ZAM. 407. — DRUKARNIA UNIWERSYTETU I POLITECHNIKI WE WROCŁAWIU — F. 17279

COLLOQUIUM MATHEMATICUM

VOL. I WROCŁAW 1948 FASC. 3

COMMUNICATIONS

REMARQUE SUR LA RÉPARTITION DES NOMBRES PREMIERS

PAR

W. SIERPIŃSKI (VARSOVIE)

Il est bien connu que, dans la suite de tous les nombres naturels, il y a des intervalles aussi longs que l'on veut ne contenant aucun nombre premier. En effet, aucun des $n-1$ nombres consécutifs

$$n!+2, \quad n!+3, \quad \ldots, \quad n!+n$$

n'est premier pour aucun nombre naturel $n>1$.

Je vais démontrer ici la propriété suivante da la répartition des nombres premiers:

Il y a des nombres premiers isolés de deux côtés par des intervalles aussi longs que l'on veut.

Plus précisément, je vais établir ce

Théorème. Il existe pour tout nombre naturel n un nombre premier $p>n$ tel qu'aucun des nombres $p\pm j$ où $j=1,2,\ldots,n$ n'est premier.

Démonstration. Étant donné un n naturel, il existe — comme on sait — un nombre premier $q>n+1$. Le nombre

$$a=\sum_{j=1}^{q-2}(q^2-j^2) \tag{1}$$

est évidemment naturel. Comme le nombre $(q-2)!$ est premier relativement au nombre premier q, on conclut sans peine de (1) que les nombres a et q sont premiers entre eux.

D'après le théorème de Lejeune-Dirichlet sur la progression arithmétique, il existe un nombre premier

$$p>q \tag{2}$$

de la forme $ak+q$, où k est un entier. La formule $p=ak+q$ donne

$$p\pm j=ak+q\pm j. \tag{3}$$

Pour $j=1,2,\ldots,n$, on a $j<q-1$. Le nombre $q\pm j$ est d'après (1) diviseur du nombre a et on a $q\pm j>1$; par conséquent, $q\pm j$ est d'après (3) aussi diviseur du nombre $p\pm j$ et on a $q\pm j<p\pm j$ en vertu de (2). Ainsi le nombre $p\pm j$, où $j=1,2,\ldots,n$, n'est pas premier, c. q. f. d.

Corollaire. Il existe une infinité des nombres premiers qui n'appartiennent à aucun couple de nombres jumeaux.

Tels sont, en effet, tous les nombres premiers p pour lesquels les nombres $p\pm 1$ et $p\pm 2$ ne sont pas premiers [1]).

Remarques. La démonstration du théorème, dont l'énoncé est fort simple, faisant intervenir le théorème sur la progression arithmétique, il serait peut-être intéressant d'en trouver une démonstration élémentaire.

Je ne connais non plus aucune démonstration élémentaire du corollaire [2]).

Jelenia Góra, septembre 1947.

[1]) Par exemple: tous les nombres premiers de la forme $15k+7$ où $k=1,2,\ldots$

[2]) Pour une démonstration par les méthodes de la théorie analytique des nombres et qui est d'ailleurs assez facile, cf. par exemple la communication de E. Ullrich, *Zum Zwillingssatz von Viggo Brun*, Bericht über die Mathematiker-Tagung in Tübingen 23-27 September 1946, p. 139-143.

UN THÉORÈME SUR LES NOMBRES $\cos 2\pi k/n$

PAR

A. MOSTOWSKI (VARSOVIE)

M. Lehmer et récemment MM. Hamming et Olmsted [1]) ont envisagé le caractère algébrique des nombres $\cos 2\pi k/n$. Je prouverai ici le théorème suivant, se rattachant aux mêmes nombres.

Théorème. Lorsque $(k,n)=1$, *le nombre* $\cos 2\pi k/n$ *s'exprime par des radicaux réels si et seulement si* $\varphi(n)$ *est une puissance de 2, c'est-à-dire si* $n=2^{\alpha}\cdot p_1\cdot p_2\cdot\ldots\cdot p_k$, *les nombres* $p_1,p_2,\ldots,p_k$ *étant premiers de la forme* $2^{\beta}+1$ *et qui diffèrent deux à deux.*

Démonstration. Le nombre $2\cos 2\pi k/n$ satisfait à une équation irréductible du degré $\varphi(n)/2$ [2]). Donc, si $\varphi(n)/2$ est divisible par un nombre impair, $2\cos 2\pi k/n$ ne s'exprime pas par des radicaux réels [3]).

Pour établir l'implication inverse, admettons que $\varphi(n)$ est une puissance de 2. Les n-ièmes racines de 1 s'expriment alors par des radicaux carrés, donc sous la forme $a+bi$, où a et b s'obtiennent des nombres rationnels par des opérations rationnelles et par des radicaux carrés portant sur des quantités réelles [4]). Le nombre $\cos 2\pi k/n$ étant la partie réelle d'une n-ième racine de l'unité, le théorème se trouve démontré.

Corollaire. Si $\cos 2\pi k/n$ *s'exprime par des radicaux réels il s'exprime aussi par des radicaux carrés, de sorte que l'angle* $2\pi k/n$ *est constructible à l'aide d'un compas et d'une règle.*

[1]) D. H. Lehmer, American Mathematical Monthly 40 (1933), p. 165-166; R. W. Hamming, ibidem 52 (1945), p. 336-337; J. M. H. Olmsted, ibidem, p. 507-508.

[2]) Lehmer, loco cit., p. 165.

[3]) N. G. Tschebotarev, *Tieoria Galois* (en russe), 1936, p. 65.

[4]) Tschebotarev, op. cit., p. 66.