Zeitschrift: L'Enseignement Mathématique

Herausgeber: Commission Internationale de l'Enseignement Mathématique

Band: 13 (1911)

Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: SUR LA DÉCOMPOSITION DES NOMBRES EN FACTEURS

Autor: Barbette, Edouard

DOI: https://doi.org/10.5169/seals-13533

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 14.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

SUR LA DÉCOMPOSITION DES NOMBRES EN FACTEURS

Dans notre ouvrage intitulé: Les sommes de ptemes puissances distinctes égales à une pième puissance¹, nous avons démontré que, quel que soit le nombre N, les équations

$$N = \frac{x(x+1)}{2} - \frac{y(y+1)}{2} ,$$

$$8N = x^{2} - y^{2} ,$$

$$Nz = \frac{x(x+1)}{2} ,$$

$$8Nz + 1 = y^{2} ,$$

sont possibles en nombres entiers; nous en avons déduit des méthodes nouvelles de décomposition des nombres en facteurs. Ce sont ces méthodes que nous allons examiner et simplifier par l'emploi des résidus triangulaires ou quadratiques.

1re méthode. — Considérons l'égalité

$$N + \frac{y(y+1)}{2} = \frac{x(x+1)}{2} \tag{1}$$

et cherchons quel nombre triangulaire, nous devons ajouter à N, pour obtenir un autre triangulaire; lorsque N est premier, les seules valeurs de x et y satisfaisant à l'équation sont

$$x = \frac{N+1}{2}$$
, $y = \frac{N-3}{2}$;

et

$$x = N$$
, $y = N - 1$.

¹ Voir l'analyse dans l'Ens. math. du 15 mai 1911. (Réd.)

Si N est composé, une décomposition de N en un produit de deux facteurs est donnée par l'égalité

$$N = \frac{(x - y)(x + y + 1)}{2}.$$

Nous admettons N impair et débarrassé des facteurs 5, par suite terminé par 1, 3, 7 ou 9; le chiffre des unités des nombres triangulaires étant 0, 1, 3, 5, 6 ou 8, il s'ensuit que:

si N est terminé par 1, les triangulaires $\frac{y(y+1)}{2}$ à ajouter sont ceux terminés par 0 et 5 et leurs rangs y sont 10+4, 10+5, 10+9 et 10;

si N est terminé par 3, les triangulaires $\frac{y(y+1)}{2}$ à ajouter sont ceux terminés par 0, 3, 5 et 8 et leurs rangs y sont 10+2, 10+4, 10+5, 10+7, 10+9 et 10;

si N est terminé par 7, les triangles $\frac{y(y+1)}{2}$ à ajouter sont ceux terminés par 1, 3, 6 ou 8 et leurs rangs y sont 10+1, 10+2, 10+3, 10+6, 10+7 et 10+8;

si N est terminé par 9, les triangulaires $\frac{y(y+1)}{2}$ à ajouter sont ceux terminés par 1 et 6 et leurs rangs y sont 10 + 1, 10 + 3, 10 + 6 et 10 + 8.

Soient maintenant, pour le module 3,

$$N \equiv \rho$$
 et $\frac{x(x+1)}{2} \equiv \rho_1$, ρ_2 , ρ_3 , ..., ρ_n ;

de l'égalité (1), nous déduisons

$$\rho + \frac{y(y+1)}{2} \equiv \rho_1, \; \rho_2, \; \rho_3, \; \dots, \; \rho_n$$

et nous devrions avoir

$$\frac{y(y+1)}{2} \equiv \rho_1 - \rho , \ \rho_2 - \rho , \ \rho_3 - \rho , \ \dots , \ \rho_n - \rho$$

ou

$$\frac{y(y+1)}{2} \equiv r_{\scriptscriptstyle 1} , r_{\scriptscriptstyle 2} . r_{\scriptscriptstyle 3} , \ldots , r_n$$

en posant $\rho_i - \rho = r_i$; mais des résidus r_i ainsi obtenus, nous ne pourrons conserver que ceux qui font partie de la suite ρ_i puisque $\frac{\gamma(\gamma+1)}{2}$ est un triangulaire; la suite des nombres triangulaires à ajouter à N se trouvera donc considérablement réduite et cette suite se réduira pour chaque nouveau diviseur d employé.

Limite des opérations. Puisque

$$2N = (x - y)(x + y + 1) ,$$

le facteur (x-y) est le plus petit diviseur de 2N; si nous ne trouvons pas de solution y inférieure à une certaine limite a, nous en conclurons

$$y > a$$
,

par suite

$$\frac{x(x+1)}{2} > N + \frac{a(a+1)}{2}$$
 d'où $x > \frac{-1 + \sqrt{8N + (2a+1)^2}}{2}$

et

$$x + y + 1 > \frac{\sqrt{8N + (2a + 1)^2 + (2a + 1)}}{2}$$

Mais $x-y=\frac{2N}{x+x+1}$; donc

$$x-y < \frac{4N}{\sqrt{8N + (2a+1)^2 + (2a+1)}}$$
 ou $\frac{\sqrt{8N + (2a+1)^2 - (2a+1)}}{2^n}$.

Si 2s + 1 et $2\sigma + 1$ sont deux diviseurs de N dont le produit égale N lui-même, à ces diviseurs correspondent les deux solutions données par les systèmes d'équations

1er système:
$$x-y=2s+1$$
; 2e système: $x-y=2(2s+1)$
 $x+y+1=2(2\sigma+1)$. $x+y+1=2\sigma+1$.

Par conséquent, si $\lambda < 2N < (\lambda + 1)^2$, les diviseurs que les essais ont éliminés sont ceux compris entre λ et $\sqrt{\frac{8N + (2a + 1)^2 - (2a + 1)}{2}}$ ainsi que ceux compris entre $\frac{\lambda}{2}$ et $\frac{\sqrt{8N + (2a + 1)^2} - (2a + 1)}{4}.$

Mais si les diviseurs que nous cherchons sont les diviseurs moindres que \sqrt{N} , la limite inférieure de α sera la partie entière de la valeur de α satisfaisant à la condition

$$\frac{\sqrt{8N + (2\alpha + 1)^2} - (2\alpha + 1)}{2} = \sqrt{N} \qquad \text{d'où} \qquad \alpha = \frac{\sqrt{N} - 1}{2}; \qquad (2)$$

si nous prenons, comme première limite supérieure, la partie entière par excès de la valeur de a satisfaisant à la condition

$$\frac{\sqrt{8N + (2a + 1)^2} - (2a + 1)}{2} = \frac{\lambda}{2} \quad \text{d'où} \quad a = \frac{8N - (\lambda^2 + 2\lambda)}{4\lambda} , \quad (3)$$

les diviseurs éliminés seront ceux compris entre \sqrt{N} et $\frac{\sqrt{8N+(2a+1)^2}-(2a+1)}{4}$. En d'autres termes, p étant le plus grand nombre premier contenu dans cette dernière limite, il restera à essayer tous les diviseurs premiers non supérieurs à p, hormis les diviseurs des modules employés; et si le nombre N n'est divisible par aucun d'eux, nous en conclurons que N est un nombre premier.

Les divisions les plus rapides sont évidemment celles par 9 et par 11; aussi ce sont là les premiers diviseurs à employer. En procédant par limites successives, à partir de $\alpha = \frac{\sqrt{N}-1}{2}$, on arrivera à décomposer avec facilité tout nombre, si grand soit-il!

Exemple. Soit à décomposer le nombre 40199; résolvons l'équation

$$40199 + \frac{y(y+1)}{2} = \frac{x(x+1)}{2} . \tag{4}$$

Observons, avant tout, que 40199 n'est divisible par aucun des nombres 3, 7, 11 et 13 que nous allons employer comme modules; de plus, 40199 étant terminé par 9, les $t_{\text{riangulaires}}$ à ajouter occupent les rangs 10 + 1, 10 + 3, 10 + 6 et 10 + 8.

Puisque $200^2 < 40199 < 201^2$ et $283^2 < 2 \times 40199 < 284^2$, les relations (2) et (3) donnent pour limite inférieure $\alpha = 99$

et pour première limite supérieure a=213; considérons donc les nombres

101	103	106	108
111	113	116	118
121	123	126	128
131	133	136	138
141	143	146	148
151	153	156	158
161	163	166	168
171	173	176	178
181	183	186	188
191	193	196	198
201	203	206	208
211	213		

Si du $101^{\rm e}$ triangulaire au $213^{\rm e}$, nous n'obtenons pas de solution, les diviseurs restant à essayer seront moindres que $\frac{\sqrt{8N + (2a + 1)^2} - (2a + 1)}{4} = \frac{\sqrt{321592 + 182329} - 427}{4} = 70, \dots,$

donc non supérieurs à 67.

L'égalité (4) donne successivement :

Pour le module 9,

$$5 + \frac{y(y+1)}{2} \equiv 0, 1, 3, 6$$

d'où nous devrions avoir

$$\frac{y(y+1)}{2} \equiv 4, 5, 7, 1;$$

mais 4, 5 et 7 sont des non-résidus triangulaires pour le module 9, par suite

$$\frac{y(y+1)}{2} \equiv 1 \pmod{9}$$

d'où

$$y = 3 + 1.$$

Pour le module 11,

$$5 + \frac{y(y+1)}{2} \equiv 0$$
, 1, 3, 4, 6, 10

d'où il faudrait

$$\frac{y(y+1)}{2} \equiv 6$$
, 7, 9, 10, 1, 5;

mais 7, 9 et 5 sont des non-résidus triangulaires pour le module 11, par suite

$$\frac{y(y+1)}{2} \equiv 1, 6, 10 \pmod{11}$$

d'où

$$y = 11 + 1, 3, 4, 6, 7, 9$$
.

Pour le module 7,

$$5 + \frac{y(y+1)}{2} \equiv 0$$
, 1, 3, 6

d'où nous devrions avoir

$$\frac{y(y+1)}{2} \equiv 2, 3, 5, 1;$$

mais 2 et 5 sont des non-résidus triangulaires pour le module 7, par suite

$$\frac{y(y+1)}{2} \equiv 1, 3 \pmod{7}$$

d'où

$$y = 7 + 1, 2, 4, 5$$
.

Pour le module 13,

$$3 + \frac{y(y+1)}{2} \equiv 0$$
, 1, 2, 3, 6, 8, 10

d'où il faudrait

$$\frac{y(y+1)}{2} \equiv 10$$
, 11, 12, 0, 3, 5, 7;

mais 11, 12, 5 et 7 sont des non-résidus triangulaires pour le module 13, par suite

$$\frac{y(y+1)}{2} \equiv 0, 3, 10 \pmod{13}$$

d'où

$$y = 1\dot{3} + 0$$
, 2, 4, 8, 10, 12.

Après avoir supprimé du tableau les nombres qui ne sont pas 3+1; 11+1, 3, 4, 6, 7, 9; 7+1, 2, 4, 5; 13+0, 2, 4, 8, 10, 12, il ne reste plus que les nombres

Aucun d'eux ne fournit de solution : par suite, si 40199 est composé, son plus petit diviseur ne peut dépasser 67. Si nous prenons maintenant a=300 et si du $214^{ième}$ triangulaire au $300^{ièmq}$, nous ne trouvons pas de solution, c'est que les diviseurs à essayer sont moindres que

$$\frac{\sqrt{321592 + 361201} - 601}{4} = 56, \dots,$$

donc non supérieurs à 53; si, au contraire, nous trouvons une solution entre les limites considérées, le nombre N admettra un diviseur plus grand que 53 et non supérieur à 67. Considérons donc les triangulaires dont les rangs sont les suivants:

		216	218
221	223	226	228
231	233	236	238
241	243	246	248
251	25 3	256	258
.261	263	266	268
271	273	276	278
281	283	286	288
291	293	296	298

Après en avoir éliminé les nombres qui ne sont pas 3+1; 11+1, 3, 4, 6, 7, 9; 7+1, 2, 4, 5; 13+0, 2, 4, 8, 10, 12, il ne reste plus que les nombres

Le triangulaire de rang 268, augmenté du nombre 40199, donne le triangulaire de rang 390; par suite,

$$40199 = 76245 - 36046 \quad \text{ou} \quad \frac{390^2 + 390}{2} - \frac{268^2 + 268}{2}$$
$$= \frac{(390 - 268)(390 + 268 + 1)}{2}$$
$$= 61 \times 659$$

2^{me} méthode. — Nous avons démontré le théorème suivant:

" Les nombres composés qui ne sont pas de la forme 2^k , pour $k \ge 2$, sont tous contenus dans l'expression

$$\frac{u(2v-u+1)}{2},$$

les nombres u et v satisfaisant aux conditions simultanées $v \ge u \ge 3$.

Si nous posons

$$\frac{u(2v-u+1)}{2} = N$$
 ou $u^2 - u(2v+1) + 2N = 0$

nous en déduisons

$$u = \frac{2v + 1 \pm \sqrt{(2v + 1)^2 - 8N}}{2} .$$

Le nombre u n'est rationnel que si

$$(2v + 1)^2 - 8N = y^2$$
 ou $8N + y^2 = x^2$ (5)

en posant 2v + 1 = x; lorsque N est premier, les seules valeurs de x et de y satisfaisant à l'équation sont

$$x = N + 2 , \qquad y = N - 2 ;$$

et

$$x = 2N + 1$$
, $y = 2N - 1$.

Si N est composé, il existe au moins un carré impair moindre que $(N-2)^2$ qui, ajouté à 8N, donne un carré x^2 ; une décomposition de N en un produit de deux facteurs est alors donnée par l'égalité

$$N = \frac{(x - y)(x + y)}{8}.$$

Nous supposons N impair et débarrassé des facteurs 5, donc terminé par 1, 3, 7 ou 9 en sorte que 8N sera terminé par 8, 4, 6 ou 2; par suite les carrés impairs étant terminés par 1, 5, ou 9:

si 8N est terminé par 8, les carrés à ajouter seront ceux

terminés par 1, carrés dont les racines sont terminées par 1 et 9;

si 8N est terminé par 4, les carrés à ajouter seront ceux terminés par 1 et 5, carrés dont les racines sont terminées par 1, 9 et 5;

si 8N est terminé par 6, les carrés à ajouter seront ceux terminés par 5 et 9, carrés dont les racines sont terminées par 5, 3 et 7;

si 8N est terminé par 2, les carrés à ajouter seront ceux terminés par 9, carrés dont les racines sont terminées par 3 et 7.

Observons en outre que les carrés terminés par 1 sont aussi terminés par 01, 21, 41, 61, 81, — que les carrés terminés par 5, le sont par 25, — que les carrés terminés par 9, le sont par 09, 29, 49, 69, 89.

Soient maintenant, pour le module 3,

$$8N \equiv \rho$$
 et $x^2 \equiv \rho_1$, ρ_2 , ρ_3 , ..., ρ_n ;

de l'égalité (5) nous déduisons

$$\rho + j^2 \equiv \rho_1$$
, ρ_2 , ρ_3 , ..., ρ_n

et nous devrions avoir

$$\mathcal{Y}^2 \equiv \rho_1-\rho\ ,\ \rho_2-\rho\ ,\ \rho_3-\rho\ ,\ \dots\ ,\ \rho_n-\rho$$
 ou
$$\mathcal{Y}^2 \equiv r_1\ ,\ r_2\ ,\ r_3\ ,\ \dots\ ,\ r_n$$

en posant $\rho_i - \rho = r_i$; mais des résidus r_i ainsi obtenus, nous ne pourrons conserver que ceux qui sont quadratiques et font partie de la suite ρ_i , puisque y^2 est un carré: la suite des carrés impairs à ajouter à 8N se trouvera ainsi considérablement réduite et cette suite se réduira pour chaque nouveau diviseur δ employé.

Limite des opérations. Puisque

$$8N = (x - y)(x + y) ,$$

le facteur (x-y) est le plus petit diviseur de 8N; si nous ne trouvons pas de solution y inférieure à une certaine li-

mite a, nous en conclurons

par suite

$$x > \sqrt{8N + a^2}$$

et

$$x + y > \sqrt{8N + a^2} + a .$$

Mais
$$x - y = \frac{8N}{x + y}$$
; donc

$$x - y < \frac{8N}{\sqrt{8N + a^2 + a}}$$
 ou $\sqrt{8N + a^2} - a$.

Si 2s + 1 et $2\sigma + 1$ sont deux diviseurs de N dont le produit égale N lui-même, à ces diviseurs correspondent les deux solutions données par les systèmes d'équations

1er système :
$$x - y = 2(2s + 1)$$
 : 2e système : $x - y = 4(2s + 1)$; $x + y = 4(2\sigma + 1)$. $x + y = 2(2\sigma + 1)$.

Par conséquent si $\lambda < 8N < (\lambda + 1)^2$, les diviseurs que les essais ont éliminés sont ceux compris entre $\frac{\lambda}{2}$ et $\frac{\sqrt{8N+a^2}-a}{2}$, ainsi que ceux compris entre $\frac{\lambda}{4}$ et $\frac{\sqrt{8N+a^2}-a}{4}$. Mais si les diviseurs que nous cherchons sont les diviseurs moindres que \sqrt{N} , la limite inférieure de a sera la partie entière de la valeur de a satisfaisant à l'équation

$$\frac{\sqrt{8N + \alpha^2} - \alpha}{2} = \sqrt{N} \qquad \text{d'où} \qquad \alpha = \sqrt{N} ; \qquad (6)$$

si nous prenons, comme première limite supérieure, la partie entière par excès de la valeur de a satisfaisant à la condition

$$\frac{\sqrt{8N + a^2} - a}{2} = \frac{\lambda}{4} \qquad \text{d'où} \qquad a = \frac{32N - \lambda^2}{4\lambda} , \qquad (7)$$

les diviseurs éliminés seront ceux compris entre \sqrt{N} et $\frac{\sqrt{8N+a^2-a}}{4}$. En d'autres termes, p étant le plus grand nombre premier contenu dans cette dernière limite, il res-

tera à essayer tous les diviseurs premiers non supérieurs à p, hormis les diviseurs des modules employés; et si le nombre N n'est divisible par aucun d'eux, nous en conclurons que N est un nombre premier.

Les divisions les plus rapides sont celles par 9 et par 11; aussi ce sont là les premiers diviseurs à employer. En procédant par limites successives, à partir de $\alpha = \sqrt{N}$, on arrivera à décomposer tout nombre, quelque grand qu'il soit!

Exemple. Soit à décomposer le nombre 40199; résolvons l'équation

$$8 \times 40199 + y^2 = x^2$$
 ou $321592 + y^2 = x^2$. (8)

Observons, avant tout, que 40199 n'est divisible par aucun des nombres 3, 7, 11 et 13 dont nous allons nous servir comme modules; de plus, 321592 étant terminé par 2, les carrés à ajouter sont ceux terminés par 9, carrés dont les racines sont terminées par 3 et 7.

Puisque $200^2 < 40199 < 201^2$ et $567^2 < 321592 < 568^2$, les relations (6) et (7) donnent pour limite inférieure $\alpha = 200$ et pour limite supérieure a = 426; considérons donc les nombres

203		25 3	303	353	403
207		257	307	357	407
213		263	313	363	413
217		267	317	367	417
22 3		273	323	373	423
227		277	327	377	
233		283	333	383	
237	<u>.</u>	287	337	387	
243		293	343	393	
247		297	347	397	

Si aucun de ces nombres ne fournit de solution, les diviseurs restant à essayer seront moindres que

$$\frac{\sqrt{8N + a^2} - a}{4} = \frac{\sqrt{321592 + 181476} - 426}{4} = 70 , \dots$$

donc non supérieurs à 67.

L'égalité (8) donne successivement : Pour le module 9,

$$4 + \gamma^2 \equiv 0, 1, 4, 7$$

d'où on devrait avoir

$$y^2 \equiv 5, 6, 0, 3;$$

mais 5, 6 et 3 sont des non-résidus quadratiques pour le module 9, par suite

$$y^2 \equiv 0 \pmod{9}$$

d'où

$$y = \dot{3}$$
.

Pour le module 11,

$$-4+y^2\equiv 0$$
, 1, 3, 4, 5, 9

d'où il faudrait

$$y^{2} \equiv 4$$
 , 5 , 7 , 8 , 9 , 2 ;

mais 7, 8 et 2 sont des non-résidus quadratiques pour le module 11, par suite

$$y^2 \equiv 4.5, 9 \pmod{11}$$

d'où

$$y = i1 + 2, 3, 4, 7, 8, 9$$
.

Pour le module 7,

$$5 + \gamma^2 \equiv 0, 1, 2, 4$$

d'où nous devrions avoir

$$y^2 \equiv 2$$
 , 3 , 4 , 6 ;

mais 3 et 6 sont des non-résidus quadratiques pour le module 7, par suite

$$y^2 \equiv 2$$
, 4 (mod 7)

d'où

$$y = 7 + 2, 3, 4, 5$$
.

Pour le module 13,

$$11 + y^2 \equiv 0$$
, 1, 3, 4, 9, 10, 12

d'où il faudrait

$$y^2 \equiv 2$$
 , 3 , 5 , 6 , 11 , 12 , 1 ;

mais 2, 5, 6 et 11 sont des non-résidus quadratiques pour le module 13, par suite

$$y^2 \equiv 1$$
 , 3 , $12 \pmod{13}$

d'où

$$\gamma = 13 + 1, 4, 5, 8, 9, 12$$
.

Après avoir supprimé du tableau les nombres qui ne sont pas $\dot{3}$; $\dot{11} + 2$, 3, 4, 7, 8 ou 9; $\dot{7} + 2$, 3, 4 ou 5; $\dot{13} + 1$, 4, 5, 8, 9 ou 12, il ne reste plus que les nombres

207 . 213 et 333 .

Aucun d'eux ne fournit de solution: par suite, si 40199 est composé, son plus petit diviseur ne peut dépasser 67. Si nous prenons maintenant a=600 et si pour cette limite nous ne trouvons pas de solution, c'est que les diviseurs restant à essayer sont moindres que $\frac{\sqrt{321592+360000}-600}{4}=56$, ..., donc non supérieurs à 53. Considérons les carrés dont les racines sont

	453	503	553
	457	507	557
	463	513	563
	467	517	567
	473	523	573
427	477	527	577
433	483	533	583
437	487	537	587
443	493	543	593
447	497	547	597

Après en avoir éliminé les nombres qui ne sont pas $\dot{3}$; $\dot{11}+2$, 3, 4, 7, 8 ou 9; $\dot{7}+2$, 3, 4 ou 5; $\dot{13}+1$, 4, 5, 8, 9 ou 12, il ne reste plus que les nombres

537 et 597.

Le carré de racine 537, augmenté du nombre 321592, donne le carré de racine 781 :

$$8 \times 40199 = 609961 - 288369$$
 ou $781^2 - 537^2$
= $(781 - 537)(781 + 537)$
= 244×1318 ;

par suite

 $40199 = 61 \times 659$.

3^{me'} méthode. — L'équation

$$Nz = \frac{x(x+1)}{2} , \qquad (9)$$

étant possible en nombres entiers pour toute valeur de N, soient pour le module δ :

$$N \equiv
ho \quad ext{et} \quad rac{x(x+1)}{2} \equiv
ho_1 \; , \;
ho_2 \; , \;
ho_3 \; , \; \ldots \; , \;
ho_{\hat{n}} \; ;$$

de l'égalité (9) nous déduisons

ρ
$$z \equiv \rho_1$$
 , ρ_2 , ρ_3 , ... , ρ_n d'où
$$z \equiv r_1$$
 , r_2 . r_3 , ... , r_n . (mod δ)

Rappelons de plus que si N est composé, le multiplicateur $\frac{\frac{N+1}{2}\times\frac{N+3}{2}}{2N}; \text{ si } \lambda \text{ est le plus grand entier contenu dans cette limite, nous éliminerons de la suite des multiplicateurs}$

$$1, 2, 3, 4, \dots, \lambda$$
 (10)

ceux qui ne sont pas de la forme z pour le module δ et le nombre d'essais se réduira considérablement. Si nous ne trouvons aucune valeur de z comprise dans la suite (10) ainsi réduite, rendant le produit Nz triangulaire, nous en conclurons que N est premier.

Observons que si N est terminé par 1, puisque le chiffre des unités des triangulaires est 0, 1, 3, 5, 6 ou 8, les multiplicateurs z seront terminés par 0, 1, 3, 5, 6 et 8; que si N est terminé par 3, les multiplicateurs z seront terminés par 0, 1, 2, 5, 6 et 7; que si N est terminé par 7, les multiplicateurs z seront terminés par 0, 3, 4, 5, 8 et 9; que si N est terminé par 9, les multiplicateurs z seront terminés par 0, 2, 4, 5, 7 et 9.

Exemple. Soit à décomposer le nombre 4321; résolvons l'équation

$$4321 \times z = \frac{x(x+1)}{2} \ . \tag{11}$$

Si 4321 est composé, cette équation admet au moins une solution pour $z \leq 540$; de plus, le nombre à décomposer étant terminé par 1, les multiplicateurs z à considérer sont ceux terminés par 0, 1, 3, 5, 6 et 8.

De l'égalité (11) nous déduisons successivement : pour le module 9,

$$z \equiv 0$$
 , 1 , 3 , 6

d'où
$$z = 9 + 0, 1, 3, 6;$$

pour le module 11,

$$9z \equiv 0$$
, 1, 3, 4, 6, 10

d'où
$$z = \dot{1}1 + 0.4, 5, 6, 8, 9$$
;

pour le module 7,

$$2z \equiv 0$$
 , 1 , 3 , 6

d'où
$$z = \dot{7} + 0$$
, 3, 4, 5;

pour le module 13,

$$5z \equiv 0$$
 , 1 , 2 , 3 , 6 , 8 , 10 d'où $z = \dot{1}3 + 0$, 2 , 3 , 8 , 9 , 11 , 12 .

Convenons de prendre les valeurs de z non supérieures à 150 et considérons la suite des multiplicateurs :

$$141$$
 , 143 , 145 , 146 , 148 , 150 .

Si de cette suite nous supprimons les nombres qui ne sont pas 9+0, 1, 3, 6; 11+0, 4, 5, 6, 8, 9; 7+0, 3, 4, 5; 13+0, 2, 3, 8, 9, 11, 12, il reste les nombres suivants :

Le produit $4321 \times 126 = 544446$ représente le $1043^{\text{ième}}$ triangulaire; par suite

$$4321 \times 126 = \frac{1043 \times 1044}{2}$$

4^{me} méthode. — L'équation

$$8Nz + 1 = y^2 , (12)$$

étant possible en nombres entiers pour toute valeur de N, soient pour le module δ :

$$8N \equiv \rho$$
 et $y^2 \equiv \rho_1$, ρ_2 , ρ_3 , ..., ρ_n ;

de l'égalité (12) nous déduisons

$$\rho z + 1 \equiv \rho_1, \ \rho_2, \ \rho_3, \ \dots, \ \rho_n$$

$$\rho z \equiv \rho_1 - 1, \ \rho_2 - 1, \ \rho_3 - 1, \dots, \ \rho_n - 1$$

par suite

$$z \equiv r_{\scriptscriptstyle 1} \;,\; r_{\scriptscriptstyle 2} \;,\; r_{\scriptscriptstyle 3} \;,\; \ldots \;,\; r_{\scriptscriptstyle n} \;\;. \tag{mod δ}$$

Rappelons que si N est composé, le multiplicateur z est $\frac{N+1}{2} \times \frac{N+3}{2}$ moindre que $\frac{N+1}{2} \times \frac{N+3}{2}$; le chiffre des unités des nombres carrés étant 0, 1, 4, 5, 6 ou 9, il s'ensuit que si N est terminé par 1, les multiplicateurs z seront terminés par 0, 1, 3, 5, 6 et 8; si N est terminé par 3, les multiplicateurs z seront terminés par 0, 1, 2, 5, 6 et 7; si N est terminé par 7, les multiplicateurs z seront terminés par 0, 3, 4, 5, 8 et 9; que si N est terminé par 9, les multiplicateurs z seront terminés par 0, 2, 4, 5, 7 et 9.

Exemple. Soit à décomposer le nombre 4321; résolvons l'équation

$$8 \times 4321 \times z + 1 = y^2$$
 ou $34568z + 1 = y^2$. (13)

Si 4321 est composé, cette équation admet au moins une solution pour $z \leq 540$; de plus, le nombre à décomposer étant terminé par 1, les multiplicateurs z à considérer sont ceux terminés par 0, 1, 3, 5, 6 et 8.

De l'égalité (13) nous déduisons successivement : pour le module 9,

$$8z + 1 \equiv 0$$
, 1, 4, 7 d'où $z = 9 + 0$, 1, 3, 6;

pour le module 11,

$$6z + 1 \equiv 0, 1, 3, 4, 5, 9$$
 d'où $z = 1\dot{1} + 0, 4, 5, 6, 8, 9;$

pour le module 7,

$$2z + 1 \equiv 0$$
, 1, 2, 4

d'où
$$z = \dot{7} + 0, 3, 4, 5;$$

pour le module 13,

$$z+1 \equiv 0$$
, 1, 3, 4, 9, 10, 12 d'où $z=13+0$, 2, 3, 8, 9, 11, 12.

Si nous ne prenons, ainsi que dans la méthode précédente, que les valeurs de z non supérieures à 150, les valeurs subsistant après l'emploi des modules 9, 11, 7 et 13 sont encore

Un seul de ces nombres, z=126, fournit une solution de l'équation et donne

$$8 \times 4321 \times 126 + 1 = 4355569$$
 ou 2087^2
 $8 \times 4321 \times 126 = 2086 \times 2088$
 $4321 \times 7 \times 9 = 1043 \times 261$;

par conséquent

$$4321 = 149 \times 29$$
;

Observation. — Les deux premières méthodes se déduisent l'une de l'autre, ainsi que les deux dernières : en effet, si nous posons x-y=u et x+y=2v-u, l'équation

$$\frac{x(x+1)}{2} - \frac{y(y+1)}{2} = N \qquad \text{devient} \qquad \frac{u(2v-u+1)}{2} = N ;$$

ensuite de l'équation

$$Nz = \frac{x(x+1)}{2} ,$$

nous déduisons

$$x = \frac{-1 + \sqrt{1 + 8Nz}}{2}$$

et x n'est rationnel que si

$$1 + 8Nz = y^2.$$

Il est bon de remarquer que la série des nombres triangulaires s'obtient par additions successives et qu'il serait plus facile d'étendre la table des 5000 premiers triangulaires que nous avons créée que la table des carrés, déjà fort étendue cependant.

Edouard BARBETTE (Liège).