

MORET-BLANC

**Solution des propositions sur les
nombres de M. C. Moreau**

Nouvelles annales de mathématiques 2^e série, tome 14
(1875), p. 391-396

http://www.numdam.org/item?id=NAM_1875_2_14__391_1

© Nouvelles annales de mathématiques, 1875, 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/>

SOLUTION DES PROPOSITIONS SUR LES NOMBRES

DE M. C. MOREAU

(voir même tome, p. 274);

PAR M. MORET-BLANC.

1. *Connaissant le mode de décomposition en facteurs premiers de l'entier n , trouver le nombre des racines de la congruence*

$$x^2 \equiv 1 \pmod{n}.$$

Cette question est résolue dans l'*Algèbre supérieure* de Serret, n° 292.

Soit m le nombre des facteurs premiers impairs de n . Le nombre des racines de la congruence $x^2 \equiv 1 \pmod{n}$ est 2^m si n est impair ou double d'un impair, 2^{m+1} si n est divisible par 4 et non par 8, et 2^{m+2} si n est multiple de 8.

2. *P désignant le produit de tous les nombres inférieurs à un nombre n et premiers avec lui, indiquer quels sont les cas où n divise $P + 1$.*

Quand n est un nombre premier, une puissance d'un nombre premier ou le double d'une telle puissance, ou enfin quand il est égal à 4 (théorème de Wilson généralisé). (Voir l'*Algèbre supérieure* de Serret, n° 296.)

3. *Soient $a, b, \dots, l$ les différents facteurs qui entrent dans la composition de l'entier n , et m le plus petit commun multiple des nombres $\frac{n}{2ab\dots l}$, $a - 1$,*

$b-1, \dots, l-1$; montrer que tout nombre premier avec n satisfait à la congruence

$$x^m \equiv 1 \pmod{n}.$$

Si $\varphi(n)$ indique combien il y a de nombres premiers avec n et non supérieurs à n , x étant premier avec n , on a

$$x^{\varphi(n)} \equiv 1 \pmod{n},$$

théorème de Fermat généralisé par Euler (SERRET, *Alg. sup.*, n° 296, ou LE BESGUE, *Introduction à la théorie des nombres*, n° 41).

Si n est un nombre premier $\varphi(n) = n-1$, et si n est une puissance d'un nombre premier a , $n = a^\alpha$, $\varphi(n) = (a-1)a^{\alpha-1}$.

De plus, si l'on a $x^m \equiv 1 \pmod{n}$, on aura aussi $x^{km} \equiv 1 \pmod{n}$, k étant un nombre entier positif quelconque. Cela posé, soit $n = a^\alpha b^\beta \dots l^\lambda$.

$x^m - 1$ sera divisible par n , s'il l'est séparément par les nombres premiers entre eux $a^\alpha, b^\beta, \dots, l^\lambda$; c'est-à-dire si m est un multiple de $(a-1)a^{\alpha-1}, (b-1)b^{\beta-1}, \dots, (l-1)l^{\lambda-1}$, ou, ce qui revient au même, puisque $a^{\alpha-1}, b^{\beta-1}, \dots, l^{\lambda-1}$ sont premiers entre eux, un multiple de $a^{\alpha-1}b^{\beta-1}l^{\lambda-1} = \frac{n}{ab\dots l}$ et de $a-1, b-1, l-1$.

Toutefois, si l'un des facteurs, a par exemple, est égal à 2, on a, n étant impair.

$$x^2 = 8k + 1, \quad x^4 = 16k + 1, \quad x^8 = 32k + 1, \dots,$$

et, en général,

$$x^{2^{n-2}} \equiv 1 \pmod{2^n};$$

donc, si n est multiple de 8, on pourra remplacer

$$\frac{n}{ab\dots l} \quad \text{par} \quad \frac{n}{2ab\dots l}.$$

Il en sera de même si n est multiple de 4, pourvu qu'il y ait un autre facteur premier impair dont l'excès sur l'unité restituera le facteur 2, nécessaire pour que $x^n - 1$ soit divisible par 4.

Si n est un nombre pair non divisible par 4, $\frac{n}{2ab\dots l}$ est fractionnaire.

On pourra donc prendre pour m le plus petit multiple commun des nombres $\frac{n}{2ab\dots l}$, $a - 1$, $b - 1, \dots, l - 1$, toutes les fois que $\frac{n}{2ab\dots l}$ sera entier, excepté pour $n = 4$.

4. n étant un entier positif quelconque, démontrer l'égalité

$$1.2.3\dots n = \sum_{k=0}^{k=n} (-1)^k \frac{n(n-1)\dots(n-k+1)}{1.2.3\dots k} (m-k+1)^n.$$

L'égalité développée s'écrit

$$1.2.3\dots n = (m+1)^n \frac{n}{1} m^n + \frac{n(n-1)}{1.2} (m-1)^n - \dots \pm (m+1-n)^n.$$

Les deux membres représentent chacun la $n^{\text{ième}}$ différence de la fonction $(x+1-n)^n$, dans laquelle on donne successivement à x les $n+1$ valeurs $m, m+1, \dots, m+n$. L'égalité est donc démontrée.

5. Quels que soient les entiers positifs m, n, p , on a

$$0 = \sum_{k=0}^{k=n} (-1)^k \frac{n(n-1)\dots(n-k+1)}{1.2.3\dots k} \times (m+kp)(m+kp-1)\dots(m+kp-n+2).$$

Développons

$$\begin{aligned}
0 &= m(m-1) \dots (m-n+2) \\
&\quad - \frac{n}{1} (m+p)(m+p-1) \dots (m+p-n+2) \\
&\quad + \frac{n(n-1)}{1 \cdot 2} (m+2p)(m+2p-1) \dots (m+2p-n+2) \dots \\
&\quad \pm (m+np)(m+np-1) \dots (m+np-n+2).
\end{aligned}$$

Le second membre représente $\pm$ la $n^{\text{ième}}$ différence de la fonction

$$x(x-1)(x-2) \dots (x-n+2),$$

dans laquelle on donne successivement à x les valeurs $m, m+p, m+2p, \dots, m+np$; or, cette fonction étant du degré $n-1$, sa différence $n^{\text{ième}} = 0$; donc, etc.

6. *On tire successivement des boules d'une urne qui en contient m , toutes différentes, et avant chaque tirage on remet dans l'urne la boule qui a été extraite au tirage précédent. Quelle est, dans ces conditions, la probabilité d'amener p fois de suite la même boule avant que pas une des q boules désignées à l'avance ne soit sortie.*

En faisant dans la formule trouvée $m=13$, $p=4$, $q=2$, on aura la chance du coup appelé lansquenet au jeu qui porte ce nom, en se servant d'un nombre infini de jeux de cartes. Cette chance est $\frac{1}{4771} = 0,0023$ environ.

Désignons par A les boules dont l'une doit sortir p fois de suite, et par b celles qui ne doivent pas sortir.

La série des p tirages consécutifs amenant la même boule A peut commencer au premier, au deuxième, au

troisième, etc., tirage, et la probabilité de l'événement désigné est la somme des probabilités correspondant à ces différents cas, sans qu'aucune boule B ne sorte.

Premier cas. — La probabilité qu'une boule A sorte au premier tirage est $\frac{m-q}{m}$, la probabilité de la sortie de cette même boule à chacun des tirages suivants est $\frac{1}{m}$ pour chaque tirage, et, par suite, la probabilité de p tirages consécutifs d'une boule A commençant au premier est $\frac{m-q}{m^p}$.

Deuxième cas. — La probabilité de la sortie d'une boule A au premier tirage suivie de la sortie d'une autre boule A au second tirage est $\frac{(m-q)(m-q-1)}{m^2}$. La probabilité de la sortie d'une boule A à p tirages consécutifs commençant au second est donc $\frac{(m-q)(m-q-1)}{m^{p+1}}$.

Troisième cas. — La probabilité que les deux premiers tirages amèneront des boules A est $\frac{(m-q)^2}{m^2}$; la probabilité de la sortie au troisième tirage d'une boule A différente de celle qui est sortie au second est $\frac{m-q-1}{m}$; on a donc, pour la probabilité de ces trois événements, $\frac{(m-q)^2(m-q-1)}{m^3}$, et, pour la probabilité de p tirages consécutifs d'une même boule A commençant au troisième,

$$\frac{(m-q)^2(m-q-1)}{m^{p+2}},$$

et ainsi de suite.

La probabilité d'amener p fois de suite une même boule A, avant que pas une des boules B ne soit sortie, est

donc

$$\begin{aligned}
 & \frac{m-q}{m^p} + \frac{(m-q)(m-q-1)}{m^{p+1}} + \frac{(m-q)^2(m-q-1)}{m^{p+2}} + \dots \\
 &= \frac{m-q}{m^p} \left\{ 1 + \frac{m-q-1}{m} \left[1 + \frac{m-q}{m} + \frac{(m-q)^2}{m^2} \right. \right. \\
 & \qquad \qquad \qquad \left. \left. + \frac{(m-q)^3}{m^3} + \dots \right] \right\} \\
 &= \frac{m-q}{m^p} \left(1 + \frac{m-q-1}{m} \times \frac{m}{q} \right) = \frac{(m-1)(m-q)}{qm^p}, \\
 & P = \frac{(m-1)(m-q)}{qm^p}.
 \end{aligned}$$

Si, dans cette formule, on fait $m = 13$, $p = 4$, $q = 2$, on a

$$\frac{12.11}{2.13^4} = \frac{66}{13^4} = \frac{66}{28561} = 0,0023 \text{ environ,}$$

valeur à très-peu près, mais non rigoureusement égale à celle que donne M. Moreau.
