

MORET-BLANC

**Questions nouvelles d'arithmétique
supérieure proposées par M. Édouard Lucas**

Nouvelles annales de mathématiques 2^e série, tome 20
(1881), p. 253-265

[<http://www.numdam.org/item?id=NAM_1881_2_20_253_0>](http://www.numdam.org/item?id=NAM_1881_2_20_253_0)

© Nouvelles annales de mathématiques, 1881, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
<http://www.numdam.org/>

**QUESTIONS NOUVELLES D'ARITHMETIQUE SUPÉRIEURE
PROPOSÉES PAR M. ÉDOUARD LUCAS;**

(voir 2^e série, t. XV, p. 83);

PAR M. MORET-BLANC.

1. Déterminer le dernier chiffre du n^{ième} terme de la série de Lamé donnée par la loi de récurrence

$$u_{n+2} = u_{n+1} + u_n$$

et les conditions initiales $u_0 = 0$, $u_1 = 1$.

Les derniers chiffres forment nécessairement une période, qui recommencera lorsque les derniers chiffres de deux termes consécutifs redeviendront les mêmes. Formons cette période :

0, 1, 1, 2, 3, 5, 8, 3, 1, 4, 5, 9, 4, 3, 7,
0, 7, 7, 4, 1, 5, 6, 1, 7, 8, 5, 3, 8, 1, 9,
0, 9, 9, 8, 7, 5, 2, 7, 9, 6, 5, 1, 6, 7, 3,
0, 3, 3, 6, 9, 5, 4, 9, 3, 2, 5, 7, 2, 9, 1.

On voit que

0	termine les termes de rang	$60m + (1, 16, 31, 46),$
1	»	$60m + (2, 3, 9, 20, 23, 29, 42, 60),$
2	»	$60m + (4, 37, 55, 58),$
3	»	$60m + (5, 8, 14, 27, 45, 47, 48, 54),$
4	»	$60m + (10, 13, 19, 52),$
5	»	$60m + (6, 11, 21, 26, 36, 41, 51, 56),$
6	»	$60m + (22, 40, 43, 49),$
7	»	$60m + (15, 17, 18, 24, 35, 38, 44, 47),$
8	»	$60m + (7, 25, 28, 34),$
9	»	$60m + (12, 30, 32, 33, 39, 50, 53, 59);$

m peut être 0.

Au moyen de ce tableau, le reste de la division de *n*

par 60 fera connaître le dernier chiffre du $n^{\text{ième}}$ terme de la série ou de u_{n-1} .

On peut remarquer que les chiffres qui terminent les 30 derniers termes de la période sont les compléments à 10 de ceux qui terminent les 30 premiers.

Il y a 4 termes terminés par chacun des chiffres pairs et 8 terminés par chacun des chiffres impairs.

2. *Formuler les restes obtenus dans la recherche du plus grand commun diviseur de deux termes donnés de la série, u_p et u_q , en fonction des rangs p et q .*

Remarquons : 1° que, si l'on prolonge la série vers la gauche en donnant aux termes des indices négatifs, on aura

$$u_{-n} = \mp u_n,$$

suivant que n est pair ou impair; 2° que, si l'on prend les termes de m en m , et que l'on désigne par v les termes de la série ainsi formée, on aura, quel que soit le point de départ,

$$(1) \quad v_{n+2} = A v_{n+1} \mp v_n,$$

suivant que m est pair ou impair, avec

$$A = \frac{u_{2m}}{u_m},$$

nombre toujours entier.

Cela posé, proposons-nous de trouver les restes obtenus dans la recherche du plus grand commun diviseur de u_p et u_q . Soient, pour fixer les idées, $q > p$ et $q - p = m$, et supposons qu'on prenne les quotients par excès si m est pair, et par défaut si m est impair, de manière à avoir toujours un reste moindre que la moitié du diviseur.

Les restes successifs seront, d'après la formule (1),

$$u_{p-m}, u_{p-2m}, u_{p-3m}, \dots,$$

jusqu'à ce que l'on passe d'un indice positif à un indice négatif. Soient p' le plus petit, q' le plus grand des deux indices en valeur absolue, et $q' - p' = m'$; on aura ensuite

$$u_{p'-m'}, u_{p'-2m'}, \dots,$$

et ainsi de suite. En d'autres termes, les restes seront des termes de la série ayant pour indices les restes qu'on obtiendrait si, dans la recherche du plus grand commun diviseur entre p et m , on faisait les divisions par soustractions successives.

Les restes sont ainsi exprimés en termes de la série dont les indices sont fonctions de p et q . Nous verrons plus loin l'expression d'un terme de la série en fonction de son indice.

3. Traiter les mêmes questions pour la série

$$0, 1, 2, 5, 12, \dots,$$

données par la loi de récurrence

$$u_{n+2} = 2u_{n+1} + u_n,$$

et généralement pour les séries récurrentes du premier genre données par la loi

$$u_{n+2} = au_{n+1} + bu_n,$$

dans laquelle a et b désignent des nombres premiers entre eux.

La période des derniers chiffres se forme de la même

manière; elle est, pour la première série,

0,	1,	2,	5,	2,	9,	0,	9,	8,	5,	8,	1;
o	termine les termes de rang $12m + (1, 7)$.										
1	» $12m + (2, 12)$,										
2	» $12m + (3, 5)$,										
5	» $12m + (4, 10)$,										
8	» $12m + (9, 11)$,										
9	» $12m + (6, 8)$.										

Aucun terme n'est terminé par 3, 4, 5, 6.

Les formules qui expriment les restes obtenus dans la recherche du plus grand commun diviseur de u_p et u_q en termes de la série restent les mêmes que pour la série de Lamé.

Considérons la série

$$0, 1, a, a^2 + b, a^3 + 2ab, a^4 + 3a^2b + b^2, \\ a^5 + 4a^3b + 3ab^2, a^6 + 5a^4b + 6a^2b^2 + b^3, \dots$$

dont la loi de récurrence est

$$u_{n+2} = au_{n+1} + bu_n.$$

Si l'on prend les termes de m en m , et qu'on désigne par v les termes de la série obtenue, on aura

$$v_{n+2} = Av_{n+1} + b^m v_n,$$

suivant que m est pair ou impair, avec

$$A = \frac{u_{2m}}{u_m},$$

nombre entier.

Si l'on a soin de supprimer, dans chaque reste obtenu dans la recherche du plus grand commun diviseur de u_p et u_q , le facteur b^m qui est premier avec le diviseur, puis $b^{m'}$, quand on sera ramené à chercher le plus grand commun diviseur de $u_{p'}$ et $u_{q'}$, ..., la loi des restes sera la même que dans les deux cas déjà considérés.

4. *Trouver l'expression générale du terme de la série, en supposant $u_0 = 0$, $u_1 = 1$, quelles que soient les valeurs de a et b .*

La fonction génératrice de la série est

$$\begin{aligned} \frac{1}{1-ax-bx^2} &= \frac{1}{\left(\frac{-a+\sqrt{a^2+4b}}{2b}-x\right)\left(\frac{a+\sqrt{a^2+4b}}{2b}+x\right)} \\ &= \frac{b}{\sqrt{a^2+4b}} \left(\frac{1}{\frac{-a+\sqrt{a^2+4b}}{2b}-x} + \frac{1}{\frac{a+\sqrt{a^2+4b}}{2b}+x} \right). \end{aligned}$$

u_n est le coefficient de x^{n-1} dans le développement de cette fonction ordonnée suivant les puissances croissantes de x ; on a donc

$$\begin{aligned} u_n &= \frac{b}{\sqrt{a^2+4b}} \left[\left(\frac{a+\sqrt{a^2+4b}}{2b} \right)^n - \left(\frac{a-\sqrt{a^2+4b}}{2b} \right)^n \right] \\ \text{ou} \\ u_n &= a^{n-1} + \frac{n-2}{1} a^{n-3} b + \frac{(n-3)(n-4)}{1 \cdot 2} a^{n-5} b^2 \\ &\quad + \frac{(n-4)(n-5)(n-6)}{1 \cdot 2 \cdot 3} a^{n-7} b^3 + \dots \end{aligned}$$

Si l'on fait $a = 1$, $b = 1$, on a, pour la série de Lamé,

$$u_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right],$$

et, en faisant $a = 2$, $b = 1$, on a, pour la série du n° 3,

$$u_n = \frac{1}{2\sqrt{2}} [(1+\sqrt{2})^n - (1-\sqrt{2})^n].$$

Nous avons obtenu les restes de la recherche du plus grand commun diviseur entre u_p et u_q , exprimés en termes de la série dont les indices sont fonctions de p et q ; on pourra donc exprimer les restes eux-mêmes en fonction de p et q .

3. Si p désigne un nombre premier et u_p l'expression

$$u_p = \frac{(a + \sqrt{b})^p - (a - \sqrt{b})^p}{\sqrt{b}},$$

démontrer que u_{p+1} est divisible par p si b est un non-résidu quadratique de p , et que u_{p-1} est divisible par p , en exceptant les valeurs de a pour lesquelles $a^2 - b$ est divisible par p , si b désigne un résidu quadratique de p .

On a

$$u_{p+1} = \frac{(a + \sqrt{b})^{p+1} - (a - \sqrt{b})^{p+1}}{\sqrt{b}}.$$

Développant et supprimant les termes qui contiennent le facteur p , on a

$$u_{p+1} = 2(p+1)a(a^{p+1} + b^{\frac{p-1}{2}}) \pmod{p}.$$

Or

$$a^{p-1} \equiv 1 \pmod{p} \quad (\text{theoreme de Fermat}),$$

et, b étant un non-résidu quadratique de p ,

$$b^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

donc

$$u_{p+1} \equiv 0 \pmod{p}. \quad \text{C. Q. F. D.}$$

On a

$$\begin{aligned} u_{p-1} &= \frac{(a + \sqrt{b})^{p-1} - (a - \sqrt{b})^{p-1}}{\sqrt{b}} \\ &= 2a(a^{p-3} + a^{p-5}b + a^{p-7}b^2 + \dots + b^{\frac{p-3}{2}}) \\ &= 2a \left[(a^2)^{\frac{p-1}{2}} - b^{\frac{p-1}{2}} \right] \equiv \frac{2a(1-1)}{a^2-b} \pmod{p}. \end{aligned}$$

Le numérateur $\equiv 0 \pmod{p}$, c'est-à-dire qu'il est divisible par p ; donc, si $a^2 - b$ n'est pas divisible par p , u_{p-1} le sera nécessairement.

C. Q. F. D.

8. Résoudre complètement l'équation

$$x^2 + (x+1)^2 + \dots + [x + (n-1)]^2 = y^2$$

pour les valeurs de n égales à 2, 11, 23, 24.

$$\begin{aligned} x^2 + (x+1)^2 + \dots + [x + (n-1)]^2 \\ = nx^2 + n(n-1)x + \frac{n(n-1)(2n-1)}{6} = y^2. \end{aligned}$$

1° Soit $n = 2$:

$$\begin{aligned} 2x^2 + 2x + 1 = y^2 &= \left(1 + \frac{m}{n}x\right)^2 \\ &= 1 + \frac{2m}{n}x + \frac{m^2}{n^2}x^2, \quad \frac{m}{n} > 1, \end{aligned}$$

d'où

$$x = \frac{2n(m-n)}{2n^2 - m^2};$$

x sera entier et positif si l'on a

$$2n^2 - m^2 = 1 \quad \text{ou} \quad 2n^2 - m^2 = 2.$$

Dans le second cas, m doit être pair; posons alors $m = 2m'$.

On a à trouver les solutions des deux équations

$$(1) \quad m^2 = 2n^2 - 1,$$

$$(2) \quad n^2 = 2m'^2 - 1.$$

Elles seront données par les réduites de rang pair pour (1) et de rang impair pour (2) dans le développement de $\sqrt{2}$ en fraction continue. On obtient ainsi les doubles séries de valeurs

$$m = 1, 7, 41, 239, 1393, 8119, \dots,$$

$$n = 1, 5, 29, 169, 985, 5741, \dots,$$

$$m = 0, 4, 24, 140, 816, 4756, \dots,$$

$$n = 1, 3, 17, 99, 577, 3363, \dots$$

(260)

On en déduit les deux séries de valeurs de x

$$x = 0, 20, 696, 23660, 803760, 27304196, \dots,$$

$$x = -1, 3, 119, 4059, 137903, 4684659, \dots,$$

qu'on peut réunir en une seule

$$x = -1, 0, 3, 20, 119, 696, 4059, 23660, 137903, 803760, \dots,$$

dont la loi de récurrence est

$$u_{n+3} = 7(u_{n+2} - u_{n+1}) + u_n.$$

2° Soit $n = 11$:

$$11x^2 + 110x + 11 \times 35 = y^2$$

ou

$$11(x+5)^2 + 110 = y^2,$$

$$y^2 - 11(x+5)^2 = 110.$$

Posons

$$y = \pm 11(x+5-10u),$$

y étant évidemment un multiple de 11; l'équation devient, en divisant par 110,

$$(x+5)^2 - 22u + 110u^2 = 1,$$

et, en posant $x+5-11u = \pm x_1$,

$$x_1^2 - 11u^2 = 1.$$

Les valeurs de x_1 et de u sont données par les réduites de rang impair dans le développement de $\sqrt{11}$ en fraction continue; ce sont

$$x_1 = 1, 10, 199, 3970, 79201, 1580050, \dots,$$

$$u = 0, 3, 60, 1197, 23880, 476403, \dots,$$

et, comme $x = 11u - 5 \mp x_1$, on a les deux séries de valeurs de x

$$x = -6, 18, 456, 9192, 183474, 3660378, \dots,$$

$$x = -4, 38, 854, 17132, 341876, 6820478, \dots,$$

(261)

et les deux séries de valeurs correspondantes de y

$$y = 11, \quad 77, \quad 1529, \quad 30503, \quad 608531, \quad \dots,$$

$$y = 11, \quad 143, \quad 2849, \quad 56837, \quad 1133891, \quad \dots$$

La loi de récurrence pour chaque série est

$$u_{n+3} = 21(u_{n+2} - u_{n+1}) + u_n.$$

3° Soit $n = 23$:

$$23x^2 + 23 \times 22x + 23 \times 165 = y^2$$

ou

$$y^2 - 23(x + 11)^2 = 23 \times 44$$

y est multiple de 23).

Posons

$$y = \pm 23(x + 11 - 22u);$$

l'équation devient, en divisant par 23×22 ,

$$(x + 11 - 23u)^2 - 23u^2 = 2,$$

ou, en posant $x + 11 - 24u = \pm x_1$,

$$x_1^2 - 23u^2 = 2.$$

Les solutions de cette équation sont données par les réduites de rang pair correspondant au quotient complet de dénominateur 2 dans le développement de $\sqrt{23}$ en fraction continue; les dénominateurs des quotients complets sont

$$7, \quad 2, \quad 7, \quad 1, \quad 7, \quad 1, \quad 7, \quad 1, \quad \dots$$

Une seule réduite satisfait à la question : c'est $\frac{5}{1}$.

On a donc

$$x_1 = 5, \quad u = 1, \quad \text{d'où} \quad x = 12 \mp 5,$$

$$x = 7, \quad y = 92,$$

$$x = 17, \quad y = 138.$$

.

En donnant à u la valeur -1 , on aurait les solutions négatives

$$x = -29, \quad x = -39.$$

4° Soit $n = 34$.

$$24x^2 + 24 \times 23x + 4 \times 23 \times 47 = y^2$$

ou

$$6(2x + 23)^2 + 1150 = y^2.$$

$2x + 23$, 1150 et y étant premiers entre eux deux à deux, on peut, si l'équation est résoluble, satisfaire à l'équation indéterminée du premier degré

$$y = n(2x + 23) - 1150u,$$

où y et x seraient des valeurs données satisfaisant à l'équation du second degré, et n et u des indéterminées.

Substituant cette valeur de y , on a

$$(n^2 - 6)(2x + 23)^2 - 2300nu(2x + 23) + 1150^2u^2 = 1150.$$

Il faut que $n^2 - 6$ soit divisible par 1150 ; or,

$$34^2 - 6 = 1150.$$

Posons donc $n = 34$ et divisons par 1150 ; il vient

$$(2x + 23)^2 - 68u(2x + 23) + 1150u^2 = 1$$

ou

$$(2x + 23 - 34u)^2 - 6u^2 = 1,$$

ou, en posant $2x + 23 - 34u = \pm x_1$,

$$x_1^2 - 6u^2 = 1.$$

Les solutions de cette équation sont données par les réduites de rang impair dans le développement de $\sqrt{6}$ en fraction continue; ce sont :

$$x_1 = 1, 5, 49, 485, 4801, 47525, 470449, 4656965, \dots,$$

$$u = 0, 2, 20, 198, 1960, 19402, 192060, 1901198, \dots,$$

$$x = \frac{34u - 23 \pm x_1}{2},$$

d'où

$$x = -11, 25, 353, 3597, 35709, 353585, 3500283, \dots,$$

$$x = -12, 20, 304, 3112, 30908, 306060, 3029784, \dots$$

puis

$$y = 34, 182, 1786, 17678, \dots,$$

$$y = 34, 158, 1546, 15302, \dots$$

La loi de récurrence pour chacune des quatre séries est

$$u_{n+3} = 11(u_{n+2} - u_{n+1}) + u_n.$$

9. *Démontrer, sans se servir de la Table des nombres premiers, que $2^{31} - 1$ est un nombre premier.*

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

dont la racine carrée, à une unité près, est 46340.

Il faut démontrer que $2^{31} - 1$ n'est divisible par aucun nombre premier inférieur à 46340.

Or, $2^{31} - 1$ n'admet que des diviseurs de la forme $62m + 1$, et comme ils doivent diviser aussi $2^{32} - 2$, qui est de la forme $t^2 - 2u^2$, et n'admet que des diviseurs de la forme $8m + 1$ et $8m + 7$, les diviseurs de $2^{31} - 1$ doivent être de la forme $248m + 1$ ou $248m + 63$.

Il y a $\left(\frac{46340}{248}\right) = 186$ nombres de chaque forme inférieurs à 46340, parmi lesquels on peut supprimer ceux qui ne sont pas premiers.

A cet effet, je représente les 186 nombres de chaque série par son numéro d'ordre 1, 2, 3, 4, ..., 186.

Considérons d'abord les nombres $248m + 1$.

Soient p un nombre premier, r le reste de la division de 248 par p , et n le numéro d'ordre du premier terme divisible par p ; on aura

$$1 + nr = mp \quad \text{ou} \quad mp - nr = 1.$$

n sera donné rapidement par la réduction de $\frac{m}{n}$ en fraction continue; ce sera le numérateur de l'avant-dernière réduite, pris avec le signe + ou le signe — suivant que cette réduite est de rang pair ou impair, $\frac{1}{0}$ étant la première. S'il est négatif, on le remplacera par le complément à p . On effacera les nombres $n + kp$.

Pour les nombres $248m + 63$, il faudra multiplier cette valeur de n par le reste de la division de 63 par p et supprimer le multiple de p contenu dans le produit.

En opérant ainsi, et ayant égard aux nombres premiers < 263 , il ne reste dans la première série que les termes

6, 11, 17, 21, 24, 26, 29, 32, 35, 36, 41,
45, 47, 50, 59, 62, 66, 71, 74, 80, 81, 87,
89, 92, 95, 96, 104, 105, 110, 111, 116, 117, 120,
125, 126, 146, 147, 150, 155, 161, 162, 171, 176, 180,
182, 186,

où n représente $248n + 1$, et dans la seconde série

1, 5, 10, 11, 20, 22, 25, 37, 46, 47, 52,
58, 62, 65, 68, 76, 82, 85, 86, 95, 113, 118,
121, 122, 125, 136, 137, 142, 143, 148, 163, 166, 167,
170, 172, 173, 176, 178, 185.

où n représente $248n + 63$.

En tout, 85 diviseurs à essayer.

Si l'on écrit les produits de 248 par les neuf premiers nombres, tous ces diviseurs s'obtiendront immédiatement ou par l'addition de deux nombres.

Trois seulement, 311, 1303, 1489, donnant des quotients de sept chiffres, on vérifie par la division ordinaire qu'ils ne divisent par 2147483647. Pour tous les

autres, on peut opérer par logarithmes; les Tables à 7 décimales donnent avec certitude le dernier chiffre du quotient, et l'on ne conserve que les diviseurs dont le dernier chiffre multiplié par le dernier chiffre du quotient donne un produit terminé par 7.

Cette condition n'est remplie que par les nombres suivants :

Diviseurs ...	{	5953, 17609, 18353, 20399, 21143,
	{	27281, 29761, 32303, 40487.
Quotients ...	{	360739, 121953, 117009, 105273, 101559,
	{	78717, 72157, 66479, 53041.

Les preuves par 9 et par 11 montrent que le produit de l'un de ces diviseurs par le quotient correspondant ne peut pas être égal à 2147483647; donc ce nombre, n'admettant pas de diviseur inférieur à sa racine carrée, est un nombre premier.

C. Q. F. D.

Note. — Il reste à résoudre les numéros 6 et 7.