Factorisation des grands nombres.

Autor(en): **Vaes, F.-J.**

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **15 (1913)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **10.08.2024**

Factorisation des grands nombres.

A propos des articles de MM. G. Loria et A. Aubry.

A propos des intéressantes Notes de MM. Loria et Aubry, publiées dans l'*Ens. math.* du 15 mai 1913 (p. 193-231), je me permets de signaler les articles parus en 1902 dans les Actes de l'Académie Royale des Sciences d'Amsterdam[1]. On y trouvera, entre autres, une méthode donnant immédiatement les facteurs du nombre que Mersenne proposa à Fermat pour la factorisation.

Si $G = a^2_1 - b_1$ est le nombre à factoriser, et p est un facteur de G, la différence des restes de a^2_1 et de b_1 après division par p, doit être divisible par p.

Ecrivons

$$G = \left(\frac{G+1}{2}\right)^2 - \left(\frac{G-1}{2}\right)^2, \qquad \text{si} \qquad \frac{G-1}{2} \equiv r \pmod p$$

il faut que

$$\frac{G+1}{2} \equiv r + 1 \pmod p .$$

Donc

$$G \equiv (r+1)^2 - r^2 \pmod p \qquad \text{ou} \qquad G \equiv 2r + 1 \pmod p ,$$

donc $2r + 1$ doit être divisible par p.

Par exemple : $G = 80047 = (40024)^2 - (40023)^2$

$$G_1 = 40023 = 200^2 + 23 ,$$

ou $G_1 = 200^2 - 1^2 + 24$, ou $G_1 = (201 \times 199) + 24$.

Chacun des diviseurs 199 et 201 donnera 24 comme reste ; mais puisque $2r + 1 = 49$ n'est pas divisible par 199 ou 201, ces deux nombres ne seront pas des diviseurs de G. On peut écrire successivement :

	r	$2r+1$
$G_1 = 201 \times 199 +$	24	49
$202 \times 198 +$	27	55
$203 \times 197 +$	32	65
$204 \times 196 +$	39	79
$205 \times 195 +$	48	97
$206 \times 194 +$	59	119
$207 \times 193 +$	72	145
$208 \times 192 +$	87	175
$209 \times 191 +$	104	209

[1] Verhandelingen van de K. Academie van Wetenschappen te Amsterdam, 1902, p. 374-384, 474-486, 623-631 et dans l'édition anglaise, p. 326-336, 425-436, 501-508. L'étude parut plus tard en brochure chez l'éditeur Versluys à Amsterdam.

Ce tableau est facilement construit puisque les restes 23, 24, 27, 32, ... ont pour différences 1, 3, 5, ... On trouve 209 comme facteur.

Le nombre $G = 100895598169$ de Mersenne-Fermat égale

$$(50447799085)^2 - (50447799084)^2$$

tandis que

$$50447799084 = 224605^2 + 393059 \quad \text{ou} \quad = (224606 \times 224605) + 168454$$

$2r + 1 = 336909$, donc 112303, diviseur commun des nombres soulignés, est un des facteurs de G.

F.-J. VAES (Rotterdam).

CHRONIQUE

Commission internationale de l'enseignement mathématique.

SOUS-COMMISSIONS NATIONALES.

Suisse. — Comme conclusion à ses rapports, la Sous-commission suisse vient de publier un fascicule annexe intitulé « Réformes à accomplir dans l'enseignement mathématique en Suisse, vœux et propositions de la Sous-commission suisse ». Le texte est reproduit dans les trois langues nationales.

L'Enseignement mathématique en Suisse, Rapports publiés sous la direction de H. FEHR. — *Annexe* (34 p., Fr. 0,50 ; Georg & Cie, Genève et Bâle) :

Reformvorschläge und Anregungen aus den Berichten über den mathematischen Unterricht in der Schweiz.

Réformes à accomplir dans l'enseignement mathématique en Suisse.

Riforme da compiere nell' insegnamento delle matematiche nella Svizzera.

Unification de la terminologie dans les théories du potentiel et de l'élasticité.

Sur l'initiative de M. le Prof. A. KORN (Charlottenbourg), il vient de se constituer une commission en vue d'une « *unification par voie d'entente internationale des notations et de la terminologie de la théorie du potentiel et de la théorie de l'élasticité* ». Nous reproduisons ci-après la *première circulaire :*

Il est superflu d'insister sur les grands avantages qu'il y aurait à provoquer une entente entre les travailleurs des diverses natio-