JOURNAL

DE

MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

J. BOURGET

Sur un problème de permutations successives nommé Battement de Monge

Journal de mathématiques pures et appliquées 3e série, tome 8 (1882), p. 413-434.

<http://www.numdam.org/item?id=JMPA_1882_3_8__413_0>

Sur un problème de permutations successives nommé Battement de Monge;

PAR M. J. BOURGET,

Recteur de l'Académie de Clermont.

---

1. Considérons $m = 2n$ objets que nous nommerons, dans un premier ordre,

$$1,\quad 2,\quad 3,\quad \ldots,\quad n,\quad (n+1),\quad \ldots,\quad (2n-2),\quad (2n-1),\quad 2n$$

et formons la substitution indiquée par l'ensemble des deux lignes correspondantes suivantes :

$$\left|\begin{array}{cccccccc} 1 & 2 & 3 & \ldots,\ n & (n+1) & \ldots,\ (2n-2) & (2n-1) & 2n \\ 2n & (2n-2) & (2-4) & \ldots,\ 2 & 1 & \ldots,\ (2n-5) & (2n-3) & (2n-1) \end{array}\right|,$$

où tous les nombres pairs, à partir du plus élevé, sont écrits, dans la seconde ligne, les uns à la suite des autres et à leur suite tous les nombres impairs dans leur ordre.

Dans le cas particulier de dix objets, la permutation donne le tableau suivant :

$$\left|\begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 8 & 6 & 4 & 2 & 1 & 3 & 5 & 7 & 9 \end{array}\right|.$$

On peut regarder les deux lignes comme indiquant une *substitution* des éléments de la seconde ligne aux éléments de la première. C'est cette substitution qu'on nomme *Battement de Monge*.

2. Si les objets donnés sont des cartes numérotées, on peut réaliser la permutation ou substitution indiquée par les deux lignes ci-dessus au moyen d'une opération matérielle fort simple et fort connue. Plaçons la deuxième carte au-dessus de la première; laissons la troisième à sa place et plaçons la quatrième au-dessus du jeu; laissons la cinquième à sa place et plaçons la sixième au-dessus du jeu, etc. Après ce battement, les cartes paires seront les unes au-dessous des autres en ordre inverse et les cartes impaires seront au-dessous des premières dans leur ordre naturel.

3. *Historique de la question.* — Le premier, à ma connaissance, qui se soit occupé des propriétés de ce battement est Bachet, sieur de Méziriac, dans son livre des *Problèmes plaisants et délectables* (1).

Monge a publié un Mémoire sur ce sujet dans le VII^e Volume des *Savants étrangers* (1re série).

La question, traitée par Bouniakowski dans son travail *Sur un problème de position relatif à la théorie des nombres* (2), n'est autre que celle du Battement de Monge. Ce Mémoire a été résumé par Terquem dans les *Nouvelles Annales de Mathématiques* (1858).

Bellavitis, dans la *Revista* de 1860 (p. 29), résume aussi le même Mémoire de Bouniakowski et fait connaître quelques propriétés nouvelles des périodes auxquelles il conduit.

On trouve dans les *Mémoires de l'Académie du Gard* (1865) un travail peu connu de M. Thomas de Saint-Laurent sur le même sujet. Cet auteur reprend et généralise le problème du battement de Monge; il ne connaît pas le travail russe que nous venons de citer, et, de plus, il commet quelques erreurs.

Je me propose ici de résumer les Mémoires que je viens de citer et d'élucider certains points restés obscurs, qui n'ont pas été traités.

4. *Propriétés du battement de Monge.* — Quand on répète indéfiniment le même battement sur un nombre de cartes choisi, on observe qu'au bout d'un nombre limité d'opérations les cartes reprennent leur

(1) *Voir* 4^e édition, Gauthier-Villars, 1879, p. 214.

(2) *Bulletin physique et mathématique de Saint-Pétersbourg*, t. XVI, 1857.

ordre primitif, et qu'elles reviennent périodiquement à l'une des places qu'elles occupent pendant les battements successifs.

Au premier rang, par exemple, viennent se placer périodiquement, dans un certain ordre, soit toutes les autres cartes, soit un certain nombre d'entre elles.

Cette période n'est pas la même en général pour tous les rangs. Parfois, certaines cartes restent immobiles. Ces faits singuliers et variables suivant le nombre $m = 2n$ méritent d'être expliqués. Ils se rattachent, comme on le verra, à la théorie des nombres.

Voici trois tableaux de ces battements successifs qui montrent bien les particularités dont nous venons de parler.

1° $m = 10$.

1	2	3	4	5	6	7	8	9	10
10	8	6	4	2	1	3	5	7	9
9	5	1	4	8	10	6	2	3	7
7	2	10	4	5	9	1	8	6	3
3	8	9	4	2	7	10	5	1	6
6	5	7	4	8	3	9	2	10	1
1	2	3	4	5	6	7	8	9	10

2° $m = 14$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
14	12	10	8	6	4	2	1	3	5	7	9	11	13
13	9	5	1	4	8	12	14	10	6	2	3	7	11
11	3	6	14	8	1	9	13	5	4	12	10	2	7
7	10	4	13	1	14	3	11	6	8	9	5	12	2
2	5	8	11	14	13	10	7	4	1	3	6	9	12
12	6	1	7	13	11	5	2	8	14	10	4	3	9
9	4	14	2	11	7	6	12	1	13	5	8	10	3
3	8	13	12	7	2	4	9	14	11	6	1	5	10
10	1	11	9	2	12	8	3	13	7	4	14	6	5
5	14	7	3	12	9	1	10	11	2	8	13	4	6
6	13	2	10	9	3	14	5	7	12	1	11	8	4
4	11	12	5	3	10	13	6	2	9	14	7	1	8
8	7	9	6	10	5	11	4	12	3	13	2	14	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14

3° $m = 22$.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
22	20	18	16	14	12	10	8	6	4	2	1	3	5	7	9	11	13	15	17	19	21
21	17	13	9	5	1	4	8	12	16	20	22	18	14	10	6	2	3	7	11	15	19
19	11	3	6	14	22	16	8	1	9	17	21	13	5	4	12	20	18	10	2	7	15
15	2	18	12	5	21	9	8	22	6	11	19	3	14	16	1	17	13	4	20	10	7
7	20	13	1	14	19	6	8	21	12	2	15	18	5	9	22	11	3	16	17	4	10
10	17	3	22	5	15	12	8	19	1	20	7	13	14	6	21	2	18	9	11	16	4
4	11	18	21	14	7	1	8	15	22	17	10	3	5	12	19	20	13	6	2	9	16
16	2	13	19	5	10	22	8	7	21	11	4	18	14	1	15	17	3	12	20	6	9
9	20	3	15	14	4	21	8	10	19	2	16	13	5	22	7	11	1	18	17	12	6
6	17	18	7	5	16	19	8	4	15	20	9	3	14	21	10	2	13	22	11	1	12
12	11	13	10	14	9	15	8	16	7	17	6	18	5	19	4	20	3	21	2	22	1
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22

Dans le premier cas, nous observerons :

Une période de six termes (1, 10, 9, 7, 3, 6);

Une période de trois termes (2, 8, 5);

Une période monôme (4).

Dans le second cas, nous ne trouvons qu'une période de quatorze termes.

Dans le troisième, nous observons :

Une période de douze termes (1, 22, 21, 19, 15, 7, 10, 4, 16, 9, 6, 12);

Une période de quatre termes (2, 20, 17, 11);

Une période de trois termes (3, 18, 13);

Une période de deux termes (5, 14);

Une période monôme (8).

Les exemples que nous venons de donner serviront de vérification expérimentale pour les théorèmes qui suivent.

5. Théorème. — *Après la répétition d'un nouveau battement semblable sur les objets disposés comme l'indique la seconde ligne, on trouvera, au-dessous de chaque numéro de la seconde ligne, les nombres qu'il y avait au-dessous des mêmes numéros de la première ligne.*

Supposons que le numéro A de la seconde ligne soit sous le numéro B de la première, et que B de la seconde soit sous le numéro C de la première. Ces deux lignes présenteront l'aspect suivant après le premier battement :

Première ligne..................	B	...	C
Deuxième ligne..	A	...	B

Faisons un nouveau battement : comme sous C de la première ligne il y a B, sous B qui joue le rôle de C il y aura A qui joue le rôle de B. C. Q. F. D.

Corollaire. — Il suit de là qu'on peut écrire immédiatement les résultats des battements successifs, quand on s'est donné la peine d'écrire les résultats du premier battement. C'est le procédé que nous avons suivi pour former les tableaux précédents.

6. Théorème. — *On retombe nécessairement sur la première disposition au bout d'un nombre limité d'opérations.*

Le battement de Monge équivaut à une substitution. Or toute substitution est décomposable en un certain nombre de substitutions circulaires. Considérons, par exemple, le cas de $m = 10$. Le battement de Monge donne la substitution

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 8 & 6 & 4 & 2 & 1 & 3 & 5 & 7 & 9 \end{matrix}$$

Prenons l'élément 1 ; il remplace 6, qui remplace 3, qui remplace 7, qui remplace 9, qui remplace 10, qui remplace 1. Nous trouvons donc déjà une substitution circulaire que nous désignerons par

$$(1 \quad 6 \quad 3 \quad 7 \quad 9 \quad 10)$$

en entendant que chaque élément remplacera le suivant, et qu'après la substitution leur ensemble présentera la disposition

$$(10 \quad 1 \quad 6 \quad 3 \quad 7 \quad 9).$$

Prenons maintenant l'un des éléments, 2, qui n'entre pas dans cette suite ; cet élément remplace 5, qui remplace 8, qui remplace 2. Donc, nous trouvons encore la substitution circulaire

$$(2 \quad 5 \quad 8).$$

Enfin, 4 reste à la même place et se substitue à lui-même; donc, enfin, le battement de Monge est équivalent à l'ensemble des trois substitutions circulaires suivantes :

$$(1\ 6\ 3\ 7\ 9\ 10),\quad (2\ 5\ 8),\quad (4),$$

et l'on peut s'assurer, en effet, qu'en effectuant successivement ces permutations circulaires, on retombe sur les résultats donnés par le battement de Monge.

Le même raisonnement s'applique à une substitution quelconque d'un nombre quelconque d'éléments; donc il est prouvé que *le battement de Monge est toujours décomposable en substitutions circulaires.*

Cela posé, soient α, β, γ, ... les nombres respectifs des éléments que contient chacune de ces substitutions élémentaires; désignons par μ le plus petit multiple commun de ces nombres. Après μ opérations, on retombera sur la disposition primitive; car, dans chaque groupe circulaire, il faut faire autant d'opérations qu'il y a d'éléments pour revenir à la disposition primitive.

Remarque. — Dans les tableaux formés ci-dessus, on voit que le nombre des termes de chaque période est un diviseur du nombre des termes de la période qui commence par 1. C'est une loi générale dont nous donnerons la raison plus loin.

7. Théorème. — *Dans le tableau des battements, si, à partir de la première ligne reproduite, on lit de bas en haut les nombres des colonnes verticales, on obtient les places successives occupées par le nombre dont on est parti.*

Pour fixer les idées, considérons le tableau relatif à $m = 10$.

$m = 10.$

1	2	3	4	5	6	7	8	9	10
10	8	6	4	2	1	3	5	7	9
9	5	1	4	8	10	6	2	3	7
7	2	10	4	5	9	1	8	6	3
3	8	9	4	2	7	10	5	1	6
6	5	7	4	8	3	9	2	10	1
1	2	3	4	5	6	7	8	9	10
...	...	...	...	...	...	...	...	...	...

La première colonne, lue de bas en haut, donne

$$1 \quad 6 \quad 3 \quad 7 \quad 9 \quad 10;$$

il s'agit de prouver que ces divers nombres indiquent les places successives occupées par 1.

1° *Un* étant sous 6, après le premier battement, occupera donc le sixième rang après ce battement.

2° Après le premier battement 6 va sous 3, et comme 1 va sous 6 après le second battement, comme après le premier le groupe $\left|\begin{matrix}6\\1\end{matrix}\right|$ se trouvera sous 3, après le second battement, donc 1 occupera le troisième rang.

3° 3 va sous 7 après le premier battement, après le second 6 va sous 3, après le troisième 1 va sous 6; donc, après ce troisième battement le groupe $\left|\begin{matrix}3\\6\\1\end{matrix}\right|$ se trouvera sous 7; donc 1 occupera le septième rang, etc. Le théorème est donc démontré.

Nous appellerons *période* d'un battement la série des places occupées par un même élément, et nous placerons cet élément au commencement de cette série, puisque c'est la première place qu'il occupe.

On obtient les périodes *mécaniquement* comme l'indique le théorème. Le terme au-dessous du terme de la première ligne d'où l'on part est donc le dernier terme de la période.

8. Problème. — *Trouver la formule du terme qui se trouve au-dessous d'un terme donné de la première ligne après un battement.*

1° Soit $n+1-p$ un terme de la première ligne. Si $p=1$, le terme situé au-dessous est 2; si $p=2$, le terme situé au-dessous est 4, etc. Donc, si p est quelconque différent de zéro, le terme situé au-dessous est $2p$.

2° Soit $n+1+p$ un terme de la première ligne; si $p=0$, le terme situé au-dessous est 1; si $p=1$, le terme situé au dessous est 3, etc. Si p est quelconque, positif, entier ou nul, le terme situé au-dessous est $2p+1$. Le tableau suivant résume le théorème :

$$\begin{array}{ll} n+1-p, \quad (p>0), & n+1+p, \quad (p \geq 0), \\ 2p, & 2p+1. \end{array}$$

Corollaire I. — Si nous lisons ce tableau de bas en haut, nous obtenons, d'après le théorème précédent, les rangs successifs occupés par un élément. Donc, après un battement,

L'élément $2p$ occupe le rang $n+1-p$.

L'élément $2p+1$ occupe le rang $n+1+p$.

Corollaire II. — Posons $n+1-p=q$, d'où nous tirons

$$p=n+1-q.$$

Le nombre situé au-dessous est $2n+2-2q$, ou $m+2-2q$, et q est au plus égal à n.

Posons de même $n+1+p=q$; d'où $p=q-n-1$. Le nombre situé au-dessous est $2q-2n-1$ ou $2q-m-1$; q est toujours supérieur à n.

Le tableau suivant peut donc remplacer celui ci-dessus :

$q \leq n$,	$q>n$,
$m+2-2q$,	$2q-m-1$.

9. Problème. — *Le battement de Monge peut-il présenter une période monôme? Dans quel cas? Quelle est la formule de ce monôme invariable de position?*

1° On ne peut pas avoir

$$2p+1=n+1+p,$$

car on en déduirait $p=n$, et, par suite, le terme invariable serait $2n+1$, ce qui est impossible.

2° On peut avoir

$$2p=n+1-p;$$

on en déduit

$$p=\frac{n+1}{3}.$$

Donc, n est l'un des nombres de la suite

$$n=2,\quad 5,\quad 8,\quad 11,\quad 14,\quad 17,\quad 20,\quad 23,\quad 26,\quad \ldots,$$

par suite m l'un des nombres de la suite :

$$m = 4, \quad 10, \quad 16, \quad 22, \quad 28, \quad 34, \quad 40, \quad 46, \quad 52, \quad \ldots.$$

La formule du terme invariable est $2p = \frac{m+2}{3}\cdot$ Suivant les cas, on aura

$$2p = 2, \quad 4, \quad 6, \quad 8, \quad 10, \quad 12, \quad 14, \quad 16, \quad 18, \quad \ldots.$$

On peut vérifier facilement l'exactitude de ces résultats.

10. Problème. — *Étant donné le rang v_1 d'un objet dans une première disposition, trouver le rang v_2 qu'il occupera après le battement.*

1° Si $v_1 = 2p$ après le premier battement, cet élément sera le $p^{\text{ième}}$ objet à gauche de $n+1$; donc il occupera le rang

$$v_2 = n + 1 - p = n + 1 - \frac{v_1}{2}\cdot$$

2° Si $v_1 = 2p+1$ après le premier battement, cet élément impair occupera le rang

$$v_2 = n + 1 + p = n + 1 + \frac{v_1 - 1}{2}\cdot$$

Nous retombons sur des résultats trouvés au n° **8**.

Le tableau suivant résume la solution de ce problème :

$$\begin{array}{ll} v_1 = 2p, & v_1 = 2p+1, \\ v_2 = n+1-p, & v_2 = n+1+p. \end{array}$$

Corollaire. — Des formules ci-dessus, on tire

Pour le premier cas : $2(2v_2 - 1) = 4n + 1 - (2v_1 - 1)$,

Pour le second cas : $2(2v_2 - 1) = 4n + 1 + (2v_1 - 1)$.

Donc, en posant

$$2v_1 - 1 = V_1, \quad 2v_2 - 1 = V_2, \quad 4n + 1 = 2m + 1 = N,$$
$$\varepsilon = (-1).$$

Ces deux formules se réduisent à la formule unique

$$(A) \qquad 2V_2 = N - \varepsilon^{\nu_1} V_1.$$

11. Problème. — *Peut-il y avoir des périodes binômes? A quelles conditions? Quelles sont les formules des termes constituant de pareilles périodes?*

Désignons par i un nombre impair et par ϖ un nombre pair. La période binôme ne peut avoir que l'une des quatre formules suivantes :

$$(i, i), \quad (i, \varpi), \quad (\varpi, i), \quad (\varpi, \varpi).$$

Si l'on trouve une période (i, ϖ), on trouvera la période (ϖ, i) avec les mêmes nombres, évidemment. Donc, en réalité, la période binôme ne peut présenter que l'une des trois formes suivantes :

$$(i, i), \quad (i, \varpi), \quad (\varpi, \varpi).$$

1° La première forme est impossible, car elle conduirait aux équations

$$2p + 1,$$

$$n + 1 + p = 2p_1 + 1,$$

$$n + 1 + p_1 = 2p + 1,$$

d'où l'on tire

$$3n + p = 4p,$$

par suite

$$p = n,$$

d'où l'on conclurait que le premier terme de cette période est $2n + 1$, ce qui est impossible.

2° La seconde forme conduit aux équations

$$n + 1 - p = 2p_1,$$

$$n - 1 + p_1 = 2p + 1,$$

d'où l'on tire

$$2p + 1 = \frac{m + 3}{5},$$

$$2p_1 = \frac{3m + 4}{5}.$$

On voit par ces formules que m ne peut avoir que l'une des valeurs suivantes :

$$m = 2,\ 12,\ 22,\ 32,\ 42,\ 52,\ \ldots.$$

Les termes correspondants de la période binôme sont

$$\begin{aligned} 2p+1 &= 1,\quad 3,\quad 5,\quad 7,\quad 9,\quad 11, \\ 2p_1 &= 2,\quad 8,\quad 14,\quad 20,\quad 26,\quad 32. \end{aligned}$$

3° Une période binôme de la forme (ϖ, ϖ) est une période monôme ; car, des équations auxquelles elle conduit,

$$\begin{aligned} n+1-p &= 2p_1, \\ n+1-p_1 &= 2p, \end{aligned}$$

on tire

$$2p = 2p_1 = \frac{m+2}{3}.$$

Remarque. — On trouverait facilement les équations qui conduiraient à la connaissance des périodes trinômes, quatrinômes, etc., de diverses formes. Ces recherches assez laborieuses peuvent être abrégées par la solution du problème suivant et par les conséquences qu'on en tire :

1° Problème. — *Quel est le nombre minimum de battements au bout desquels on retombera sur la première disposition?*

Pour résoudre ce problème difficile, je me servirai de la formule trouvée dans le corollaire du problème n° **10**.

Après p battements, on obtient la série des équations

$$\begin{aligned} 2V_2 &= N - \varepsilon^{\nu_1} V_1, \\ 2V_3 &= N - \varepsilon^{\nu_2} V_2, \\ 2V_4 &= N - \varepsilon^{\nu_3} V_3, \\ 2V_5 &= N - \varepsilon^{\nu_4} V_4, \\ &\ldots\ldots\ldots\ldots\ldots\ldots, \\ 2N_{p+1} &= N - \varepsilon^{\nu_p} V_p. \end{aligned}$$

De là nous tirons, par substitutions successives,

$$2^p V_{p+1} = \left(2^{p-1} - 2^{p-2}\varepsilon^{\nu_p} + 2^{p-3}\varepsilon^{\nu_{p-1}+\nu_p} - 2^{p-4}\varepsilon^{\nu_{p-2}+\nu_{p-1}+\nu_p} + \ldots - \varepsilon^{p+\nu_2+\nu_3+\ldots+\nu_p}\right)N + \varepsilon^{p+\nu_1+\nu_2+\ldots+\nu_p} V_1.$$

Mais, si, après ces p battements, ν_1 a repris sa première place, on a $V_{p+1} = V$; donc

$$(2^p - \varepsilon^{p+\nu_1+\nu_2+\ldots+\nu_p})V_1 = (2^{p-1} - 2^{p-2}\varepsilon^{\nu_p} + 2^{p-3}\varepsilon^{\nu_{p-1}+\nu_p} - \ldots - \varepsilon^{p+\nu_2+\nu_3+\ldots+\nu_p})N.$$

La parenthèse du second membre est un nombre entier : donc N est un diviseur du premier membre. On voit déjà que la plus grande valeur de p, ou la plus longue période, s'obtiendra en supposant $V_1 = 1$ ou $\nu_1 = 1$.

Pour nous débarrasser de la considération des valeurs $\nu_2, \nu_3, \ldots, \nu_p$ intermédiaires, remarquons que

$$2^p - \varepsilon^{p+\nu_1+\nu_2+\ldots+\nu_p}$$

est égal à $2^p \pm 1$. Multiplions les deux membres de l'égalité par

$$2^p + \varepsilon^{p+\nu_1+\nu_2+\ldots+\nu_p},$$

il viendra

$$(2^{2p} - 1)V_1 = \mathfrak{M}N,$$

ou bien

$$(4^p - 1)V_1 = \mathfrak{M}N,$$

ou bien

$$(2^p - 1)(2^p + 1)V_1 = \mathfrak{M}N,$$

d'où l'on voit que l'on est ramené à chercher la plus petite valeur de p, qui rend $(4^p - 1)V_1$ divisible par N.

Cette valeur de p étant trouvée, on s'assurera que l'un ou l'autre des produits

$$(2^p - 1)V_1, \quad (2^p + 1)V_1$$

est divisible par N. Si l'un d'eux est divisible par N, la valeur de p est trouvée. Si aucun n'est divisible par N, le produit $(2^{2p} - 1)V_1$ l'est par hypothèse; donc la période est $2p$.

Corollaire. — Pour trouver la période relative à $v_1 = V_1 = 1$, il faut chercher la plus petite valeur de p qui rend

$$4^p - 1$$

divisible par $N = 2m + 1$. Cette valeur de p étant trouvée, on cherchera si l'un des facteurs

$$2^p - 1, \quad 2^p + 1$$

est divisible par N. Si l'un de ces facteurs est divisible, la valeur trouvée pour p est la période. Si aucun de ces facteurs n'est divisible par N, la période est $2p$, puisque $2^{2p} - 1$ est divisible par N, par hypothèse.

Premier exemple. — Soit $m = 22$, d'où $N = 45$.

Cherchons les restes successifs que les puissances de 4 donnent quand on les divise par 45; nous trouvons

$$4 \quad 16 \quad 19 \quad 31 \quad 34 \quad 1.$$

Donc la première puissance de 4 qui, diminuée de 1, est divisible par 45, est la sixième.

Cherchons maintenant les restes donnés par les diverses puissances de 2 pour le même diviseur; nous trouvons

$$2 \quad 4 \quad 8 \quad 16 \quad 32 \quad 19 \quad 38 \quad 31 \quad 17 \quad 34 \quad 23 \quad 1.$$

Donc ni $2^6 - 1$, ni $2^6 + 1$ ne sont divisibles par 45; donc la période relative à l'élément 1 est 12.

Deuxième exemple. — Soit $m = 28$, d'où $N = 57$.

Les restes successifs des puissances de 4 divisées par 57 sont

$$4 \quad 16 \quad 7 \quad 28 \quad 55 \quad 49 \quad 25 \quad 43 \quad 1.$$

Les restes successifs des puissances de 2 divisées par 57 sont

$$2 \quad 4 \quad 8 \quad 16 \quad 32 \quad 7 \quad 14 \quad 28 \quad -1.$$

Donc 2^9+1 est divisible par 57, donc la période relative à 1 a neuf chiffres, ce qu'on peut vérifier expérimentalement.

13. Théorème. — *Si l'on désigne par* $\varphi(\mathrm{N})$ *le nombre des entiers premiers à* N *et inférieurs à lui, la période relative à* $v_1 = 1$ *est égale à* $\varphi(\mathrm{N})$ *ou à un sous-multiple de ce nombre.*

En effet, N étant impair est premier avec 4 : donc, d'après le théorème de Fermat généralisé, on a

$$4^{\varphi(\mathrm{N})} - 1 = \mathfrak{M}\mathrm{N};$$

et, comme les restes des puissances d'un nombre se reproduisent périodiquement, $\varphi(\mathrm{N})$ est la plus petite valeur de la puissance de 4 congrue à 1, ou bien un multiple de cette valeur minima. C. Q. F. D.

Ainsi, par exemple, soit $m = 12$ et $\mathrm{N} = 25$. Nous trouvons

$$\varphi(25) = \varphi(5^2) = 5.4 = 20.$$

Donc la première période est 20, ou un diviseur de 20; nous voyons expérimentalement qu'elle est 10.

14. Théorème. — *Si, décomposé en facteurs premiers,* N *donne*

$$\mathrm{N} = a^\alpha b^\beta c^\gamma,$$

et si l'on designe par μ *le plus petit commun multiple des nombres*

$$\varphi(a^\alpha),\ \varphi(b^\beta),\ \varphi(c^\gamma),$$

la première période sera μ *ou un diviseur de* μ.

En effet on a, d'après le théorème de Fermat,

$$2^{\varphi(a^\alpha)} - 1 = \mathfrak{M}a^\alpha,$$
$$2^{\varphi(b^\beta)} - 1 = \mathfrak{M}b^\beta,$$
$$2^{\varphi(c^\gamma)} - 1 = \mathfrak{M}c^\gamma;$$

donc

$$2^\mu - 1$$

sera aussi divisible par a^α, b^β, c^γ, et, comme ces nombres sont premiers entre eux, il sera divisible par leur produit, et l'on peut poser

$$2^\mu - 1 = \mathfrak{M}N.$$

μ peut n'être pas la plus petite puissance de 2 congrue à 1, et l'on peut avoir trouvé une puissance de 2 inférieure congrue à -1; mais ces puissances sont des sous-multiples de μ; donc le théorème est démontré.

Si, par exemple, $m = 52$, d'où $N = 105$, nous trouverons

$$N = 3.5.7,$$

donc

$$\varphi(3) = 2, \quad \varphi(5) = 4, \quad \varphi(7) = 6;$$

par suite,

$$\mu = 12.$$

La première est 12 ou un sous-multiple. Nous pouvons vérifier expérimentalement qu'elle est 12.

Le théorème que nous venons de démontrer assigne une limite supérieure facile à trouver du nombre de termes de la première période.

15. Théorème. — *Si m est la forme*

$$m = 2^\alpha,$$

la première période a $\alpha + 1$ termes.

En effet, nous avons vu qu'un nombre impair $2p + 1$ occupe le rang $1 + n + p$ après un battement. Donc les rangs successifs occupés par 1 seront, dans ce cas,

$$\begin{aligned}
&1,\\
&1 + 2^{\alpha-1},\\
&1 + 2^{\alpha-1} + 2^{\alpha-2},\\
&1 + 2^{\alpha-1} + 2^{\alpha-2} + 2^{\alpha-3},\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&1 + 2^{\alpha-1} + 2^{\alpha-2} + \ldots + 2 + 1 = 2^\alpha.
\end{aligned}$$

Arrivés là, nous avons le nombre impair; 2^α le rang suivant sera 1. Donc la période a bien $\alpha + 1$ termes. C. Q. F. D.

On peut en conclure que, pour

$$m = 4 \quad 8 \quad 16 \quad 32 \quad 64 \quad \ldots,$$

les premières périodes ont respectivement

$$3 \quad 4 \quad 5 \quad 6 \quad 7 \quad \ldots$$

termes.

16. Théorème. — *Toute période du battement de Monge a un nombre de termes qui divise le nombre des termes de la première période relative à* 1.

Reprenons l'équation du problème du n° **12**,

$$(4^p - 1)V_1 = \mathfrak{M}N.$$

Supposons que Δ soit le plus grand commun diviseur des nombres V_1 et N; posons

$$V_1 = \Delta V'_1, \quad N = \Delta N'.$$

L'équation donnera

$$(4^p - 1)V'_1 = \mathfrak{M}N',$$

N' étant premier avec V'_1 devra diviser $4^p - 1$: donc on sera ramené à trouver la première puissance de 4, qui, diminuée de 1, sera divisible par N', diviseur de N. La période demandée sera cette puissance ou le double. Cette puissance sera au plus égale à celle qui a été trouvée pour le cas de $V_1 = 1$; donc déjà nous pouvons affirmer qu'il n'y a pas de période plus longue que la première.

Mais nous pouvons aller plus loin.

Soit p le nombre trouvé pour le cas de $V_1 = 1$, de telle sorte que l'on ait

$$4^p - 1 = \mathfrak{M}N = \mathfrak{M}\Delta N' = \mathfrak{M}N'.$$

Soit p' le nombre trouvé pour le cas de $V_1 > 1$, de telle sorte que

$$4^{p'} - 1 = \mathfrak{M}N'.$$

Nous avons nécessairement

$$p = p'q,$$

q pouvant être égal à l'unité.

1° Si $q \geqq 2$, la période relative à v_1 a p' termes ou $2p'$ termes, et, comme la première période a p termes ou $2p$, on voit que le nombre des termes de la première période est bien un multiple du nombre des termes de la période relative à v_1.

2° Si $q = 1$, on a

$$p = p'.$$

Le nombre p' sera le nombre des termes de la période relative à 1, si l'un des deux facteurs

$$2^{p'} - 1 = 2^p - 1, \quad 2^{p'} + 1 = 2^p + 1$$

est divisible par N'; dans le cas contraire, ce sera $2p'$.

De même, p sera le nombre des termes de la première période si l'un de ces deux facteurs est divisible par N : ce sera $2p$ dans le cas contraire.

Or, si l'un de ces deux facteurs est divisible par N, il le sera nécessairement par N', diviseur de N; donc le nombre des termes de la première période sera, dans ce cas, égal au nombre des termes de la période relative à V_1.

Mais il peut arriver qu'aucun de ces deux facteurs ne soit divisible par N, et que cependant l'un des deux soit divisible par N'; dans ce cas, la période relative à 1 a $2p$ termes, et la période relative à V_1 a $p' = p$. Donc encore le nombre des termes de la première période est un multiple du nombre des termes de la période relative à V_1.

C. Q. F. D.

17. PROBLÈME. — *Trouver les nombres de termes des diverses périodes d'un battement déterminé.*

Premier exemple. — Proposons-nous de trouver les diverses périodes du battement relatif à $m = 22$.

Nous formons le Tableau suivant :

$v_1 =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
$V_1 =$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43
N' =	45	15	9	45	5	45	45	3	45	45	15	45	9	5	45	45	15	9	45	15	45	45
Période =	12	4	3	12	2	12	12	1	12	12	4	12	3	2	12	12	4	3	12	4	12	12

Les nombres de la troisième ligne sont les quotients de la division du nombre N par le plus grand commun diviseur des nombres V_1 et N. Pour avoir le nombre des termes de la période relative à 2, on cherche les restes des diverses puissances de 4 divisées par 15 : la première puissance qui donne 1 pour reste est la deuxième, et, comme 2^2+1 et 2^2-1 ne sont ni l'un ni l'autre divisibles par 15, la période a quatre termes. On trouve de même les nombres de termes de toutes les autres.

Deuxième exemple. — Soit encore $m = 52$; nous formons sans peine le Tableau suivant :

$v_1 =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
$V_1 =$	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51
$N' =$	105	35	21	15	35	105	105	7	105	105	5	105	21	35	105	105	35	3	105	35	105	105	7	105	15	35
Période =	12	12	6	4	12	12	12	3	12	12	2	12	6	12	12	12	12	1	12	12	12	12	3	12	4	12

$v_1 =$	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52
$V_1 =$	53	55	57	59	61	63	65	67	69	71	73	75	77	79	81	83	85	87	89	91	93	95	97	99	101	103
$N' =$	105	21	35	105	105	5	21	105	35	105	105	–	15	105	35	105	21	35	105	105	35	21	105	35	105	105
Période =	12	6	12	12	12	2	6	12	12	12	12		4	12	12	12	6	12	12	12	12	6	12	12	12	12

Remarque. — Le procédé que nous venons d'employer dispense d'écrire même le résultat matériel d'un seul battement. Toutefois il est moins rapide que celui qui consiste à faire un battement et à partager la substitution en substitutions circulaires, comme nous l'avons indiqué au n° **6**.

Dans le cas de 52 cartes, la substitution qu'indique le battement de Monge équivaut à la suite des substitutions circulaires :

(1 27 40 7 30 12 21 37 45 49 51 52),
(2 26 14 20 17 35 44 5 29 41 47 50),
(3 28 13 33 43 48),
(4 25 39 46),
(6 24 15 34 10 22 16 19 36 9 31 42),
(8 23 38),
(11 32),
(18).

Ce Tableau fait connaître immédiatement le nombre des termes de chaque période ; mais il faut dire qu'il ne donne pas la raison cachée de la périodicité. Cette raison se trouve, en réalité, dans le théorème du n° **16** et le problème du n° **17**.

18. Dans son Opuscule, M. Thomas de Saint-Laurent affirme que le premier terme de chaque période, le plus faible, peut être mis sous la forme

$$\frac{m+y}{2y-1},$$

y étant un nombre entier. L'auteur ne démontre pas cette proposition, il y arrive par induction. Il est facile de voir qu'elle est erronée.

Dans le cas de $m = 52$, considérons la période de 12 termes commençant par 6. Si nous posons

$$\frac{m+y}{2y-1} = 6,$$

nous en tirerons

$$11y = 58,$$

et y n'est pas un nombre entier.

Voici le théorème vrai qu'il faut substituer à celui de M. Thomas de Saint-Laurent.

19. Théorème. — *Tout terme v_1 peut être mis sous la forme*

$$\frac{mx+y}{2y-1},$$

x et y étant positifs et entiers, si m et V_1 sont premiers entre eux.

Posons

$$\frac{mx+y}{2y-1} = v_1,$$

nous en tirons

$$mx + v_1 = V_1 y.$$

Nous remarquerons maintenant que, cette égalité ayant lieu, si V_1

et m avaient un facteur premier commun, il diviserait v_1, par suite $2v_1$, par suite $2v_1 - V_1 = 1$, ce qui est impossible; donc cette égalité ne peut avoir lieu que si m et V_1 sont premiers entre eux.

Cela étant, on sait qu'il est possible de trouver un entier x, tel que $v_1 + mx$ soit un multiple de V_1, et cet entier est inférieur à $V_1 - 1$.

Remarque. — Dans le cas où m et V_1 ne seraient pas premiers entre eux, divisons m par le plus grand commun diviseur de ces deux nombres, st soit m' le quotient, qui sera le premier avec V_1. Posons

$$\frac{m'x + y}{2y - 1} = v_1.$$

Nous déduirons de là

$$v_1 + m'x = V_1 y.$$

On pourra toujours trouver un nombre entier x inférieur à V_1, tel que $v_1 + m'x$ sera un multiple de V_1, ce qui fera connaître x et y.

Ce théorème va nous servir à démontrer quelques propriétés remarquables des périodes énoncées par M. Thomas.

20. Théorème. — *Si un élément est invariable pendant le battement, il a après lui deux fois plus d'éléments qu'avant.*

Nous avons trouvé

$$\frac{m+2}{3}$$

pour formule de l'élément invariable. Avant cet élément, il y a

$$\frac{m+2}{3} - 1 = \frac{m-1}{3}$$

éléments.

Après cet élément, il y a

$$m - \frac{m+2}{3} = \frac{2m-2}{3}.$$

Ce dernier nombre est double du premier. C. Q. F. D.

21. Théorème. — *Si l'on considère les objets dans leur première disposition, il y a toujours, après le dernier terme d'une période, deux fois plus d'éléments qu'avant le premier terme.*

En effet, le premier terme d'une période peut toujours se mettre sous la forme

$$\frac{m'x+y}{2y-1}.$$

Avant ce premier terme, il y a

$$\frac{m'x+y}{2y-1}-1=\frac{m'x-y+1}{2y-1}$$

termes.

Cela posé, le premier terme de la période étant $\frac{m'x+y}{2y-1}$ et étant situé nécessairement dans la première moitié de la suite totale, le terme situé au dessous ou le dernier terme de la période sera

$$m+2-\frac{2m'x+2y}{2y-1}.$$

A la suite de ce terme, il y aura

$$m-m-2+\frac{2m'x+2y}{2y-1}=\frac{2m'x-2y+2}{2y-1}$$

termes.

Ce nombre est évidemment double du premier. C. Q. F. D.

22. Théorème. — *Entre l'avant-dernier terme d'une période et le dernier, il y a toujours autant de termes qu'après le dernier.*

Nous venons de voir qu'après le dernier il y a

$$\frac{2m'x-2y+2}{2y-1}$$

termes.

Nous avons trouvé, pour le dernier terme de la période,

$$m+2-\frac{2m'x+2y}{2y-1}.$$

Ce dernier terme est dans la seconde moitié de la série; donc le terme situé au-dessous ou l'avant-dernier de la série sera

$$2m+4-\frac{4m'x+4y}{2y-1}-m-1=m+3-\frac{4m'x+4y}{2y-1}.$$

Entre ce terme et le dernier, il y a un nombre de termes marqué par leur différence moins *un*, ou

$$-2+\frac{2m'x+2y}{2y-1},$$

ou bien

$$\frac{2m'x-2y+2}{2y-1}.$$

Or ce nombre est précisément le nombre des termes qui suivent le dernier. C. Q. F. D.