suite.

Quant aux nombres de Mersenne $M_n = 2^n-1$ on a énoncé l'hypothèse que si le nombre M_n est premier, le nombre M_{M_n} est aussi premier. Or, d'après un calcul qui a été fait en 1953 par D. J. Wheeler, le nombre $M_{M_{13}} = 2^{8191}-1$ (qui a 2466 chiffres) est composé, bien que le nombre M_{13} soit premier.

On a encore énoncé l'hypothèse que les nombres q_n ($n = 0, 1, 2, \ldots$), où $q_0 = 2$ et $q_{k+1} = 2^{q_k}-1$ pour $k = 0, 1, 2, \ldots$, sont tous premiers. Cela est vrai pour $0 \leqslant n \leqslant 4$. Or, le nombre q_5 a plus de 10^{37} chiffres et nous ne savons pas s'il est premier ou non.

En 1742 Ch. Goldbach a énoncé l'hypothèse que tout nombre pair >4 est la somme de deux nombres premiers impairs. On peut énoncer l'hypothèse G un peu plus forte: tout nombre pair >6 est la somme de deux nombres premiers distincts. On peut démontrer que l'hypothèse G équivaut à l'hypothèse que tout nombre naturel >17 est la somme de trois nombres premiers distincts. Or, de l'hypothèse de Goldbach A. Schinzel a déduit que tout nombre impair >17 est la somme de trois nombres premiers distincts. En 1937 J. Vinogradoff a démontré que tout nombre impair suffisamment grand est la somme de trois nombres premiers impairs. Quant à l'hypothèse G, S. Gołaszewski et B. Leszczyński l'ont vérifiée pour tous les nombres pairs $\leqslant 50000$.

On a aussi énoncé l'hypothèse que le nombre des décompositions d'un nombre pair $2n$ en une somme de deux nombres premiers tend vers l'infini avec n (cf. [10], Conjecture A). Il est probable que les nombres pairs >188 ont plus de 10 décompositions et que les nombres pairs >4574 donnent plus de 100 décompositions.

Nous déduirons de l'hypothèse G quelques conséquences.

P_1. *Tout nombre impair est de la forme $n-\varphi(n)$ où n est un nombre naturel.*

Démonstration de l'implication $G \to P_1$. On a $1 = 2-\varphi(2)$, $3 = 9-\varphi(9)$, $5 = 25-\varphi(25)$. Si m est un nombre impair >5 on a $m+1 > 6$ et de G résulte l'existence des nombres premiers distincts p et q tels que $m+1 = p+q$ et on a $pq-\varphi(pq) = pq-(p-1)(q-1) = p+q-1 = m$, donc $m = n-\varphi(n)$ pour $n = pq$. L'implication $G \to P_1$ se trouve ainsi démontrée.

P_2. *Tout nombre impair $m > 7$ est de la forme $\sigma(n)-n$, où n est un nombre impair $> m$.*

Démonstration de l'implication $G \to P_2$. Si m est un nombre impair >7, il résulte de G qu'il existe des nombres premiers distincts p et $q < p$ tels que $m-1 = p+q$, et on a $\sigma(pq)-pq = (p+1)(q+1)-pq = p+q+1 = m$. Comme m est impair >7, les nombres p et q sont impairs, $q \geqslant 3$, donc $pq \geqslant 3p = 2p+p > p+q+1 = m$ et en posant $n = pq$ on obtient un nombre impair $n > m$ tel que $m = \sigma(n)-n$. L'implication $G \to P_2$ est ainsi démontrée.

P. Erdös a posé la question s'il existe une infinité de nombres naturels qui ne sont pas termes de la suite $\sigma(n)-n$. (Tels sont par exemple les nombres 2 et 5). Une question analogue peut être posée pour la suite $n-\varphi(n)$. (Les quatre nombres naturels les plus petits qui ne sont pas termes de cette suite sont 10, 26, 34 et 50).

$P_{2,1}$. *Il existe des suites aussi longues que l'on veut*

$$(1) \qquad n,\ f(n),\ ff(n),\ fff(n),\ \ldots, \quad \text{où} \quad f(n) = \sigma(n)-n,$$

dont le dernier terme est 1.

Démonstration de l'implication $P_2 \to P_{2,1}$. D'après P_2 pour tout nombre impair $m > 7$ il existe un nombre impair $n = g(m) > m$, tel que $f(n) = m$. Pour tout n impair >7 la suite infinie de nombres naturels

$$n,\ g(n),\ gg(n),\ \ldots$$

est donc croissante. k étant un nombre naturel, posons $n = g^k(11)$. Nous obtenons ainsi la suite

$$n = g^k(n),\ f(n) = g^{k-1}(n),\ \ldots,\ f^k(n) = 11,\ f^{k+1}(n) = 1$$

(puisque $f(11) = \sigma(11)-11 = 1$) qui a $k+2$ termes dont le dernier est $=1$. L'implication $P_2 \to P_{2,1}$ se trouve ainsi démontrée.

$P_{2,2}$. *Il existe un infinité de nombres naturels n tels que la suite infinie (1) est périodique.*

Démonstration de l'implication $P_2 \to P_{2,2}$. Soit $g(m)$ la fonction définie dans la démonstration de l'implication $P_2 \to P_{2,1}$ et posons pour k naturels $n = g^k(25)$. Nous obtiendrons la suite

$$n = g^k(25),\ f(n) = g^{k-1}(25),\ \ldots,\ f^k(n) = 25,\ f^{k+i}(n) = 6$$

pour $i = 1, 2, \ldots$ (puisque $f(25) = 6$ et $f(6) = 6$).

La suite infinie (1) a donc ici k nombres impairs suivis d'une infinité de nombres 6.

Il est à remarquer que L. E. Dickson a énoncé l'hypothèse que pour tout nombre naturel $n > 1$ la suite (1) ou bien se termine par le nombre 1 ou bien elle est périodique (Dickson [5]; cf. Catalan [3]).

On voit sans peine que l'on peut exprimer cette hypothèse en disant que la suite (1) et toujours bornée.

On ne sait pas s'il existe une infinité de nombres naturels n pour lesquels la suite (1) est périodique et la période est pure (comme par exemple pour $n = 220$, où la période est formée de deux termes ou pour $n = 12496$, où la période est formée de 5 termes).

En 1950 G. Giuga a énoncé l'hypothèse que pour qu'un nombre naturel $p > 1$ soit premier, il faut et il suffit que le nombre $1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1}+1$ soit divisible par p. (On démontre sans peine que cette condition est nécessaire). Il affirme que cette hypothèse est vraie pour tous les nombres $< 10^{1000}$.

Hypothèse de A. Schinzel. A. Schinzel a énoncé l'hypothèse H_0 suivante:

H_0. *s étant un nombre naturel et $f_1(x), f_2(x), \ldots, f_s(x)$ des polynômes en x à coefficients entiers, où le coefficient de la plus haute puissance de x est positif, et satisfaisant à la condition*

S. *Il n'existe aucun entier > 1 qui divise le produit $f_1(x)f_2(x)\ldots f_s(x)$ quel que soit l'entier x,*

alors il existe au moins un nombre naturel x pour lequel les nombres $f_1(x), f_2(x), \ldots, f_s(x)$ sont tous premiers.

On démontre sans peine que l'hypothèse H_0 équivaut à l'hypothèse H suivante:

H. *s étant un nombre naturel et $f_1(x), f_2(x), \ldots, f_s(x)$ des polynômes en x satisfaisant aux conditions de l'hypothèse H_0, il existe une infinité de nombres naturels x pour lesquels les nombres $f_1(x), f_2(x), \ldots, f_s(x)$ sont premiers.*

En effet, supposons que l'hypothèse H_0 soit vraie et soient $f_1(x), f_2(x), \ldots, f_s(x)$ des polynômes satisfaisant aux conditions de l'hypothèse H_0. On démontre sans peine que, quel que soit le nombre naturel k, les polynômes $f_1(x+k), f_2(x+k), \ldots, f_s(x+k)$ satisfont aussi aux conditions de l'hypothèse H_0. D'après H_0 il existe donc un nombre naturel x tel que les nombres $f_1(x+k), f_2(x+k), \ldots, f_s(x+k)$ sont tous premiers et, comme on le prouve aisément, pour k suffisamment grand tous ces nombres premiers sont aussi grands que l'on veut. On a donc $H_0 \to H$ et comme, d'autre part, on a évidemment $H \to H_0$, l'équivalence $H_0 \equiv H$ se trouve démontrée.

Quant à l'hypothèse H il est à remarquer que du théorème 1 du travail de G. Ricci [13] on déduit sans peine que si les polynômes $f_1(x), f_2(x), \ldots, f_s(x)$ satisfont aux conditions de l'hypothèse H_0, il existe une constante C dépendant de $f_1, f_2, \ldots, f_s$ telle que pour une infinité de nombres naturels x chacun des nombres $f_1(x), f_2(x), \ldots, f_s(x)$ a au plus C diviseurs premiers.

Nous déduirons maintenant de l'hypothèse H plusieurs conséquences.

C_1. *Si s est un nombre naturel, $a_1 < a_2 < \ldots < a_s$ des entiers et si les binômes $f_i(x) = x + a_i$ $(i = 1, 2, \ldots, s)$ satisfont à la condition* S, *il existe une infinité de nombres naturels x pour lesquels $f_1(x), f_2(x), \ldots, f_s(x)$ sont des nombres premiers consécutifs.*

Démonstration de l'implication $H \to C_1$. Nos binômes étant irréductibles et satisfaisant à la condition S, il résulte de H qu'il existe une infinité de nombres naturels x pour lesquels les nombres $f_i(x)$ $(i = 1, 2, \ldots, s)$ sont premiers. Soit $h \geqslant a_s - 2a_1 + 2$ un tel nombre naturel et posons

$$b = \frac{(h+a_s)!}{(h+a_1)!(h+a_2)\ldots(h+a_s)} \tag{1}$$

et

$$g_i(x) = bx + h + a_i \quad \text{pour} \quad i = 1, 2, \ldots, s.$$

On a $2(h+a_i) = h+h+2a_i \geqslant h+h+2a_1 \geqslant h+a_s+2 > h+a_s$ et, le nombre $h+a_i = f_i(h)$ étant premier, les facteurs de $(h+a_s)!$ autres que $h+a_i$, étant $< 2(h+a_i)$, ne sont pas divisibles par $h+a_i$ et il en résulte que $(b, h+a_i) = 1$.

Supposons maintenant qu'il existe un nombre premier p tel que $p \mid g_1(x)g_2(x)\ldots g_s(x)$ pour $x = 0, 1, 2, \ldots, p-1$. On a donc $p \mid g_1(0)g_2(0)\ldots g_s(0) = (h+a_1)(h+a_2)\ldots(h+a_s)$ et tous ces facteurs étant premiers, il existe un nombre naturel $k \leqslant s$ tel que $p = h+a_k$ et d'après (1) et $h+a_s < 2(h+a_k) = 2p$ on en conclut que p ne divise pas b. Il existe donc pour tout nombre naturel $i \leqslant s$ un seul nombre x de la suite $0, 1, 2, \ldots, p-1$, tel que $p \mid bx+h+a_i = g_i(x)$ et il résulte tout de suite de $p \mid g_1(x)g_2(x)\ldots g_s(x)$ pour $x = 0, 1, 2, \ldots, p-1$ que $p \leqslant s$, donc $h+a_k \leqslant s$, et comme, d'autre part, $h+a_k \geqslant h+a_1 \geqslant a_s - a_1 + 2 \geqslant s+1$ (puisque les entiers $a_1, a_2, \ldots, a_s$ vont en croissant) on aboutit à une contradiction.

Les binômes irréductibles $g_i(x)$ $(i = 1, 2, \ldots, s)$ satisfont donc à la condition S et, d'après H, il existe une infinité de nombres naturels x tels que les nombres $g_i(x)$ $(i = 1, 2, \ldots, s)$ sont premiers. Si pour un tel

x ces nombres premiers n'étaient pas consécutifs, il existerait un entier j tel que $a_1 \leqslant j \leqslant a_s$ et $j \neq a_1, a_2, \ldots, a_s$ tel que le nombre $q = bx+h+j > h+j$ serait premier. Or, comme $a_1 \leqslant j \leqslant a_s$ et $j \neq a_1, a_2, \ldots, a_s$, on a, d'après (1), $h+j|b$, donc $h+j|q > h+j$, ce qui est impossible, puisque $h+j > h+a_1$ qui est premier.

L'implication H $\rightarrow$ C_1 se trouve ainsi démontrée.

$C_{1.1}$. *Tout nombre pair peut être représenté d'une infinité de manières comme la différence de deux nombres premiers consécutifs.*

Démonstration de l'implication $C_1 \rightarrow C_{1.1}$. Soit $f_1(x) = x$, $f_2(x) = x+2n$ (où n est un nombre naturel donné). Comme $(f_1(1)f_2(1), f_1(2)f_2(2)) = (2n+1, 2(2+2n)) = 1$, il résulte de C_1 qu'il existe une infinité de nombres naturels x tels que x et $x+2n$ sont deux nombres premiers consécutifs, soit $x = p_k$, $x+2n = p_{k+1}$ (où p_i désigne le i-ème nombre premier), d'où $2n = p_{k+1}-p_k$. Cela prouve que $C_1 \rightarrow C_{1.1}$ (cf. Hardy and Littlewood [10], Conjecture B).

$C_{1.2}$. *m étant un nombre naturel donné, il existe $2m$ nombres premiers consécutifs formant m couples de nombres jumeaux.*

Démonstration de l'implication $C_1 \rightarrow C_{1.2}$. Soit

$$f_{2i-1}(x) = x+(2m)!\,(i-1),$$

$$f_{2i}(x) = x+(2m)!\,(i-1)+2 \qquad \text{pour} \qquad i = 1, 2, \ldots, n$$

et

$$P(x) = f_1(x)f_2(x)\ldots f_{2m}(x).$$

Soit p est un nombre premier tel que $p|P(x)$ pour $x = 0, 1, \ldots, p-1$. Comme $P(x)$ est un polynôme en x de degré $2m$ où le coefficient de x^{2m} est $= 1$, d'après le théorème de Lagrange la congruence $P(x) \equiv 0 \pmod p$ a au plus $2m$ racines. Or, comme $P(x) \equiv 0 \pmod p$ pour $x = 0, 1, \ldots, p-1$, on en conclut que $p \leqslant 2m$. Mais $P(1)$ est évidemment un nombre impair et comme $p|P(1)$, on trouve $p > 2$. D'autre part, d'après $p \leqslant 2m$ on a $p|(2m)!\,i$ pour i entier et comme $p|P(2)$, on trouve $p|2^{3m}$, ce qui est impossible. Les binômes $f_j(x)$ $(j = 1, 2, \ldots, 2m)$ satisfont donc à la condition S et il résulte de C_1 qu'il existe une infinité de nombres naturels x tels que $f_j(x)$ $(j = 1, 2, \ldots, 2m)$ sont des nombres premiers consécutifs, $f_j(x) = p_{k+j-1}$ pour $j = 1, 2, \ldots, 2m$. On a donc $p_{k+2i-1}-p_{k+2i-2} = 2$ pour $i = 1, 2, \ldots, n$ et l'implication $C_1 \rightarrow C_{1.2}$ se trouve démontrée.

On peut démontrer pareillement qu'il existe pour tout m naturel $4m+1$ nombres premiers consécutifs dont les $2m$ premiers et de même les $2m$ derniers donnent m couples de nombres jumeaux.

V. Thébault a démontré [18] que si $n > 1$ termes d'une progression arithmétique de raison r sont des nombres premiers $> n$, alors r est divisible par tout nombre premier $\leqslant n$. Or, nous démontrerons que C_1 entraîne la conséquence suivante:

$C_{1.4}$. *Si r est un nombre naturel divisible par tout nombre premier $\leqslant n$, où n est un nombre naturel donné > 1, il existe une infinité de systèmes de n nombres premiers consécutifs formant une progression arithmétique de raison r.*

Démonstration de l'implication $C_1 \rightarrow C_{1.4}$. Soit $f_i(x) = x+ir$ pour $i = 0, 1, 2, \ldots, n-1$. S'il existait un nombre premier p tel que $p|f_0(x)f_1(x)\ldots f_{n-1}(x)$ pour $x = 0, 1, 2, \ldots, p-1$, il résulterait du théorème de Lagrange que $p \leqslant n$, donc $p|r$. D'autre part on a

$$p|f_0(1)f_1(1)\ldots f_{n-1}(1) = 1(1+r)(1+2r)\ldots(1+(n-1)r)$$

et vu que $p|r$ on trouve $p|1$, ce qui est impossible. La condition S est donc satisfaite et il résulte de C_1 qu'il existe une infinité de nombres naturels x tels que les nombres $f_i(x)$ $(i = 1, 2, \ldots, n)$ sont des nombres premiers consécutifs. Nous avons ainsi démontré que $C_1 \rightarrow C_{1.4}$.

En particulier, pour $n = 3$, il résulte de $C_{1.4}$ qu'il existe pour tout nombre naturel h une infinité de nombres naturels k tels que $p_{k+1}-p_k = p_{k+2}-p_{k+1} = 6h$. Il en résulte qu'il existe une infinité de progressions arithmétiques formées de trois nombres premiers consécutifs. Or, d'après L. E. Dickson ([6], p. 425) Moritz Cantor a énoncé l'hypothèse ([2]) que trois nombres premiers consécutifs dont aucun n'est le nombre 3 ne peuvent pas former de progression arithmétique. En 1955 A. Schinzel a remarqué que cette hypothèse est en défaut puisque 47, 53 et 59 sont trois nombres premiers consécutifs formant une progression arithmétique de raison 6. Parmi les nombres < 1000 on trouve plusieurs telles progressions dont les premiers termes sont respectivement 151, 167, 367, 557, 587, 601, 647, 727, 941, 971. Les nombres 199, 211 et 223 et pareillement les nombres 1499, 1511 et 1523 forment des progressions arithmétiques de raison 12 composées de nombres premiers consécutifs et les nombres

$$251,\ 257,\ 263,\ 269 \qquad \text{et} \qquad 1741,\ 1747,\ 1753,\ 1759$$

forment des progressions arithmétiques de raison 6 composées chacune de quatre nombres premiers consécutifs. D'après $C_{1.4}$ (pour $n = 4$) il existe une infinité de telles progressions.

Nous déduirons maintenant de l'hypothèse H la conséquence suivante:

C_2. *a, b, c étant des nombres naturels tels que $(a, b) = (a, c) = (b, c) = 1$ et $2|abc$, l'équation $ap-bq = c$ a une infinité de solutions en nombres pre-*

miers p et q. (Cette hypothèse a été énoncée par Hardy et Littlewood [10], p. 45, Conjecture D).

Démonstration de l'implication $H \to C_2$. a, b, c étant des nombres naturels tels que $(a, b) = (a, c) = (b, c) = 1$ et $2|abc$, il existe, on le sait, des nombres naturels r et s tels que $ar - bs = c$. Soit $f_1(x) = bx + r$, $f_2(x) = ax + s$, on a donc $f_1(x)f_2(x) = abx^2 + (ar + bs)x + rs$.

S'il existait un nombre premier p tel que $p|f_1(x)f_2(x)$ pour tout entier x, on aurait (pour $x = 0$) $p|rs$, donc (pour $x = \pm 1$) $p|ab \pm (ar + bs)$, d'où $p|2ab$ et $p|2(ar + bs)$. Si l'on avait $p = 2$, on aurait, d'après $p|rs$, $2|r$ ou bien $2|s$. Si $2|r$, on ne peut avoir $2|s$, puisqu'alors il viendrait $2|ar \pm bs$, donc $2|ab$ et $2|c$, contrairement à $(ab, c) = 1$. Donc, si $2|r$, s est impair et de $p|ab + (ar + bs)$ il résulte que $2|(a+1)b$, donc ou bien a est impair ou bien b est pair. Si b était pair, alors, d'après $ar - bs = c$, c serait pair, contrairement à $(b, c) = 1$. Donc b est impair et a impair et aussi $c = ar - bs$ impair, contrairement à $2|abc$. Donc r ne peut pas être pair; s est donc pair et comme plus haut on démontre que cela implique une contradiction.

On a donc $p \neq 2$, par conséquent $p|ab$ et $p|ar + bs$ et, comme $p|rs$, d'après $p|ar^2 + brs$ on trouve $p|ar^2$, d'où $p|ar$ et, comme en vertu de $p|ars + bs^2$ on a $p|bs^2$, d'où $p|bs$, il vient $p|ar - bs = c$, ce qui est impossible, puisque $(ab, c) = 1$. Les binômes $f_1(x)$ et $f_2(x)$ satisfont donc à la condition S et il existe une infinité de nombres naturels x tels que $p = f_1(x)$ et $q = f_2(x)$ sont des nombres premiers, donc $bx + r = p$ et $ax + s = q$, ce qui donne $ap - bq = ar - bs = c$. L'implication $H \to C_2$ se trouve ainsi démontrée.

Voici maintenant une conséquence de C_2:

$C_{2.1}$. *Tout nombre rationnel positif peut être représenté d'une infinité de manières sous la forme $(p+1)/(q+1)$ ainsi que sous la forme $(p-1)/(q-1)$, où p et q sont des nombres premiers.*

Démonstration de l'implication $C_2 \to C_{2.1}$. Soit r un nombre rationnel > 1; on peut le représenter sous la forme $r = b/a$, où a et b sont des nombres naturels, $b > a$; $(a, b) = 1$ et il en résulte que $(a, b-a) = 1$ et on a évidemment $2|ab(b-a)$. D'après C_2 il existe donc une infinité de systèmes de deux nombres premiers p et q tels que $ap - bq = b - a$, d'où $b/a = (p+1)/(q+1)$.

Si r était rationnel, $0 < r < 1$, on aurait $r = a/b$ où $b > a$ et on trouverait $a/b = (q+1)/(p+1)$. Pour la forme $(p-1)/(q-1)$ la démonstration serait analogue, en partant de l'équation $ap - bq = a - b$ pour $a > b$. Pour $r = 1$ la proposition $C_{2.1}$ est évidente.

En particulier, pour $r = 2$ il résulte de $C_{2.1}$ qu'il existe une infinité de nombres premiers p pour lesquels le nombre $2p+1$, respectivement le nombre $2p-1$ est premier.

Si p et $2p+1$ sont premiers, on a $\varphi(2p+1) = 2p$, donc de $C_{2.1}$ résulte la proposition suivante:

$C_{2.1.1}$. *La suite $\frac{1}{2}\varphi(n)$ $(n = 1, 2, \ldots)$ contient une infinité de nombres premiers.*

Soit k un nombre naturel pair. D'après $C_{2.1}$ il existe une infinité de nombres premiers $p > k$ tels que $2p-1$ est un nombre premier. k étant pair, on a $k = 2l$. Or, pour tout l naturel on a $\varphi(4l) = 2\varphi(2l)$, donc $\varphi(4lp) = 2\varphi(l)\varphi(p) = 2(p-1)\varphi(l)$ et $\varphi[2l(2p-1)] = \varphi(2l)\varphi(2p-1) = (2p-2)\varphi(2l)$ donc $\varphi(4lp - 2l) = \varphi(4lp)$ et l'équation $\varphi(x+k) = \varphi(k)$ est remplie pour $x = 4lp - 2l$, $k = 2l$. On a ainsi la proposition suivante:

$C_{2.1.2}$. *L'équation $\varphi(x+k) = \varphi(x)$, où k est un nombre naturel pair, a une infinité de solutions.*

Pour k impairs l'étude de cette équation est beaucoup plus compliquée: voir A. Schinzel [16].

Il résulte tout de suite de $C_{2.1}$ qu'il existe pour tout nombre rationnel $r > 0$ une infinité de couples de nombres naturels x et y tels que $\sigma(x)/\sigma(y) = r$ (on peut prendre pour x et y des nombres premiers).

Une propriété analogue de la fonction φ peut aisément être démontrée sans faire appel à l'hypothèse H. En effet, si $r = l/m$, où l et m sont des nombres naturels et $(l, m) = 1$ et si k est un nombre naturel quelconque tel que $(k, lm) = 1$, on a

$$\varphi(l^2mk)/\varphi(lm^2k) = l/m = r.$$

Or, il résulte tout de suite de $C_{2.1}$ que, pour tout nombre rationnel $r > 0$, l'équation $\varphi(x)/\varphi(y) = r$ a une infinité de solutions en nombres premiers x et y.

P. Erdös a démontré d'une façon élémentaire l'existence des suites infinies m_k et n_k $(k = 1, 2, \ldots)$ de nombres naturels tels que $m_k/n_k \to +\infty$ et $\varphi(m_k) = \varphi(n_k)$ pour $k = 1, 2, \ldots$ Sa méthode n'est pas applicable à la fonction σ. Or, $C_{2.1}$ entraîne le corollaire suivant:

$C_{2.1.3}$. *Quel que soit le nombre naturel k, il existe des nombres naturels m et n tels que $\sigma(m) = \sigma(n)$ et $m/n > k$.*

Démonstration de l'implication $C_{2.1} \to C_{2.1.3}$. Comme on sait, il existe pour tout nombre naturel k un nombre naturel l tel que $\sigma(l)/l > 2k$ (ce qui résulte par exemple de l'inégalité

$$\frac{\sigma(n!)}{n!} \geqslant \frac{1}{1} + \frac{1}{2} + \ldots + \frac{1}{n} \qquad \text{pour} \qquad n = 1, 2, \ldots$$

et de la divergence de la série harmonique). Or, d'après $C_{2.1}$ (pour $r = \sigma(l)$) il existe des nombres premiers $p > l$ et $q > l$ tels que

$$\frac{\sigma(p)}{\sigma(q)} = \frac{p+1}{q+1} = \sigma(l).$$

Posons $m = p$, $n = lq$. On aura donc $\sigma(n) = \sigma(lq) = \sigma(l)\sigma(q) = \sigma(p) = \sigma(m)$ donc $\sigma(m) = \sigma(n)$, et

$$\frac{m}{n} = \frac{p}{lq} = \frac{p}{\sigma(p)} \cdot \frac{\sigma(q)}{q} \cdot \frac{\sigma(l)}{l} > \frac{p}{p+1} \cdot 2k > k, \quad \text{c. q. f. d.}$$

C_3. *Si a, b et c sont des entiers, $a > 0$, $(a, b, c) = 1$ et les nombres $a+b$ et c ne sont pas simultanément pairs, et b^2-4ac n'est pas un carré, il existe une infinité de nombres premiers de la forme ax^2+bx+c.* (Cf. Hardy et Littlewood [10], p. 48, Conjecture F).

Démonstration de l'implication $H \to C_3$. Comme b^2-4ac n'est pas un carré, le trinôme ax^2+bx+c est irréductible. Il remplit aussi la condition S, puisque

$$\big(f(0), f(1), f(2)\big) = (c, a+b+c, 4a+2b+c) = (c, a+b, 2a)$$
$$= (c, a+b, a) = (c, b, a) = 1.$$

L'implication $H \to C_2$ se trouve ainsi démontrée.

$C_{3.1}$. *Si k est un entier et $-k$ n'est pas un carré, il existe une infinité de nombres premiers de la forme x^2+k.* (Pour $k = 1$ cf. Hardy et Littlewood [10], p. 48, Conjecture E).

Pour déduire $C_{3.1}$ de C_3 il suffit de poser, dans C_3, $a = 1$, $b = 0$, $c = k$.

$C_{3.1.1}$. *Tout nombre naturel pair est d'une infinité de manières somme de deux nombres premiers conjugués du corps $K(\sqrt{-1})$.*

Démonstration de l'implication $C_{3.1} \to C_{3.1.1}$. Pour k naturel donné il existe, d'après $C_{3.1}$, une infinité de nombres premiers > 2 de la forme $p = x^2+k^2$; ces nombres sont, on le voit sans peine, de la forme $4t+1$, et on a $p = (k+xi)(k-xi)$ où $k+xi$ et $k-xi$ sont des nombres premiers conjugués du corps $K(\sqrt{-1})$, et $2k = (k+xi)+(k-xi)$.

Quant aux nombres impairs, on peut démontrer que tout nombre naturel impair < 29 est la somme de deux nombres premiers du corps $K(\sqrt{-1})$, mais il existe une infinité de nombres impairs qui ne sont pas de telles sommes, par exemple tous les nombres $170k+29$ et tous les nombres $130k+33$ où $k = 0, 1, 2, \ldots$

Il est à remarquer que sans avoir recours à l'hypothèse H nous ne savons pas démontrer non seulement qu'il existe une infinité de nombres premiers de la forme x^2+1, où x est un nombre naturel, mais aussi qu'il existe une infinité de nombres premiers de la forme x^2+y^2+1, où x et y sont des nombres naturels. Cependant on sait démontrer qu'il existe une

infinité de nombres premiers de la forme $x^2+y^2+z^2+1$, où x, y, z sont des nombres naturels: tels sont, par exemple, tous les nombres premiers de la forme $8k+7$.

C_4. *L'équation $ax^2+bx+c = dy$, où a, b, c, d sont des entiers, $a > 0$ et $d > 0$, a une infinité de solutions en nombres premiers x et y si et seulement si $\Delta = b^2-4ac$ n'est pas un carré (d'un nombre entier) et si elle a au moins une solution en nombres entiers x_0, y_0, tels que $(x_0y_0, 6ad) = 1$.*

Démonstration de l'implication $H \to C_4$. Nous prouverons sans avoir recours à l'hypothèse H que la condition est nécessaire.

Si l'équation $ax^2+bx+c = dy$ a une infinité de solutions en nombres premiers, il existe des nombres premiers x_0 et y_0 plus grands que $6ad$ et tels que $ax_0^2+bx_0+c = dy_0$ et alors on a $(x_0y_0, 6ad) = 1$.

Si Δ était un carré, soit $b^2-4ac = k^2$, où k est un entier $\geqslant 0$, on aurait, comme on le vérifie aisément $4ady_0 = (2ax_0+b+k)(2ax_0+b-k)$. Or, on déduit sans peine de cette égalité que pour x_0 premiers suffisamment grands le nombre y_0 ne peut pas être premier.

La condition de C_4 est donc nécessaire. Supposons maintenant que le nombre Δ ne soit pas un carré et que x_0 et y_0 soient des entiers tels que $ax_0^2+bx_0+c = dy_0$ et $(x_0y_0, 6ad) = 1$. Posons

$$f_1(x) = dx+x_0, \qquad f_2(x) = adx^2+(2ax_0+b)x+y_0.$$

Les polynômes f_1 et f_2 sont irréductibles, puisque

$$(2ax_0+b)^2-4ady_0 = (2ax_0+b)^2-4a(ax_0^2+bx_0+c) = b^2-4ac = \Delta$$

et, d'après l'hypothèse, Δ n'est pas un carré (d'un nombre rationnel).

S'il existait un nombre premier p tel que $p|f_1(x)f_2(x)$ pour x entiers, alors, en vertu du théorème de Lagrange, on aurait ou bien $p \leqslant 3$ ou bien $p|ad^2$, donc toujours $p|6ad^2$ et $p|f_1(0)f_2(0) = x_0y_0$ et, comme $(x_0y_0, 6ad) = 1$, d'où $(x_0y_0, 6ad^2) = 1$, on aurait $p|1$, ce qui est impossible. Les polynômes $f_1(x)$ et $f_2(x)$ satisfont donc aux conditions de l'hypothèse H, par conséquent pour une infinité de nombres naturels x les nombres $f_1(x) = p$ et $f_2(x) = q$ sont premiers et on vérifie sans peine que $ap^2+bp+c = dq$. L'implication $H \to C_4$ est ainsi démontrée.

$C_{4.1}$. *Tout nombre rationnel > 1 peut être représenté d'une infinité de manières sous la forme $(p^2-1)/(q-1)$, où p et q sont des nombres premiers.*

Démonstration de l'implication $C_4 \to C_{4.1}$. Soit r un nombre rationnel > 1, donc $r = d/a$, où a et d sont des nombres naturels, $d > a$. Posons, dans C_4, $b = 0$, $c = d-a$. On aura donc $b^2-4ac = -4a(d-a) < 0$, ce qui n'est pas un carré. Or, les nombres $x_0 = y_0 = 1$ sont tels que $(x_0y_0, 6ad) = 1$ et $ax_0^2+(d-a) = dy_0$. En vertu de C_4 il existe donc

une infinité de nombres premiers p et q tels que $ap^2+(d-a) = dq$, d'où $(p^2-1)/(q-1) = d/a = r$, ce qui prouve que $C_4 \to C_{4.1}$.

$C_{4.1.1}$. *Il existe une infinité de triangles orthogonaux de côtés naturels dont deux sont des nombres premiers.*

Démonstration de l'implication $C_{4.1} \to C_{4.1.1}$. Pour $r = 2$ il résulte de $C_{4.1}$ que l'équation $p^2 = 2q-1$ a une infinité de solutions en nombres premiers. Or, cette équation équivaut évidemment à l'équation $p^2+(q-1)^2 = q^2$. On a donc $C_{4.1} \to C_{4.1.1}$. Voici quelques triangles satisfaisant aux conditions de $C_{4.1.1}$:

$$(3, 4, 5),\ (5, 12, 13),\ (11, 60, 61),\ (19, 180, 181),\ (29, 240, 241),$$
$$(61, 1860, 1861).$$

Dans Scripta Mathematica 22 (1956), p. 158, Curiosum 435 (G. *An interesting Observation*) on trouve l'observation qu'il existe un grand nombre de cas où pour p premier l'addition de l'unité au nombre triangulaire d'ordre p, respectivement la soustraction du nombre 2 donne un nombre premier, par exemple $t_3+1 = 7$, $t_7+1 = 29$, $t_5-2 = 13$. Nous déduirons de l'hypothèse H les conséquences $C_{4.2}$ et $C_{4.3}$ suivantes:

$C_{4.2}$. *Il existe une infinité de nombres premiers p tels que $\frac{1}{2}p(p+1)+1$ est un nombre premier.*

Démonstration de l'implication $C_4 \to C_{4.2}$. Posons, dans C_4, $a = b = 1$, $c = d = 2$. Le nombre $b^2-4ac = -7$ n'est pas un carré. L'équation $x^2+x+2 = 2y$ admet la solution $x_0 = -1$, $y_0 = 1$ qui remplit la condition $(x_0y_0, 6ad) = 1$, et la proposition $C_{4.2}$ résulte immédiatement de C_4.

$C_{4.3}$. *Il existe une infinité de nombres premiers p tels que le nombre $\frac{1}{2}p(p+1)-2$ est premier.*

Démonstration de l'implication $C_4 \to C_{4.3}$. Posons, dans C_4, $a = b = 1$, $c = -4$, $d = 2$. Le nombre $b^2-4ac = 17$ n'est pas un carré. L'équation $x^2+x-4 = 2y$ admet la solution $x_0 = 1$, $y_0 = -1$, telle que $(x_0y_0, 6ad) = 1$, donc C_4 entraîne immédiatement $C_{4.3}$.

$C_{4.4}$. *La suite $\sigma(n)$ $(n = 1, 2, \ldots)$ contient une infinité de nombres premiers.*

Démonstration de l'implication $C_4 \to C_{4.4}$. Posons, dans C_4, $a = b = c = d = 1$. Le nombre $b^2-4ac = -3$ n'est pas un carré. L'équation $x^2+x+1 = y$ admet la solution $x_0 = -1$, $y_0 = 1$, où $(x_0y_0, 6ad) = 1$, et, comme pour p premiers on a $\sigma(p^2) = p^2+p+1$, C_4 entraîne la proposition $C_{4.4}$.

C_5. *Tout nombre naturel peut être représenté d'une infinité de manières sous la forme $\sigma(x)-\sigma(y)$ (où x et y sont des nombres naturels).*

Démonstration de l'implication $H \to C_5$. Si n est pair, il existe, d'après $C_{1.1}$, une infinité de nombres premiers p et q tels que $p-q = n$, d'où $\sigma(p)-\sigma(q) = (p+1)-(q+1) = n$. Or, si n est impair, posons, dans C_4, $a = b = d = 1$, $c = n$. Le nombre $b^2-4ac = 1-4n < 0$ n'est pas un carré. Si $3|n$, alors, n étant impair, on a $(n+2, 6) = 1$ et pour $x_0 = 1$, $y_0 = n+2$ on a $x_0^2+x+n = y_0$ et $(x_0y_0, 6ad) = (n+2, 6) = 1$. Si l'on n'a pas $3|n$, alors $(n, 6) = 1$ et pour $x_0 = -1$, $y_0 = n$ on trouve $x_0^2+x_0+n = y_0$ et $(x_0y_0, 6ad) = (-n, 6) = 1$. D'après C_4 il existe donc une infinité de nombres premiers p et q tels que $p^2+p+n = q$, d'où

$$\sigma(q)-\sigma(p^2) = q+1-(p^2+p+1) = q-p^2-p = n.$$

On a donc $H \to C_5$.

Il est à remarquer que pour la fonction φ la proposition analogue à C_5 est fausse, car on peut démontrer d'une façon élémentaire qu'aucun des nombres $2\cdot 7^n-1$ $(n = 1, 2, \ldots)$ n'est de la forme $\varphi(x)-\varphi(y)$, mais, comme pour p et q premiers on a $\varphi(p)-\varphi(q) = p-q$, on déduit de $C_{1.1}$ que tout nombre pair est de la forme $\varphi(x)-\varphi(y)$.

C_6. *n étant un nombre impair >1, k un entier donné quelconque qui n'est pas une puissance d'un entier à l'exposant $d>1$ et $d|n$, il existe une infinité de nombres premiers de la forme x^n+k, où x est un nombre naturel* (pour $n = 3$ cf. Hardy et Littlewood [10], p. 50, Conjecture K). *Si, en outre k est pair, il existe une infinité de nombres premiers p tels que p^n+k est un nombre premier.*

Démonstration de l'implication $H \to C_6$. n étant un nombre impair et k n'étant pas une puissance d'un entier à l'exposant $d>1$ et $d|n$, le polynôme $f(x) = x^n+k$ est irréductible. Or, on a $(f_1(0), f_1(1)) = (k, k+1) = 1$ et on déduit de H la première partie de C_6. Si k est pair, alors, en posant $f_2(x) = x$ on a $(f_1(-1)f_2(-1), f_1(1)f_2(1)) = (k-1, k+1) = 1$ la condition S est encore remplie et H entraîne la deuxième partie de C_6.

Il est à remarquer que sans l'aide de l'hypothèse H nous ne savons démontrer même pas l'existence d'une infinité de nombres premiers de la forme $x^3+y^3+z^3$, où x, y et z sont des entiers. On sait cependant démontrer (sans l'aide de l'hypothèse H) l'existence d'une infinité de nombres premiers de la forme $x^3+y^3+z^3+t^3$ où x, y, z, t sont des entiers: tels sont, par exemple, tous les nombres de la forme $9k\pm1$.

C_7. *Il existe une infinité de nombres naturels n tels que chacun des nombres n, $n+1$, $n+2$ est le produit de deux nombres premiers distincts.*

Démonstration de l'implication $H \to C_7$. Soit $f_1(x) = 10x+1$, $f_2(x) = 15x+2$, $f_3(x) = 6x+1$. On a ici $a = f_1(0)f_2(0)f_3(0) = 2$ et $b = f_1(1)f_2(1)f_3(1) = 11\cdot 17\cdot 7$, donc $(a, b) = 1$ et il résulte de H qu'il

existe une infinité de nombres naturels x tels que les nombres $p = 10x+1$, $q = 15x+2$, $r = 6x+1$ sont premiers. Pour $n = 3p$ on trouve $n+1 = 3p+1 = 2(15x+2) = 2q$, $n+2 = 2q+1 = 30x+5 = 5(6x+1) = 5r$ et $p \geqslant 11 > 3$, $q \geqslant 17 > 2$, $r \geqslant 7 > 5$, d'où il résulte que chacun des nombres n, $n+1$, $n+2$ est le produit de deux nombres distincts. De C_7 résulte tout de suite l'existence d'une infinité de nombres naturels n tels que les nombres n, $n+1$ et $n+2$ ont le même nombre de diviseurs.

Or, il n'existe pas quatre nombres naturels consécutifs dont chacun serait le produit de nombres premiers distincts, un de ces nombres étant toujours divisible par 4.

C_8. *Il existe pour tout nombre naturel s un nombre naturel m_s tel que chacune des équations $\varphi(x) = m_s$ et $\sigma(x) = m_s$ a plus de s solutions.* (Ce problème a été posé par P. Erdös).

Démonstration de l'implication $H \to C_8$. Posons $f_i(x) = 2^i x+1$ et $g_i(x) = 2^i x-1$ $(i = 0, 1, \ldots, 2s+1)$.

Comme $f_0(0)f_1(0)\ldots f_{2s+1}(0)g_0(0)\ldots g_{2s+1}(0) = 1$, les polynômes f_i et g_i $(i = 0, 1, 2, \ldots, 2s+1)$ satisfont à la condition S et d'après H, il existe un nombre naturel x tel que tous les nombres $f_i(x)$ et $g_i(x)$ pour $i = 0, 1, \ldots, 2s+1$ sont premiers. Posons

$$a_i = f_i(x)f_{2s-i+1}(x), \qquad b_i = g_i(x)g_{2s-i+1}(x) \qquad (i = 0, 1, \ldots, 2s+1)$$

$f_i(x)$ et $f_{2s-i+1}(x)$, respectivement $g_i(x)$ et $g_{2s-i+1}(x)$ étant (pour $i = 0, 1, \ldots, 2s+1$) des nombres premiers distincts, on a

$$\big(f_i(x), f_{2s-i+1}(x)\big) = 1 \quad \text{et} \quad \big(g_i(x), g_{2s-i+1}(x)\big) = 1 \quad \text{pour} \quad i = 1, 2, \ldots, 2s+1,$$

donc, pour $i = 0, 1, \ldots, 2s+1$:

$$\varphi(a_i) = \varphi\big(f_i(x)\big)\varphi\big(f_{2s-i+1}(x)\big) = 2^i x 2^{2s-i+1}x = 2^{2s+1}x^2,$$
$$\sigma(b_i) = \sigma\big(g_i(x)\big)\sigma\big(g_{2s-i+1}(x)\big) = 2^i x 2^{2s-i+1}x = 2^{2s+1}x^2.$$

Les nombres a_i $(i = 0, 1, \ldots, s)$ et de même les nombres b_i $(i = 0, 1, \ldots, s)$ étant distincts, l'implication $H \to C_8$ se trouve démontrée.

Il est à remarquer qu'une proposition analogue pour la fonction φ a été démontrée sans avoir recours à l'hypothèse H par P. Erdös ([7], p. 213) et que, selon son avis, une modification de sa démonstration permettrait de démontrer une proposition analogue pour la fonction σ. Or, une démonstration tout à fait élémentaire pour la fonction φ à été donnée par A. Schinzel [15].

Sans avoir recours à l'hypothèse H nous ne savons pas démontrer que l'équation $\varphi(x) = \sigma(y)$ a une infinité de solutions en nombres naturels x et y.

C_9. *Il existe une infinité de nombres premiers p pour lesquels le nombre 2^p-1 est composé.*

Démonstration de l'implication $H \to C_9$. Soit $f_1(x) = 4x-1$, $f_2(x) = 8x-1$. Il résulte de H qu'il existe une infinité de nombres naturels x pour lesquels les nombres $p = 4x-1$ et $q = 8x-1$ sont premiers. Mais alors on a $q-1 = 2p$ et, come on sait, $q|2^p-1$ et, si $x > 1$, on a $2^p-1 > q$ et le nombre 2^p-1 est composé. Il résulte donc de l'hypothèse H qu'il existe une infinité de nombres de Mersenne $M_p = 2^p-1$ composés dont les indices p sont des nombres premiers.

Un nombre naturel composé n est dit absolument pseudo-premier si pour tout entier a on a $n|a^n-a$.

C_{10}. *Il existe une infinité de nombres absolument pseudo-premiers.*

Démonstration de l'implication $H \to C_{10}$. Soit $f_1(x) = 6x+1$, $f_2(x) = 12x+1$, $f_3(x) = 18x+1$. Comme $f_1(0)f_2(0)f_3(0) = 1$, il résulte de H qu'il existe une infinité de nombres naturels x tels que chacun des nombres $p = 6x+1$, $q = 12x+1$, $q = 18x+1$ est premier et alors on le sait, le nombre pqr est absolument pseudo-premier (il est donc aussi un nombre de Carmichael) (voir [4], p. 271).

C_{11} (Hypothèse de E. Artin). *Tout nombre entier $g \neq -1$ qui n'est pas un carré est racine primitive pour une infinité de nombres premiers.*

Démonstration de l'implication $H \to C_{11}$. Soit $g = a^2b$, où a est un nombre naturel, b un entier qui n'est divisible par aucun carré > 1. Comme g n'est pas un carré, on a $b \neq 1$. Soit b_1 le plus grand diviseur impair de b.

Nous prouverons d'abord qu'il existe des binômes $f_1(x)$ et $f_2(x)$ satisfaisant à la condition S et tels que

1° *quel que soit le nombre naturel x, b est un non-résidu quadratique pour $f_1(x)$;*

2° $f_1(x)-1 = 2f_2(x)$ *si* $b \neq 3$ *et* $f_1(x)-1 = 4f_2(x)$ *si* $b = 3$.

Si $b < 0$, soit $f_1(x) = -4bx-1$, $f_2(x) = -2bx-1$. La condition 2° est évidemment remplie et, comme $f_1(0)f_2(0) = 1$, les binômes $f_1(x)$ et $f_2(x)$ satisfont à la condition S.

Si b est pair, on a $f_2(x) \equiv -1 \pmod 8$ et le symbole de Jacobi

$$\left(\frac{2}{f_1(x)}\right) = 1$$

et

$$\left(\frac{b}{f_1(x)}\right) = \left(\frac{-b_1}{f_1(x)}\right) = -\left(\frac{b_1}{f_1(x)}\right) = -(-1)^{(b_1-1)/2}\left(\frac{f_1(x)}{b_1}\right)$$

$$= -(-1)^{(b_1-1)/2}\left(\frac{-1}{b_1}\right) = -1,$$

ce qui prouve que b est un non-résidu quadratique pour $f_1(x)$, c'est-à-dire que la condition 1° est remplie. Si b est impair, on a $b = -b_1$ et on parvient au même résultat.

Si $b > 0$ et b est pair, on a $b = 2b_1$. Soit $f_1(x) = 4bx+2b-1$, $f_2(x) = 2bx+b-1$, $P(x) = f_1(x)f_2(x)$. On a $P(1)+P(-1)-2P(0) = 16b^2$, $P(0) = (2b-1)(b-1)$ et, b étant pair, on a $\big(P(1)+P(-1)-2P(0), P(0)\big) = 1$ et on en conclut que la condition S est remplie. La condition 2° est évidemment aussi remplie. Comme $b = 2b_1 = 2(2k+1)$, on trouve

$$f_1(x) \equiv 3 \pmod 8, \qquad \text{d'où} \qquad \left(\frac{2}{f_1(x)}\right) = -1$$

et

$$\left(\frac{b}{f_1(x)}\right) = \left(\frac{2}{f_1(x)}\right)\left(\frac{b_1}{f_1(x)}\right) = -\left(\frac{b_1}{f_1(x)}\right) = -(-1)^{(b_1-1)/2}\left(\frac{f_1(x)}{b_1}\right)$$
$$= -(-1)^{(b_1-1)/2}\left(\frac{-1}{b_1}\right) = -1,$$

ce qui prouve que b est un non-résidu quadratique pour $f_1(x)$ et la condition 1° est remplie.

Soit maintenant b un nombre impair > 3, donc $b = q_1 q_2 \dots q_k$, où q_i $(i = 1, 2, \dots, k)$ sont des nombres premiers, $q_1 < q_2 < \dots < q_k$ et $q_k > 3$. Le nombre premier q_k a donc au moins deux non-résidus quadratiques et l'un d'eux est $n_0 \not\equiv -1 \pmod{q_k}$. Le système des deux congruences $n \equiv -1 \pmod{4q_1 q_2 \dots q_{k-1}}$ et $n \equiv -n_0 \pmod{q_k}$ a évidemment une solution $n = n_1$. Soit

$$f_1(x) = 4bx+n_1, \qquad f_2(x) = 2bx+\tfrac{1}{2}(n_1-1), \qquad P(x) = f_1(x)f_2(x).$$

On trouve sans peine

$$P(0) = \tfrac{1}{2}n_1(n_1-1), \qquad P(1)+P(-1)-2P(0) = 16b^2.$$

Or, comme $n_1 \equiv -1 \pmod{4q_1 q_2 \dots q_{k-1}}$, d'où $\frac{1}{2}(n_1-1) \equiv -1 \pmod{2q_1 q_2 \dots q_{k-1}}$, et $n_1 \not\equiv 0 \pmod{q_k}$ (puisque $n_1 \equiv -n_0 \pmod{q_k}$ et n_0 est un non-résidu quadratique pour q_k) et $\frac{1}{2}(n_1-1) \not\equiv 0 \pmod{q_k}$ (puisque $n_1-1 \equiv -n_0 - 1 \not\equiv 0 \pmod{q_k}$), on a $(4b, n_1) = 1$ et $\big(2b, \frac{1}{2}(n_1-1)\big) = 1$, d'où $\big(16b^2, \frac{1}{2}n_1(n_1-1)\big) = 1$, donc $\big(P(0), P(1)+P(-1)-2P(0)\big) = 1$, d'où il résulte que les binômes $f_1(x)$ et $f_2(x)$ satisfont à la condition S. Or, la condition 2° est evidemment remplie. Or, on a $f_1(x) \equiv -1 \pmod{4q_1 q_2 \dots q_{k-1}}$ et $f_1(x) \equiv n_1 \pmod{q_k}$ d'où

$$\left(\frac{b}{f_1(x)}\right) = (-1)^{(b-1)/2}\left(\frac{f_1(x)}{b}\right) = \left(\frac{-f_1(x)}{b}\right) = \left(\frac{-n_1}{q_1 q_2 \dots q_{k-1}}\right)\left(\frac{-n_1}{q_k}\right)$$
$$= \left(\frac{1}{q_1 q_2 \dots q_{k-1}}\right)\left(\frac{n_0}{q_k}\right) = -1.$$

Le nombre b est donc un non-résidu quadratique pour $f(x)$ et la condition 1° est remplie.

Dans le cas $b = 3$ soit $f_1(x) = 12x+5$, $f_2(x) = 3x+1$. Ici on vérifie sans peine que les conditions S, 1° et 2° sont remplies.

Il résulte de l'hypothèse H qu'il existe une infinité de nombres naturels x tels que les nombres $f_1(x)$ et $f_2(x)$ sont tous les deux premiers. Soit x un de ces nombres, tel que $f_1(x) > g^4$. Si g appartenait modulo $f_1(x)$ à un exposant $< f_1(x)-1$, on aurait, d'après 2°, $f_1(x) | g^{(f_1(x)-1)/2}-1$ ou bien $f_1(x) | g^1-1$. Or, vu le théorème d'Euler relatif au symbole de Legendre, l'égalité $g = a^2 b$ et la condition 1°, on a

$$g^{(f_1(x)-1)/2} \equiv \left(\frac{g}{f_1(x)}\right) \equiv \left(\frac{b}{f_1(x)}\right) \equiv -1 \pmod{f_1(x)},$$

ce qui est incompatible avec $f_1(x) | g^{(f_1(x)-1)/2}-1$ (puisque $f_1(x)$ est impair). On a donc $f_2(x) | g^4-1$, ce qui est impossible vu que $f_1(x) > g^4 > 1$. g est donc une racine primitive pour le module $f_1(x)$. L'hypothèse de Artin est donc une conséquence de l'hypothèse H.

Nous étudierons maintenant la fonction

$$\varrho(x) = \overline{\lim_{y \to \infty}} [\pi(y+x)-\pi(y)].$$

(Cf. Hardy et Littlewood [10], p. 52-68).

On a $\varrho(1) = \varrho(2) = 1$, mais nous ne connaissons pas des valeurs $\varrho(x)$ pour aucun nombre naturel $x > 2$.

Il sera utile d'introduire la fonction auxiliaire

$$\bar{\varrho}(x) = \max_{0 < y \leqslant x!} [\varphi(x!, y+x)-\varphi(x!, y)]$$

où $\varphi(m, n)$ désigne le nombre de nombres naturels ne dépassant pas n et premiers avec m.

De la définition de la fonction $\bar{\varrho}(x)$ résultent les lemmes suivantes:

LEMME 1. $$\bar{\varrho}(x) = \max_{y, z = 1, 2, \dots} \{\min[z, \varphi(z!, y+x)-\varphi(z!, y)]\}$$
$$\geqslant \max_{y = 1, 2, \dots} \{\min[y, \pi(y+x)-\pi(y)]\} \geqslant \varrho(x).$$

LEMME 2. $\bar{\varrho}(x+1) \geqslant \bar{\varrho}(x)$.

LEMME 3. $\bar{\varrho}(x)+\bar{\varrho}(y) \geqslant \bar{\varrho}(x+y)$.

LEMME 4. $\bar{\varrho}(x) \leqslant \varphi(x)$.

Nous démontrerons maintenant:

THÉORÈME 1. $\bar{\varrho}(1) = \bar{\varrho}(2) = 1$, $\bar{\varrho}(3) = \varrho(4) = \bar{\varrho}(5) = \bar{\varrho}(6) = 2$, $\bar{\varrho}(7) = \bar{\varrho}(8) = 3$, $\bar{\varrho}(9) = \dots = \bar{\varrho}(12) = 4$, $\bar{\varrho}(13) = \dots = \bar{\varrho}(16) = 5$, $\bar{\varrho}(17) = \dots = \bar{\varrho}(20) = 6$, $\bar{\varrho}(21) = \dots = \bar{\varrho}(26) = 7$, $\bar{\varrho}(27) = \dots = \bar{\varrho}(30) = 8$, $\bar{\varrho}(31) = \bar{\varrho}(32) = 9$, $\bar{\varrho}(33) = \dots = \bar{\varrho}(36) = 10$.

Démonstration. D'après le lemme 4 on trouve $\bar{\varrho}(2) \leqslant 1$, $\bar{\varrho}(6) \leqslant 2$, $\bar{\varrho}(12) \leqslant 4$, $\bar{\varrho}(30) \leqslant 8$. En vertu du lemme 3 on a $\bar{\varrho}(8) \leqslant \bar{\varrho}(6)+\bar{\varrho}(2) \leqslant 3$, $\bar{\varrho}(32) \leqslant \bar{\varrho}(30)+\bar{\varrho}(2) \leqslant 9$, $\bar{\varrho}(36) \leqslant \bar{\varrho}(30)+\bar{\varrho}(6) \leqslant 10$. Enfin il est facile de démontrer que parmi 16 nombres naturels consécutifs quelconques il y a au plus 5 nombres qui ne sont divisibles par aucun des nombres 2, 3 et 5, parmi 20 nombres naturels consécutifs quelconques il y a au plus 6 tels nombres et parmi 26 nombres naturels consécutifs quelconques il y a au plus 7 nombres qui ne sont divisibles par aucun des nombres 2, 3, 5 et 7. Donc $\bar{\varrho}(16) \leqslant 5$, $\bar{\varrho}(20) \leqslant 6$, $\bar{\varrho}(26) \leqslant 7$. D'autre part on a $\pi(1+1)-\pi(1) = 1$, $\pi(3+2)-\pi(2) = 2$, $\pi(7+4)-\pi(4) = 3$, $\pi(9+4)-\pi(4) = 4$, $\pi(13+6)-\pi(6) = 5$, $\pi(17+6)-\pi(6) = 6$, $\pi(21+10)-\pi(10) = 7$, $\pi(27+10)-\pi(10) = 8$, $\pi(31+10)-\pi(10) = 9$, $\pi(33+10)-\pi(10) = 10$. Donc, en vertu du Lemme 1 on a $\bar{\varrho}(1) \geqslant 1$, $\bar{\varrho}(3) \geqslant 2$, $\bar{\varrho}(7) \geqslant 3$, $\bar{\varrho}(9) \geqslant 4$, $\bar{\varrho}(13) \geqslant 5$, $\bar{\varrho}(17) \geqslant 6$, $\bar{\varrho}(21) \geqslant 7$, $\bar{\varrho}(27) \geqslant 8$, $\bar{\varrho}(31) \geqslant 9$, $\bar{\varrho}(33) \geqslant 10$. La fonction $\bar{\varrho}(x)$ étant monotone (Lemme 2), notre théorème résulte sans peine des inégalités obtenues.

Appelons k-jumeaux (en allemand *k-linge*) k nombres premiers $k < q_1 < q_2 < \ldots < q_k$ tels que $\bar{\varrho}(q_k-q_1) = k-1$. Ainsi deux nombres premiers $q_1 > 2$ et q_2 seront 2-jumeaux si $\bar{\varrho}(q_2-q_1) = 1$, c'est-à-dire $q_2-q_1 = 2$. Les nombres premiers $q_1, q_2, q_3, \ldots$ tels que $3 < q_1 < q_2 < q_3$ et $\bar{\varrho}(q_3-q_1) = 2$ seront appelés 3-jumeaux etc.

Les données numériques concernant les nombres k-jumeaux ont été données

pour $k = 2$, $q_k \leqslant 10^6$ par G. H. Hardy et J. E. Littlewood ([10], p. 44),
pour $k = 3$, $q_k \leqslant 10^6$ par G. H. Hardy et J. E. Littlewood ([10], p. 63),
pour $k = 4$, $q_k \leqslant 10^6$ par G. H. Hardy et J. E. Littlewood ([10], p. 63),
pour $k = 4$, $10^6 < q_k \leqslant 2 \cdot 10^6$ par Ch. Sexton [17],
pour $k = 4$, $2 \cdot 10^6 < q_k \leqslant 3 \cdot 10^6$ par W. A. Goloubieff ([8], p. 153-157),
pour $k = 4$, $3 \cdot 10^6 < q_k \leqslant 5 \cdot 10^6$ par W. A. Goloubieff ([9], p. 82-87),
pour $k = 5$, $q_k \leqslant 2 \cdot 10^6$ par W. A. Goloubieff ([8], p. 153-157),
pour $k = 5$, $2 \cdot 10^6 < q_k \leqslant 5 \cdot 10^6$ par W. A. Goloubieff ([9], p. 82-87),
pour $k = 6$, $q_k \leqslant 14 \cdot 10^6$ par W. A. Goloubieff ([9], 82-87).

Le problème si pour tout k naturel il existe une infinité de nombres k-jumeaux équivaut, comme on le démontre sans peine, au problème si l'on a pour tout x, $\varrho(x) = \bar{\varrho}(x)$: l'hypothèse H résout donc ce problème positivement (voir plus loin C_{12}).

Théorème 2. $\bar{\varrho}(57) = \bar{\varrho}(58) = \bar{\varrho}(59) = \bar{\varrho}(60) = 15$.

Démonstration. L.Aubry a démontré (voir L. E. Dickson [6], p. 355) que parmi 30 nombres impairs consécutifs il y a au plus 15 nombres qui ne sont divisibles par aucun des nombres 3, 5 et 7. Il en résulte que $\bar{\varrho}(60) \leqslant 15$. D'autre part on a $\pi(57+16)-\pi(16) = 15$, donc $\bar{\varrho}(57) \geqslant 15$. Vu le lemme 2 on a donc $\bar{\varrho}(57) = \ldots = \bar{\varrho}(60) = 15$, c. q. f. d.

Théorème 3. *On a* $\bar{\varrho}(95) = \ldots = \bar{\varrho}(100) = 23$.

A. Schinzel a démontré (dans un article qui paraîtra ailleurs) que parmi 100 nombres naturels consécutifs quelconques il y a au plus 23 nombres qui ne sont divisibles par aucun nombre premier $\leqslant 17$, d'où résulte tout de suite que $\bar{\varrho}(100) \leqslant 23$. D'autre part on a $\varrho[23!, 4083966+95]-\varphi[23!, 4083966] = 23$, donc d'après le lemme 1: $\bar{\varrho}(95) \geqslant 23$.

La fonction $\bar{\varrho}(x)$ étant monotone on en obtient le théorème 3.

En vertu du lemme 1, le théorème 3 donne $\varrho(100) \leqslant 23$, ce qui est incompatible avec l'inégalité $\varrho(97) \geqslant 24$ qui a été déduite à la p. 67 du travail cité de Hardy et Littlewood [10] de leur hypothèse X. Or, cette déduction était fausse, car ces auteurs affirment qu'aucun des nombres premiers $\geqslant 17$ et $\leqslant 113$ ne donne le reste 8 mod 17, ce qui n'est pas vrai, puisque $59 \equiv 8 \pmod{17}$.

Théorème 4. *On a* $\bar{\varrho}(x) \leqslant \pi(x)$ *pour* $1 < x \leqslant 132$.

Démonstration. Vu le théorème 1 nous avons $\bar{\varrho}(2) = 1 = \pi(2)$, $\bar{\varrho}(6) = 2 = \pi(3)$, $\bar{\varrho}(8) = 3 < \pi(7)$, $\bar{\varrho}(12) = 4 = \pi(9)$, $\bar{\varrho}(16) = 5 < \pi(13)$, $\bar{\varrho}(20) = 6 < \pi(17)$, $\bar{\varrho}(26) = 7 < \pi(21)$, $\bar{\varrho}(30) = 8 < \pi(27)$, $\bar{\varrho}(32) = 9 < \pi(31)$, $\bar{\varrho}(36) = 10 < \pi(33)$, et, les fonctions $\bar{\varrho}(x)$ et $\pi(x)$ étant monotones, cela prouve le théorème 4 pour $1 < x \leqslant 36$.

Or, en vertu du lemme 3 on a

$$\bar{\varrho}(38) \leqslant \bar{\varrho}(30)+\bar{\varrho}(8) = 8+3 = 11 < \pi(37),$$

$$\bar{\varrho}(42) \leqslant \bar{\varrho}(30)+\bar{\varrho}(12) = 8+4 = 12 = \pi(39),$$

$$\bar{\varrho}(46) \leqslant \bar{\varrho}(30)+\bar{\varrho}(16) = 8+5 = 13 < \pi(43),$$

$$\bar{\varrho}(50) \leqslant \bar{\varrho}(30)+\bar{\varrho}(20) = 8+6 = 14 < \pi(47).$$

D'après le théorème 2 on a $\bar{\varrho}(60) = 15 = \pi(51)$. En vertu du lemme 3 on trouve

$$\bar{\varrho}(62) \leqslant \bar{\varrho}(60)+\bar{\varrho}(2) = 15+1 = 16 < \pi(61),$$

$$\bar{\varrho}(66) \leqslant \bar{\varrho}(60)+\bar{\varrho}(6) = 15+2 = 17 < \pi(63),$$

$$\bar{\varrho}(68) \leqslant \bar{\varrho}(60)+\bar{\varrho}(8) = 15+3 = 18 < \pi(67),$$

$$\bar{\varrho}(72) \leqslant \bar{\varrho}(60)+\bar{\varrho}(12) = 15+4 = 19 = \pi(69),$$

$$\bar{\varrho}(76) \leqslant \bar{\varrho}(60)+\bar{\varrho}(16) = 15+5 = 20 < \pi(73),$$

$$\bar{\varrho}(80) \leqslant \bar{\varrho}(60)+\bar{\varrho}(20) = 15+6 = 21 = \pi(77),$$

$$\bar{\varrho}(86) \leqslant \bar{\varrho}(60)+\bar{\varrho}(26) = 15+7 = 22 = \pi(81).$$

En vertu du théorème 3 on a $\bar{\varrho}(100) \leqslant 23 = \pi(87)$. En vertu du lemme 3 on trouve

$$\bar{\varrho}(102) \leqslant \bar{\varrho}(100)+\bar{\varrho}(2) = 23+1 = 24 < \pi(101),$$

$$\bar{\varrho}(106) \leqslant \bar{\varrho}(100)+\bar{\varrho}(6) = 23+2 = 25 < \pi(103),$$

$$\bar{\varrho}(108) \leqslant \bar{\varrho}(100)+\bar{\varrho}(8) = 23+3 = 26 < \pi(107),$$

$$\bar{\varrho}(112) \leqslant \bar{\varrho}(100)+\bar{\varrho}(12) = 23+4 = 27 < \pi(109),$$

$$\bar{\varrho}(116) \leqslant \bar{\varrho}(100)+\bar{\varrho}(16) = 23+5 = 28 < \pi(113),$$

$$\bar{\varrho}(120) \leqslant \bar{\varrho}(100)+\bar{\varrho}(20) = 23+6 = 29 < \pi(117),$$

$$\bar{\varrho}(126) \leqslant \bar{\varrho}(100)+\bar{\varrho}(26) = 23+7 = 30 < \pi(121),$$

$$\bar{\varrho}(130) \leqslant \bar{\varrho}(100)+\bar{\varrho}(30) = 23+8 = 31 < \pi(127),$$

$$\bar{\varrho}(132) \leqslant \bar{\varrho}(100)+\bar{\varrho}(32) = 23+9 = 32 = \pi(131).$$

Les fonctions $\bar{\varrho}(x)$ et $\pi(x)$ étant monotones, nous en concluons que le théorème 4 est vrai pour $1 < x \leqslant 132$.

COROLLAIRE 1. *$\varrho(x) \leqslant \pi(x)$ pour $1 < x \leqslant 132$.*

La démonstration résulte du lemme 1 et du théorème 4.

Hardy et Littlewood ont énoncé ([10], p. 54) l'hypothèse que $\varrho(x) \leqslant \pi(x)$ quel que soit le nombre $x > 1$.

COROLLAIRE 2. *Si $x > 1$, $y > 1$ et si l'un au moins des nombres x et y est $\leqslant 132$, on a*

$$\pi(x+y) \leqslant \pi(x)+\pi(y).$$

Démonstration. Sans nuire à la généralité nous pouvons supposer que $x < y$, $1 < x \leqslant 132$. En vertu du théorème 4 on a donc $\bar{\varrho}(x) \leqslant \pi(x)$. Or, en vertu du Lemme 1 on a, pour tout nombre y,

$$\min\bigl(y, \pi(x+y)-\pi(y)\bigr) \leqslant \pi(x).$$

Comme $y \geqslant x \geqslant \pi(x+y)-\pi(y)$, on a $\pi(x+y)-\pi(y) \leqslant \pi(x)$, c'est-à-dir $\pi(x+y) \leqslant \pi(x)+\pi(y)$, c. q. f. d.

Il est à remarquer que E. Landau [12] a démontré que pour x suffisamment grands on a $\pi(2x) < 2\pi(x)$.

Nous appliquerons maintenant l'hypothèse H à l'étude de la fonction $\varrho(x)$.

C_{12}. *$\varrho(x) = \bar{\varrho}(x)$ pour x naturels.*

Démonstration de $H \to C_{12}$. D'après le lemme 1 il suffit de prouver que $\varrho(x) \geqslant \bar{\varrho}(x)$. Dans ce but supposons que pour x naturel donné $s = \bar{\varrho}(x)$. D'après la définition de $\bar{\varrho}(x)$ il existe un entier y tel que $0 \leqslant y < x!$ et

que $s = \varphi(x!, y+x)-\varphi(x!, y)$. Évidemment on a $s \leqslant x$ et il existe s entiers croissants $a_1, a_2, \ldots, a_s$ où $0 \leqslant a_1 < a_s \leqslant x$ tels que $(y+a_i, x!) = 1$ pour $i = 1, 2, \ldots, s$.

Soit $f_i(\xi) = \xi+a_i$ pour $i = 1, 2, \ldots, s$,

$$P(\xi) = \prod_{i=1}^{s} f_i(\xi).$$

Si p est un nombre premier tel que $p|P(\xi)$ pour ξ entiers, on a, d'après le théorème de Lagrange, $p \leqslant s \leqslant x$, donc $p|x!$ et, d'après $(y+a_i, x!) = 1$, $(y+a_i, p) = 1$ pour $i = 1, 2, \ldots, s$, et comme $P(y) = \prod_{i=1}^{s}(y+a_i)$, cela donne $(P(y), p) = 1$, contrairement à $p|P(y)$.

La condition S est donc remplie et d'après H il existe une infinité de nombres naturels ξ tels que les nombres $\xi+a_i$ $(i = 1, 2, \ldots, s)$ sont tous premiers. Comme $0 \leqslant a_1 < a_s \leqslant x$, il en résulte que $\pi(\xi+x)-\pi(\xi) \geqslant s = \bar{\varrho}(x)$ pour une infinité de nombres naturels ξ et, vu la définition de la fonction $\varrho(x)$ cela donne $\varrho(x) \geqslant \bar{\varrho}(x)$. L'implication $H \to C_{12}$ se trouve ainsi démontrée.

$C_{12.1}$. $\varrho(1) = \varrho(2) = 1$, $\varrho(3) = \ldots = \varrho(6) = 2$, $\varrho(7) = \varrho(8) = 3$, $\varrho(9) = \ldots = \varrho(12) = 4$, $\varrho(13) = \ldots = \varrho(16) = 5$, $\varrho(17) = \ldots = \varrho(20) = 6$, $\varrho(21) = \ldots = \varrho(26) = 7$, $\varrho(27) = \ldots = \varrho(30) = 8$, $\varrho(31) = \varrho(32) = 9$, $\varrho(33) = \ldots = \varrho(36) = 10$, $\varrho(57) = \ldots = \varrho(60) = 15$, $\varrho(95) = \ldots = \varrho(100) = 23$.

$C_{12.1}$ est une conséquence immédiate de C_{12} et des théorèmes 1, 2 et 3.

$C_{12.2}$. *L'hypothèse de Hardy et Littlewood suivant laquelle $\varrho(x) \leqslant \pi(x)$ pour x naturels > 1 équivaut à l'inégalité*

$$(*) \qquad \pi(x+y) \leqslant \pi(x)+\pi(y) \quad \text{pour} \quad x > 1,\ y > 1.$$

Démonstration de $C_{12} \to C_{12.2}$. L'inégalité (*) entraîne tout de suite l'inégalité $\varrho(x) \leqslant \pi(x)$ (sans avoir recours à l'hypothèse H).

Supposons maintenant que $\varrho(x) \leqslant \pi(x)$ pour x naturels > 1 et soient x et y deux nombres naturels > 1. Sans diminuer la généralité du raisonnement nous pouvons supposer que $1 < x \leqslant y$. Comme $\varrho(x) \leqslant \pi(x)$, on a, d'après C_{12}, $\bar{\varrho}(x) \leqslant \pi(x)$, donc d'après le lemme 1, pour tout y, $\min\bigl(y, \pi(x+y)-\pi(x)\bigr) \leqslant \pi(x)$. Or, $y \geqslant x \geqslant \pi(x+y)-y$, donc $\pi(x+y)-\pi(y) \leqslant \pi(x)$, c'est-à-dire $\pi(x+y) \leqslant \pi(x)+\pi(y)$, c. q. f. d.

Il est intéressant qu'on ne puisse démontrer par le calcul ni la fausseté de l'hypothèse H ni celle de l'hypothèse de Hardy-Littlewood sur la fonction $\varrho(x)$. (Quant à cette dernière, si l'inégalité $\varrho(x) \geqslant 2$ avait lieu pour un x quelconque, on aurait $\varliminf_{k\to\infty}(p_{k+1}-p_k) < \infty$). Il est cependant possible qu'on puisse trouver des nombres x et y plus grands que 1 pour lesquels

$\pi(x+y) > \pi(x)+\pi(y)$, ce qui prouverait que l'hypothèse H et l'hypothèse de Hardy-Littlewood sur la fonction $\varrho(x)$ ne peuvent pas être simultanément vraies.

Hypothése H_1 de W. Sierpiński. *Si pour un nombre naturel $n>1$ les nombres $1, 2, 3, \ldots, n^2$ sont rangés succesivement en n lignes, n nombres dans chaque ligne, alors chaque ligne contient au moins un nombre premier.*

La proposition que la deuxième ligne contient au moins un nombre premier équivaut évidemment au théorème de Tchebycheff que pour n naturels >1 il existe entre n et $2n$ au moins un nombre premier.

La proposition que pour $n \geqslant 9$ chacune des 9 premières lignes contient au moins un nombre premier peut sans peine être déduite du théorème de R. Breusch [1] d'après lequel pour $x \geqslant 48$ il y a entre x et $\frac{9}{8}x$ au moins un nombre premier. Ensuite il est facile de déduire du théorème d'Hadamard-de la Vallée Poussin sur les nombres premiers que pour tout k et $n \geqslant n_0(k)$ chacune des k premières lignes contient au moins un nombre premier. On a ici $\lim\limits_{k\to\infty} n_0(k) = +\infty$ et le problème se pose si le plus grand nombre n pour lequel il n'existe aucun nombre premier entre $(k-1)n$ et kn tend vers $+\infty$ avec k.

Par la méthode de Brun on pourrait démontrer (voir G. Ricci [13]), que chacune des lignes de notre carré contient un nombre dont le nombre des diviseurs premiers est limité par une constante universelle.

Conséquence. *Entre deux carrés consécutifs il existe au moins deux nombres premiers distincts.*

En effet, pour démontrer cette implication, il suffit de remarquer que si n est un nombre naturel >1 les nombres naturels consécutifs $(n-1)^2, (n-1)^2+1, \ldots, n^2$ forment les deux dernières lignes dans notre carré composé des nombres $1, 2, \ldots, n^2$. En observant que dans tout intervalle fermé dont les extrémités sont les cubes de nombres naturels consécutifs, il y a au moins deux carrés distincts, on en déduit tout de suite qu'entre deux cubes de nombres naturels consécutifs il y a au moins deux nombres premiers. Cette proposition n'est pas encore démontrée sans avoir recours à l'hypothèse H_1, mais on a démontré que pour n naturels suffisamment grands il existe entre n^3 et $(n+1)^3$ au moins un nombre premier. (On ne sait pourtant pas si cela est vrai pour tout n naturel).

Remarquons que l'hypothèse H_1 pour les nombres n premiers résulte tout de suite de l'hypothèse suivante enoncée en 1932 par R. Haussner: entre deux multiples consécutifs d'un nombre premier p_i qui sont tous les deux inférieurs à p_{i+1}^2 il existe au moins un nombre premier (Haussner [11], p. 192). Pour $n = 7$, par exemple, il résulte de l'hypothèse de R. Haussner que non seulement chacune des 7 lignes de notre carré des nombres

$1, 2, \ldots, 49$, mais aussi les 10 lignes suivantes (dont la première contient sept nombres $50, 51, \ldots, 56$ et la dernière les nombres $113, 114, \ldots, 119$) contient chacune au moins un nombre premier. Il est intéressant de remarquer ici que la ligne suivante la 18-ème, formée des nombres $120, 121, \ldots, 126$, ne contient aucun nombre premier.

Hypothèse H_2 de A. Schinzel. *Si pour un nombre naturel n les nombres $1, 2, 3, \ldots, n^2$ sont rangés en n lignes, n nombres dans chaque ligne, alors, si $(k, n) = 1$, la k-ième colonne contient au moins un nombre premier.*

Nous ne savons pas quel sera le sort de nos hypothèses, cependant nous pensons que même si elles seront mises en défaut, cela ne sera pas sans profit pour la théorie des nombres.

Travaux cités

[1] R. Breusch, *Zur Verallgemeinerung des Bertrandschen Postulates, daß zwischen x und $2x$ stets Primzahlen liegen*, Math. Zeitschrift 34 (1932), p. 505-526.

[2] Moritz Cantor, *Ueber arithmetische Progressionen von Primzahlen*, Zeitschrift für Math. u. Phys. 6 (1861), p. 340-343.

[3] E. Catalan, *Propositions et questions diverses*, Bull. Soc. Math. France 16 (1888), p. 128-129.

[4] J. Chernick, *On Fermat's simple theorem*, Bull. of the Amer. Math. Soc. 45 (1945), p. 269-274.

[5] L. E. Dickson, *Theorems and tables on the sum of the divisors of a number*, Quarterly Journ. of Math. 44 (1913), p. 264-288.

[6] — *History of the Theory of Numbers*, I, New York 1952.

[7] P. Erdös, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function*, Quarterly Journ. of Math. 44 (1935), p. 205-213.

[8] W. A. Golubiew, *Abzählung von „Vierlingen" von 2000000 bis 3000000 und von „Fünflingen" von 0 bis 2000000*, Anzeiger der mat.-naturw. Klasse der Österreichischen Akademie der Wissenschaften 1956, p. 153-157.

[9] — *Abzählung von „Vierlingen" und „Fünflingen" bis zu 5000000 und von „Sechslingen" von 0 bis 14000000*, Anzeiger der math.-naturw. Klasse der Österreichischen Akademie der Wissenschaften, 1957, p. 82-87.

[10] G. H. Hardy and J. E. Littlewood, *Some problems of partitio numerorum III*, Acta Mathematica 44 (1923), p. 1-70.

[11] R. Haussner, *Über die Verteilung von Lücken- und Primzahlen*, Journ. für reine und angewandte Mathematik 168 (1932), p. 1192.

[12] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, T. 1, 1909, p. 215-216.

[13] G. Ricci, *Su la congettura di Goldbach e la costante di Schnirelman*, Annali della R. Scuola Normale Superiore di Pisa 6(2) (1937), p. 71-116.

[14] R. M. Robinson, *Factors of Fermat numbers*, Mathematical Tables and other Aids to Computation, vol. XI, 1957, p. 21-22.

[15] A. Schinzel, *Sur un problème concernant la fonction* φ, Tschekoslovak Math. Journ. 6 (1956), p. 164-165.

[16] — *Sur l'équation* $\varphi(x+k) = \varphi(k)$, Acta Arithmetica ce volume, p. 181-184.

[17] Ch. Sexton, *Abzählung von „Vierlingen" von* 1000000 *bis* 2000000, Anzeiger der math.-nat. Klasse der Österreichischen Akademie der Wissenschaften, 1955, p. 236-239.

[18] V. Thébault, *Sur les nombres premiers impairs*, C. R. Acad. Sci. Paris 218 (1944), p. 223.

Reçu par la Rédaction le 24. 6. 1957

On the Möbius function

by

S. Knapowski (Poznań)

1. Let $\mu(n)$ denote the Möbius function: $\mu(1) = 1$, $\mu(n) = (-1)^k$ if n is the product of k different primes, $\mu(n) = 0$ if n contains any factor to a power higher than the first. The well-known connection with the Riemann ζ-function is the following (see *e. g.* [2], p. 3, (1.1.4)):

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \qquad s = \sigma + it, \qquad \sigma > 1. \tag{1.1}$$

Write

$$M(x) = \sum_{n \leqslant x} \mu(n).$$

Here the most interesting question is that of the behaviour of $\max_{1 \leqslant x \leqslant T} |M(x)|$ as $T \to \infty$. This problem has been studied by many mathematicians. It is known at present that

$$M(x) = O\left(x \exp\left(-c_1 \sqrt{\log x}\right)\right) \text{ (1)}$$

and even slightly better estimates have been obtained.

It has been proved by Littlewood (see *e. g.* [1], p. 161) that the relation

$$M(x) = O(x^{1/2+\varepsilon}) \quad \text{for every} \quad \varepsilon > 0$$

is equivalent to the truth of the Riemann hypothesis.

Some conjectures, in connection with the subject, should be noted. The Mertens hypothesis

$$|M(n)| < \sqrt{n} \quad \text{for} \quad n > 1 \tag{1.2}$$

has not been proved or disproved yet (see [2], p. 320). Also slightly less drastic conjectures:

$$M(x) = O(x^{1/2}) \tag{1.3}$$

(1) See *e. g.* [1], p. 157, Theorem 478. Throughout this paper $c_1, c_2, \ldots$ denote numerical positive constants.