

Transcription de deux extraits des Comptes-Rendus de l'Académie des Sciences, de la série de Mathématiques (série A), 87, n° 1, de juillet 1878

[p. 374]

Mémoires présentés¹.

M. F. PROTH adresse l'énoncé du théorème suivant, relatif à la théorie des nombres : "Si le nombre $2^k + 1$ est premier, il divise la quantité $3^{2^{k-1}} + 1$. Si le nombre $2^k + 1$ est composé, il ne divise pas la quantité $3^{2^{k-1}} + 1$ (k est égal à 2^n)".

(Commissaires : MM. Hermite, Bouquet).

[p. 926]

ANALYSE. *Théorèmes sur les nombres premiers.* Note de M. E.² PROTH³.

I. Le nombre N est un nombre premier, si $a^x - 1$ est divisible par N , pour x égal à $\frac{N-1}{2}$, et non pour toute autre valeur de x , diviseur de $\frac{N-1}{2}$.

II. Le nombre N est un nombre premier, si $a^x - 1$ est divisible par N , pour x égal à $N-1$, et si $a^x - 1$ est premier avec N , pour toute valeur de x , diviseur de $N-1$, moindre que $\sqrt[2]{N}$ (caractéristique).⁴

III. Soit donné le nombre $N = m2^k$, où m est impair et $2^k > m$. Soit a non résidu de N . Cela posé, le nombre N est premier, si $a^{\frac{N-1}{2}} + 1$ divisible par N . N est composé dans le cas contraire.

IV. Soit donné $N = mP + 1$, où m est un entier quelconque et P un nombre premier plus grand que $\frac{1}{2}\sqrt[2]{N}$. Cela posé, le nombre N est premier, si $a^{N-1} - 1$ est divisible par N , sans que $a^m \pm 1$ le soit.

Remarque. Dans ce qui précède, nous supposons toujours a et N premiers entre eux, et $a < N$.

À l'aide des théorèmes précédents et de quelques autres, nous avons trouvé la solution générale du problème suivant : *Vérifier rapidement si un nombre quelconque est premier ou non*, et même trouvé les diviseurs de certaines classes de nombres.

Transcription en L^AT_EX : Denise Vella-Chemla, février 2026.

1. Référence : <https://gallica.bnf.fr/ark:/12148/bpt6k3044x/f406.item>.

2. Note de la transcriptrice : erreur sur l'initiale, les prénoms de Proth sont François Toussaint.

3. Référence : <https://gallica.bnf.fr/ark:/12148/bpt6k3044x/f1011.item>.

4. ajouté par la transcriptrice : Carl Friedrich Gauss, *Disquisitiones arithmeticae*, 1801.