NOUVELLES ANNALES DE MATHÉMATIQUES

ÉDOUARD LUCAS

Sur la décomposition des nombres en facteurs premiers

Nouvelles annales de mathématiques 2^e série, tome 14 (1875), p. 523-525

<http://www.numdam.org/item?id=NAM_1875_2_14__523_1>

SUR LA DÉCOMPOSITION DES NOMBRES EN FACTEURS PREMIERS;

PAR M. ÉDOUARD LUCAS.

Les opérations que l'on effectue habituellement pour décomposer un nombre en ses facteurs premiers sont longues et pénibles, puisque l'on est obligé de faire

exactement les divisions de ce nombre, souvent très-grand, par une série de diviseurs que l'on essaye successivement. On peut, à l'aide de la remarque suivante, abréger le calcul d'une manière notable. Considérons, par exemple, le nombre

$$\frac{2^{40}+1}{2^{8}+1} = 4278255361,$$

dont tous les diviseurs sont de la forme $80p+1$. Prenons les logarithmes des nombres de cette forme, compris entre 60 000 et 62 000, et retranchons-les du logarithme du nombre donné; nous pouvons déterminer exactement les cinq chiffres du quotient et former le tableau suivant :

Diviseurs.	631 2667		Quotients.
60 161	779 3150	851 9517	71 112
60 961	785 0521	846 2146	70 180
61 121	786 1905	845 0762	69 996
61 441	788 4583	842 8084	69 632
61 681	790 1514	841 1153	69 361

On rejettera d'abord tous les quotients non terminés par l'unité; puis, parmi ceux qui font exception, on rejettera tous ceux qui ne satisferont pas à la preuve par 9 ou par 11, en supposant la division exacte. Lorsque le calcul logarithmique ne donne pas un nombre suffisant de chiffres sur lesquels on peut compter, on peut obtenir le dernier, les deux ou les trois derniers, en déterminant, ce qui est facile, les trois derniers chiffres du quotient à l'aide des derniers chiffres du dividende et du diviseur, en supposant toujours la division exacte. J'ai ainsi démontré que le nombre pris pour exemple est premier. Il est plus grand que celui que Legendre considère, d'après Euler, comme le plus grand des nombres pre-

miers connus, à savoir :

$$2^{31} - 1 = 2147483647.$$

Nous remarquerons que le dernier nombre essayé dans le tableau donne le produit

$$61681 \times 69361 = 4278255841,$$

qui ne diffère que par deux chiffres du nombre donné.

J'observerai, à ce propos, qu'il serait bon, dans les Tables de logarithmes, d'indiquer par un signe placé à côté du dernier groupe, formant chacun des logarithmes de 10000 à 100000, le cas où le nombre considéré est premier. On aurait ainsi, sans plus d'espace et sans plus de frais, une Table des nombres premiers de 1 à 108000 avec le logarithme en regard, ce qui serait un véritable progrès dans l'étude de la théorie des nombres.

Nous indiquerons encore les décompositions suivantes :

$$30^{15} - 1 = 7^2 . 19 . 29 \; 12211 \; 837931 . 51941161,$$
$$30^{15} + 1 = 11 . 13 . 31 . 67 . 271 . 4831 . 71261 . 517831,$$
$$2^{41} + 1 = 3 . 83 . 8831418697.$$

J'ai essayé ce dernier nombre pour tous les facteurs premiers, inférieurs à 60000, et ainsi

$$57073 \times 154739 = 8831418947$$

ne diffère que par deux chiffres de ce nombre, et d'ailleurs le dernier facteur est divisible par 13. L'opération qui consiste à essayer les autres nombres premiers de 60000 à 95100, et qui comporterait une seule page de calculs, reste à faire; mais je n'ai pu continuer, n'ayant pas à ma disposition les Tables de Chernac. Il serait donc facile de s'assurer si ce nombre est premier, et, dans le cas de réussite, ce serait, je pense, le plus grand nombre premier connu actuellement.