Mathematics. — *Sur l'hypothèse de* GOLDBACH. Par J. G. VAN DER CORPUT.

(Communicated at the meeting of January 29, 1938.)

Dans une lettre adressée à EULER et datée le 7 juin 1742 GOLDBACH a énoncé l'hypothèse que tout nombre pair supérieur à 2 est la somme de deux nombres premiers, par exemple $10 = 3 + 7$. Nombre de mathématiciens ingénieux ont essayé de démontrer ou de réfuter cette hypothèse, mais jusqu'à présent en vain. Si l'hypothèse de GOLDBACH est vraie, tout nombre impair w supérieur à 5 est la somme de trois nombres premiers; en effet $w - 3$ est alors pair et supérieur à 2, donc, d'après l'hypothèse, égal à la somme de deux nombres premiers, d'où il suit que le nombre w lui-même est la somme de trois nombres premiers. Cette dernière hypothèse, qui est appelée l'hypothèse de GOLDBACH pour les nombres impairs, a été démontrée en mai 1937 par M. I. M. VINOGRADOW, il est vrai avec une certaine restriction. Cette restriction n'est pas d'ailleurs essentielle. Il a démontré que tout nombre impair suffisamment grand est la somme de trois nombres premiers.

La méthode créée par lui fournit beaucoup de résultats remarquables. Qu'il me soit permis de traiter ici quelques-uns de ces résultats.

Presque tout nombre positif pair est la somme de deux nombres premiers, c'est-à-dire, ε désignant un nombre positif quelconque, le nombre des exceptions $\leqq N$ est inférieur à εN, si N est suffisamment grand. Il existe même une constante absolue c_1 telle que pour tout nombre $N \geqq 3$ le nombre des exceptions $\leqq N$ soit inférieur à $\frac{c_1 N}{(\log N)^{1000}}$ [1]). Il est donc encore possible qu'il y a une infinité d'exceptions, mais en tout cas ces exceptions sont clairsemées dans la suite des nombres positifs pairs.

Comme on peut vérifier par l'expérience, les nombres 4996, 4998 et 5000 peuvent être écrits respectivement de 124, 288 et 150 manières différentes comme la somme de deux nombres premiers. Si $F(t)$ désigne le nombre de manières différentes dont on peut écrire t comme la somme de deux nombres premiers, on a donc

$$F(4996) = 124; \quad F(4998) = 288; \quad F(5000) = 150 \quad . \quad . \quad . \quad (1)$$

Ce résultat nous montre que l'ordre de grandeur de $F(t)$ ne dépend pas seulement de l'ordre de grandeur de t; il dépend aussi du caractère arithmétique de t. D'une manière plus précise: l'expérience nous apprend (mais naturellement pas avec une certitude mathématique) que $F(t)$ possède pour

---

[1]) On peut remplacer l'exposant 1000 par un nombre quelconque m, mais alors le nombre c, figurant dans la formule, désigne un nombre convenablement choisi, dépendant de m.

tout nombre positif pair une valeur approximative qui est égale à un produit $\Omega(t)\Phi(t)$, où $\Omega(t)$ dépend du caractère arithmétique de t, et $\Phi(t)$ de l'ordre de grandeur de t;

$$\Phi(t) = \int_2^{t-2} \frac{du}{\log u \log (t-u)}$$

et

$$\Omega(t) = K \prod_{\substack{p|t \\ p>2}} \frac{p-1}{p-2},$$

où le produit est étendu à tous les facteurs premiers impairs de t, tandis que K est la constante absolue

$$K = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right),$$

le produit étant étendu à tous les nombres premiers impairs.

Si l'hypothèse que $\Omega(t)\Phi(t)$ est une valeur approximative de $F(t)$ est vraie, on a pour deux nombres pairs t qui sont à peu près égaux que les nombres $F(t)$ sont approximativement proportionnels à $\Omega(t)$; donc

$F(4996) = F(2^2 . 1249)$; $F(4998) = F(2 . 3 . 7^2 . 17)$ et $F(5000) = F(2^3 5^4)$

seraient approximativement proportionnels à

$$\frac{1248}{1247}, \quad \frac{2}{1} \cdot \frac{6}{5} \cdot \frac{16}{15} \quad \text{et} \quad \frac{4}{3},$$

ce qui concorde très bien avec (1).

Il est vrai que nous ne sommes pas encore persuadés avec une certitude mathématique de la vérité de l'hypothèse que $\Omega(t)\Phi(t)$ est pour tout nombre positif pair une valeur approximative de $F(t)$, mais maintenant nous savons du moins que cette hypothèse est vraie pour presque tout nombre positif pair. Dit plus précisément: pour tout $N \geqq 3$ le nombre des nombres positifs pairs $t \leqq N$ qui ne satisfont pas à l'inégalité

$$\left| \frac{F(t)}{\Omega(t)\Phi(t)} - 1 \right| < \frac{1}{(\log N)^{1000}}$$

est inférieur à $\dfrac{c_2 N}{(\log N)^{1000}}$, où c_2 désigne une constante absolue [1]).

La méthode peut être appliquée non seulement à la somme, mais aussi à la différence de deux nombres premiers. Presque tout nombre pair est la différence de deux nombres premiers; pour toute valeur $\geqq 3$ de N le nombre des exceptions situées entre $-N$ et N est inférieur à $\dfrac{c_3 N}{(\log N)^{1000}}$ où c_3 désigne une constante absolue [1]).

Si $F(t, N)$ désigne le nombre de manières différentes dont il est possible d'écrire t comme la différence de deux nombres premiers $\leqq N$, l'expérience

---

[1]) Voir la note à la première page de cet article.

donne une grande plausibilité à l'hypothèse que $F(t, N)$ possède pour toute valeur paire $\neq 0$ de t et pour toute valeur $\geqq 3$ de N la valeur approximative

$$\Omega(t) \iint \frac{du\,dv}{\log u \log v}, \quad \ldots \ldots \ldots \quad (2)$$

où l'intégrale double est étendue à l'ensemble des points du carré $2 \leqq u \leqq N$, $2 \leqq v \leqq N$ pour lesquels on a $|u - v - t| \leqq \frac{1}{2}$. Par exemple le nombre de manières dont on peut écrire 2 comme la différence de deux nombres premiers $\leqq 10^6$ est égal à 8164, tandis que l'expression (2) est pour $t = 2$ et $N = 10^6$ à peu près égale à 8200. Nous ne savons pas encore si l'expression (2) fournit toujours une valeur approximative de $F(t, N)$, mais en tout cas elle donne presque toujours une telle valeur.

Plus généralement nous nous demandons maintenant quels nombres w possèdent la forme $ap + bq$ où p et q désignent des nombres premiers impairs, a et b des nombres entiers donnés non-nuls. Il est évident que seules les valeurs de w entrent en considération qui ont la même parité que $a + b$, c'est-à-dire qui sont paires ou impaires selon que $a + b$ est pair ou impair. Inversement, si les coefficients donnés a et b sont premiers entre eux et ne sont pas tous les deux négatifs, presque tout nombre positif de la même parité que $a + b$, possède la susdite forme $ap + bq$. Par exemple: presque tout nombre positif impair est le double d'un nombre premier, augmenté d'un nombre premier; presque tout nombre positif pair est un nombre premier, augmenté du triple d'un nombre premier.

On peut encore imposer aux nombres premiers p et q la condition, qu'ils appartiennent à des progressions arithmétiques données. Si p est un multiple de 10, augmenté de 1 et si q est un multiple de 10, augmenté de 7, le nombre $2p + 3q$ est un multiple de 10, augmenté de $2.1 + 3.7 - 20 = 3$. La méthode, dont il est question ici, nous apprend que presque tout nombre positif qui est égal à un multiple de 10, augmenté de 3, possède la forme $2p + 3q$, où p et q désignent des nombres premiers qui sont égaux à un multiple de 10, augmenté respectivement de 1 et de 7.

Il est remarquable que la méthode peut être appliquée non seulement à des problèmes linéaires, mais aussi à des problèmes quadratiques. Considérons l'expression $ap^2 + bq^2 + cr^2 + ds^2$, où p, q, r et s désignent des nombres premiers > 3. Supposons que les coefficients a, b, c et d soient des entiers donnés non-nuls tels qu'un nombre premier quelconque figure comme facteur dans deux de ces quatre coefficients tout au plus. Il est évident que tout nombre w possédant la susdite forme est égal à un multiple de 24, augmenté de $a + b + c + d$. Inversement presque tout nombre naturel qui est égal à un multiple de 24, augmenté de $a + b + c + d$ peut être mis sous la forme en question. Par conséquent presque tout nombre naturel qui est égal à un multiple de 24, augmenté de 4, est la somme des carrés de quatre nombres premiers.

D'une manière analogue on peut traiter la forme intermédiaire

$ap + bq^2 + cr^2$. Considérons le cas spécial $a = b = c = 1$: tout nombre qui est égal à un nombre premier > 3, augmenté de la somme des carrés de deux nombres premiers > 3, est nécessairement un multiple de 6, augmenté de 1 ou 3. Le développement des mathématiques pendant les derniers mois nous apprend inversement que presque tout nombre naturel qui est un multiple de 6, augmenté de 1 ou 3, est égal à un nombre premier, augmenté de la somme des carrés de deux nombres premiers.

Les propositions précitées ont le désavantage qu'elles contiennent une restriction essentielle, exprimée par le mot „presque", mais elles nous permettent de déduire des autres propositions qui ne possèdent pas cet inconvénient. Soit par exemple w un nombre impair > 3. Il y a plus de $\frac{w}{5 \log w}$ nombres premiers impairs $p < w$, donc plus de $\frac{w}{5 \log w}$ nombres positifs pairs de la forme $w - p$. Presque tous ces nombres sont égaux à la somme de deux nombres premiers, c'est-à-dire, le nombre des exceptions est inférieur à $\frac{c_4 w}{(\log w)^2}$ où c_4 désigne une constante absolue convenablement choisie. Par conséquent le nombre des nombres de la forme $w - p$ qui peuvent être écrits comme la somme de deux nombres premiers est égal à $\frac{w}{5 \log w} - \frac{c_4 w}{(\log w)^2}$, donc positif, si $\log w$ est supérieur à $5 c_4$. Ainsi nous trouvons le théorème de M. I. M. VINOGRADOW que tout nombre impair suffisamment grand est la somme de trois nombres premiers.

On obtient un résultat encore plus remarquable dans le problème suivant. Considérons un nombre impair non-nul quelconque w et un nombre $N \geqq 3$. Il y a plus de $\frac{N}{5 \log N}$ nombres premiers impairs $\leqq N$, donc plus de $\frac{N}{5 \log N} - |w|$ nombres positifs pairs de la forme $w + p$, où p parcourt les nombres premiers impairs $\leqq N$. Presque tous ces nombres $w + p$ sont la somme de deux nombres premiers; le nombre des exceptions est inférieur à $\frac{c_5 N}{(\log N)^2}$ où c_5 désigne un nombre dépendant uniquement de w. Par conséquent il y a plus de

$$\frac{N}{5 \log N} - |w| - \frac{c_5 N}{(\log N)^2}$$

manières différentes, dont on peut écrire w comme la somme de deux nombres premiers, diminuée d'un nombre premier. La borne inférieure, trouvée pour le nombre de manières en question, croît indéfiniment avec N, d'où il suit: tout nombre impair peut être écrit, même d'une infinité de manières, comme la somme de deux nombres premiers, diminuée d'un nombre premier.

Des résultats trouvés par un raisonnement analogue je ne mentionne ici que les suivants:

Tout nombre suffisamment grand qui est égal à un multiple de 24, augmenté de 5, est la somme des carrés de cinq nombres premiers.

Tout nombre qui est égal à un multiple de 24, augmenté de 3, peut être écrit, même d'une infinité de manières, comme la somme des carrés de quatre nombres premiers, diminuée du carré d'un nombre premier.

Tout nombre pair suffisamment grand est la somme de deux nombres premiers, augmentée de la somme des carrés de deux nombres premiers.

Tout nombre pair peut être écrit, même d'une infinité de fois, comme la somme de deux nombres premiers, diminuée de la somme des carrés de deux nombres premiers.

Tout nombre impair suffisamment grand est la somme de deux nombres premiers, augmentée de la dixième puissance d'un nombre premier (au lieu de dix on peut choisir tout exposant positif et entier).

Tout nombre impair peut être écrit, même d'une infinité de manières, comme la différence de deux nombres premiers, augmentée de la dixième puissance d'un nombre premier.

Finissons par le problème suivant, dans lequel nous supposons que les coefficients a, b et c soient entiers et non-nuls tels que a soit premier avec b et avec c et que b soit premier avec c. Nous nous demandons quels nombres w possèdent la forme

$$w = ap + bq + cr,$$

où p, q et r désignent des nombres premiers, appartenant à des progressions arithmétiques données. Supposons que ces progressions arithmétiques aient la même différence et que cette différence soit un nombre naturel pair U. Désignons les termes initials des progressions arithmétiques contenant p, q et r respectivement par P, Q et R; donc p est un multiple de U, augmenté de P, etc. Nous supposons naturellement que la différence U soit première avec chacun de ces trois termes initials.

Il est évident que seuls les nombres w qui sont égaux à un multiple de U, augmenté de $aP + bQ + cR$ entrent en considération. Pour la formulation de la proposition inverse nous distinguerons trois cas:

1. Si les coefficients a, b et c sont tous les trois positifs, tout nombre w suffisamment grand qui est égal à un multiple de U, augmenté de $aP + bQ + cR$, possède la susdite forme, où p, q et r désignent des nombres premiers, appartenant aux progressions arithmétiques précitées.

2. Si les coefficients a, b et c sont tous les trois négatifs, tout nombre négatif w dont la valeur absolue est suffisamment grande et qui est égal à un multiple de U, augmenté de $aP + bQ + cR$, possède la susdite forme.

3. Si les trois coefficients a, b et c ne possèdent pas le même signe, tout nombre qui est égal à un multiple de U, augmenté de $aP + bQ + cR$, peut être écrit, même d'une infinité de manières différentes, sous la susdite forme.

Par exemple chaque multiple de 10 peut être écrit d'une infinité de manières sous la forme $p + 2q - 3r$, où p, q et r désignent des nombres premiers, qui sont tous les trois égaux à un multiple de 10, augmenté de 1.