**Zeitschrift:** Commentarii Mathematici Helvetici

**Herausgeber:** Schweizerische Mathematische Gesellschaft

**Band:** 12 (1939-1940)

**Artikel:** Les systèmes imprimitifs dans lesquels se répartissent les combinaisons i à i de m éléments par les substitutions du groupe cyclique de degré m.

**Autor:** Bays, S. / Hsia, Chuin-Ché

**DOI:** https://doi.org/10.5169/seals-12809

**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:** 12.12.2025

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

# Les systèmes imprimitifs dans lesquels se répartissent les combinaisons $i$ à $i$ de $m$ éléments par les substitutions du groupe cyclique de degré $m$

Par S. Bays et Chuin-Ché Hsia, Fribourg

**1.** Le nombre des combinaisons des $m$ éléments $0, 1, 2, \ldots m-1$, $i$ à $i$, est $C_m^i$. Si nous appliquons à l'une de ces combinaisons les $n!$ substitutions du groupe *symétrique* des $m$ éléments, nous engendrons successivement toutes les autres. Si nous appliquons à l'une de ces combinaisons un sous-groupe seulement du groupe symétrique, dans notre cas le groupe *cyclique* des $m$ éléments, nous engendrons une partie seulement des $C_m^i$ combinaisons.

Dans un travail antérieur[1]), j'attachais de l'importance à résoudre cette question: En combien de *parties différentes* se répartit l'ensemble des $C_m^i$ combinaisons $i$ à $i$ par le groupe cyclique des $m$ éléments? Cette réponse a toujours son intérêt; elle servirait grandement dans l'établissement de systèmes cycliques de $n$-uples supérieurs, à diverses propriétés, analogues aux systèmes cycliques de triples de Steiner, si l'on ne se butait pas dans la construction de ces systèmes combinatoires à des difficultés considérables. Elle s'exprime en tout cas par des formules dont la simplicité et l'élégance nous paraissent justifier cette publication.

La répartition cherchée est évidemment indépendante du groupe cyclique des $m$ éléments que nous choisissons. Nous prenons la substitution immédiate $s = (0, 1, 2, \ldots, m-1)$ et le groupe cyclique $\{s\}$. Si nous appelons, comme dans le mémoire cité, *colonne cyclique* l'ensemble des combinaisons $i$ à $i$ issu de l'une d'entre elles par les substitutions du groupe $\{s\}$ et *$i$-uple* une combinaison $i$ à $i$, la question posée s'énonce: *En combien de colonnes cycliques différentes se répartissent les $i$-uples des $m$ éléments par les substitutions du groupe $\{s\}$?* Dans un langage plus conforme à la théorie des groupes de substitutions, on a l'énoncé du titre ci-dessus.

La voie pour obtenir la répartition cherchée aurait pu être la constitution même des substitutions du groupe $\{s\}$. Pour qu'une substitution du groupe $\{s\}$ autre que l'identité, change un $i$-uple en lui-même, il *faut* et il

---

[1]) *S. Bays.* — Sur les systèmes cycliques de triples de Steiner différents pour $N$ premier de la forme $6n+1$. Commentarii math. helvetici, vol. 4, pages 187—189.

*suffit* que ce $i$-uple soit constitué exclusivement des éléments de *un* ou *plusieurs* cycles de cette substitution (l. c. p. 189). Mais un essai fait sur cette base conduit à des complications extrêmes. Mr. Ch. Hsia a cherché une voie plus élémentaire et plus simple; c'est celle que nous allons suivre.

**2.** Soit les $m$ éléments $0, 1, 2, \ldots, m-1$ dans l'ordre de la substitution $s$. Nous appellerons *déplacement* le passage de chaque élément au suivant et du dernier au premier. Tout ensemble de $i$ de ces éléments, $1 \leqq i \leqq m$, se retrouve en tout cas identique à lui-même après $m$ déplacements. Il peut se faire qu'il se retrouve identique à lui-même avec *moins* de $m$ déplacements; $m$ étant fixé, cela dépendra de $i$ et pour un même $i$, de la nature de l'ensemble.

*Théorème 1.* Le nombre $\alpha$ *minimum* des déplacements nécessaires pour reproduire un ensemble initial $E_0$ est *diviseur* de $m$. Nous appellerons $\alpha$ le *caractère* de $E_0$.

*Preuve:* Désignons par $E_0, E_1, E_2, \ldots, E_{m-1}, E_0, E_1, \ldots$ la suite des ensembles obtenus de l'ensemble initial $E_0$ par $1, 2, 3, \ldots$ déplacements successifs. Si $\alpha < m$ n'était pas diviseur de $m$, on aurait $m = \alpha q + r$, $0 \leqq r < \alpha$ ; $E_\alpha, E_{2\alpha}, \ldots, E_{q\alpha}$ reproduisent $E_0$. Donc $E_r$ reproduirait $E_0$, ce qui est en contradiction avec l'hypothèse faite sur $\alpha$. Donc c. q. f. d.

**3.** Soit $d$ un diviseur de $m$. Nous disposons les éléments $0, 1, 2, \ldots, m-1$, relativement à $d$, en tableau rectangulaire de la façon suivante:

$$\begin{array}{llll}
0 & 1 & 2 & \cdots \frac{m}{d}-1 \\
\frac{m}{d} & \frac{m}{d}+1 & \frac{m}{d}+2 & \cdots \frac{2m}{d}-1 \\
\cdots & \cdots & \cdots & \cdots \\
\frac{(d-1)m}{d} & \frac{(d-1)m}{d}+1 & \frac{(d-1)m}{d}+2 & \cdots m-1 .
\end{array} \qquad (1)$$

Nous appellerons ce schéma *la division $d$ de $m$*. Les $d$ éléments d'une même colonne de la division seront dits *correspondants*. Chaque colonne de la division est reproduite par $\frac{m}{d}$ déplacements et un élément quelconque, par $\frac{m}{d}$ déplacements, est toujours transformé dans le correspondant qui le suit. Il en résulte sans autre la proposition suivante et son inverse:

*Théorème 2.* Tout ensemble qui contient tous les correspondants de chacun de ses éléments dans la division $d$ de $m$ est reproduit par $\frac{m}{d}$ déplacements. Inversement tout ensemble qui est reproduit par $\frac{m}{d}$ déplacements, doit contenir pour chacun de ses éléments tous les correspondants dans la division $d$ de $m$.

*Remarque:* Les deux propositions du théorème 2 sont valables aussi pour les cas extrêmes $d = 1$ et $d = m$.

Pour $d = 1$, $\frac{m}{d} = m$; la division (1) n'a qu'une ligne; chaque élément est son unique correspondant et les deux propositions sont évidentes.

Pour $d = m$, $\frac{m}{d} = 1$; la division (1) n'a qu'une colonne; les $m$ éléments sont tous correspondants entre eux et les deux propositions sont encore évidentes.

**4.** Il résulte immédiatement du théorème 2, les corollaires suivants:

*Corollaire 1.* Le nombre des ensembles à $i$ éléments (nous dirons pour abréger ensembles *i-uples*) qui se reproduisent par $\frac{m}{d}$ déplacements est $C_{\frac{m}{d}}^{\frac{i}{d}}$.

En effet puisqu'un tel ensemble doit contenir pour chaque élément la colonne entière de la division (1) qui le contient, $d$ doit être *diviseur* de $i$ et le nombre de ces ensembles est le nombre des combinaisons des $\frac{m}{d}$ éléments d'une ligne quelconque fixée de (1), $\frac{i}{d}$ à $\frac{i}{d}$.

Dans le cas $d = 1$, $C_{\frac{m}{d}}^{\frac{i}{d}} = C_m^i$; le nombre des ensembles *i-uples* qui se reproduisent par $m$ déplacements est bien $C_m^i$.

Dans le cas $d = m$, $d$ étant diviseur de $i$, $i = m$; $C_{\frac{m}{d}}^{\frac{i}{d}} = C_1^1 = 1$; le seul ensemble qui se reproduise par 1 déplacement est bien l'ensemble même des $m$ éléments.

*Corollaire 2.* Les diviseurs $d$ qui peuvent intervenir dans la constitution d'ensembles *i-uples* reproduits par $\frac{m}{d}$ déplacements sont donc uniquement

les diviseurs *communs* à $i$ et $m$; si $\delta$ est le p.g.c.d. de $i$ et $m$, ces diviseurs communs sont les diviseurs de $\delta$.

Nous appellerons les ensembles $i$-uples constitués d'après le corollaire 1, par chaque combinaison de $\frac{i}{d}$ éléments pris dans les $\frac{m}{d}$ éléments d'une ligne fixée de (1), les ensembles $i$-uples *fournis* par la division $d$ de $m$, ou qui *appartiennent* à la division $d$ de $m$. Leur ensemble est identique à celui des ensembles $i$-uples qui se reproduisent par $\frac{m}{d}$ déplacements. Il y en a donc $C_{\frac{m}{d}}^{\frac{i}{d}}$.

Nous appellerons les ensembles $i$-uples pour lesquels le caractère $\alpha = \frac{m}{d}$, les ensembles $i$-uples *propres* à la division $d$ de $m$. Ils sont donc reproduits pour la *première* fois par $\frac{m}{d}$ déplacements. Ceux qui sont reproduits pour la première fois par un nombre *moindre* de déplacements et qui appartiennent cependant à la division $d$ de $m$, seront dits *impropres* à la division $d$ de $m$.

5. *Théorème 3.* Soit $d_1$ et $d_2$ deux diviseurs de $\delta$. Si $d_1$ est multiple de $d_2$, les ensembles $i$-uples propres et impropres fournis par la division $d_1$ de $m$, appartiennent à ceux fournis par la division $d_2$ de $m$.

En effet:

$$d_1 = kd_2 \quad , \quad k \gtreqless 1$$

$$\frac{m}{d_2} = \frac{m}{\frac{d_1}{k}} = k\frac{m}{d_1} \quad .$$

Donc les ensembles $i$-uples reproduits par $\frac{m}{d_1}$ déplacements, le seront aussi par $\frac{m}{d_2}$ déplacements, c. q. f. d.

La conséquence de cette proposition est donc la suivante: les ensembles $i$-uples fournis par une division fixée $d$ de $m$, $d$ diviseur de $\delta$, contiennent tous les ensembles $i$-uples propres et impropres fournis par les divisions $d'$ de $m$ dans lesquelles $d'$, diviseur de $\delta$, est multiple de $d$.

En particulier les ensembles $i$-uples fournis par la division $d = 1$ de $m$ dont le nombre est $C_m^i$ et qui sont tous reproduits par $m$ déplacements, contiennent tous les ensembles $i$-uples propres et impropres fournis par les divisions $d'$ de $m$ dans lesquelles $d'$, diviseur de $\delta$, est multiple de 1, ce qui est une proposition *évidente*.

En particulier aussi, les ensembles $i$-uples fournis par la division $d = \delta$ de $m$ dont le nombre est $C_{\frac{m}{\delta}}^{\frac{i}{\delta}}$ et qui se trouvent reproduits par le nombre *minimum absolu* de déplacements $\frac{m}{\delta}$, sont *tous propres* à cette division, puisqu'ils n'en contiennent aucun qui se reproduise par un nombre de déplacements plus petit (corollaire 2, § 4).

La proposition réciproque du théorème 3 n'existe pas d'une façon exactement inverse. Elle revient en définitive à la suivante qui est le complément ou la généralisation du théorème 1:

*Théorème 4.* Les nombres de déplacements qui reproduisent un ensemble $i$-uple donné $E_0$ sont les multiples du caractère $\alpha$ de $E_0$ et uniquement ces multiples.

En effet chaque nombre de déplacements multiple de $\alpha$ reproduit $E_0$. D'autre part un nombre de déplacements $\beta$ qui n'est pas multiple de $\alpha$, $\beta > \alpha$, peut se mettre sous la forme $\beta = \alpha q + r$, $0 < r < \alpha$, et pour la même raison qu'au théorème 1, ne peut pas reproduire $E_0$.

Ce théorème permet maintenant l'énoncé partiellement inverse complétant le théorème 3 et qui fixe *avec lui* quelles sont les divisions et les seules qui contiennent un ensemble $i$-uple donné.

*Théorème 5.* Soit un ensemble $i$-uple $E_0$ fourni par la division $d$ de $m$.

S'il est *propre* à cette division, c'est-à-dire s'il est reproduit pour la première fois par $\frac{m}{d}$ déplacements, il appartient *uniquement* aux divisions $d'$ de $m$, dans lesquelles $d'$ est diviseur de $d$.

En effet $\frac{m}{d}$ est le caractère de $E_0$. L'ensemble appartient donc uniquement aux divisions $d'$ pour lesquelles $\frac{m}{d'} = d_k \frac{m}{d}$, c'est-à-dire $d' = \frac{d}{d_k}$, $d_k$ comme $\frac{d}{d_k}$ parcourant les diviseurs de $d$.

S'il est *impropre* à cette division, c'est-à-dire s'il est reproduit pour la première fois par un nombre de déplacements *moindre* que $\frac{m}{d}$, le caractère $\alpha$ de $E_0$ est un diviseur de $\frac{m}{d}$, $\alpha < \frac{m}{d}$. $E_0$ est donc *propre* à une division $d_1$ de $m$ où $d_1 = \frac{m}{\alpha}$ est multiple (propre) de $d$. Dans ce cas $E_0$ appartiendra, en plus de la division $d$ de $m$, *uniquement* aux divisions $d'$ pour lesquelles $d'$ est diviseur de $d_1$.

Evidemment les deux propositions ci-dessus pourraient être formulées en une seule.

**6.** La réponse à la question posée au § 1 ne fait maintenant aucune difficulté.

Soit $\delta$ le p. g. c. d. de $m$ et $i$; soit $d$ diviseur de $\delta$. Notons le nombre des ensembles $i$-uples fournis par la division $d$ de $m$, $C_{\frac{m}{d}}^{\frac{i}{d}}$, simplement par $C(d)$, le nombre des ensembles $i$-uples *propres* à la division $d$ de $m$, par $P(d)$.

D'après la conséquence du théorème 3, les ensembles $i$-uples fournis par la division $d$ de $m$ *contiennent tous ceux fournis* par les divisions $d'$ de $m$, dans lesquelles $d'$ est *multiple* de $d$. D'autre part d'après la première proposition du théorème 5, la division $d$ de $m$ *ne peut pas contenir d'autres* ensembles $i$-uples que ceux qui appartiennent à une telle division $d'$, $d'$ *multiple* de $d$. En effet chaque ensemble $i$-uple est propre à une certaine division $d' = \frac{m}{\alpha}$ de $m$, $\alpha$ étant le caractère de l'ensemble. D'après la proposition indiquée, si l'ensemble est propre à une division $d'$, il appartient uniquement aux divisions $d$ dans lesquelles $d$ est *diviseur* de $d'$, c'est-à-dire $d'$ *multiple* de $d$, c. q. f. d.

Les ensembles $i$-uples fournis par la division $d$ de $m$ étant propres chacun à une division $d'$, où $d'$ est multiple de $d$, $d$ et $d'$ diviseurs de $\delta$, on a ainsi la formule:

$$C(d) = \sum_{d_k \mid \frac{\delta}{d}} P(dd_k) \tag{2}$$

dans laquelle la sommation s'étend à tous les multiples $dd_k$ de $d$, diviseurs de $\delta$, c'est-à-dire à tous les diviseurs $d_k$ de $\frac{\delta}{d}$.

La formule connue, dite *d'inversion de Möbius*[2]) permet alors d'inverser le résultat et de donner $P(d)$ en fonction des $C(dd_k)$. La formule donne:

---

[2]) Le théorème de *Möbius* est généralement donné sous la forme, $F(a)$ étant une fonction quelconque de valeurs entières et $G(a)$, la sommation indiquée:

$$\text{de } G(a) = \sum_{d \mid a} F(d) \text{ , il suit } F(a) = \sum_{d \mid a} \mu(d)\, G\left(\frac{a}{d}\right) .$$

Dans notre cas nous écrirons pour faciliter l'inversion:

$$C(d) = C_1\left(\frac{\delta}{d}\right) \quad , \quad P(d) = P_1\left(\frac{\delta}{d}\right) .$$

La formule directe (2) devient, $d_k$ et $\frac{\delta}{dd_k}$ parcourant les mêmes nombres, si $d_k$ parcourt les diviseurs de $\frac{\delta}{d}$:

$$C_1\left(\frac{\delta}{d}\right) = \sum_{d_k \mid \frac{\delta}{d}} P_1\left(\frac{\delta}{dd_k}\right) = \sum_{d_k \mid \frac{\delta}{d}} P_1(d_k) .$$

$$P(d) = \sum_{d_k \mid \frac{\delta}{d}} \mu(d_k)\ C(dd_k) \tag{3}$$

où $\mu\ (d_k)$ est la fonction dite de Möbius dont le sens est le suivant:

$\mu\ (d_k) = 1$ pour $d_k = 1$

$\mu\ (d_k) = (-1)^r$ si $d_k$ est le produit de $r$ ($r \geqq 1$) facteurs premiers différents

$\mu\ (d_k) = 0$ si $d_k$ est divisible au moins par un facteur premier au carré.

En particulier pour les deux cas extrêmes on a:

Cas $d = \delta$. La formule directe et la formule inverse donnent le même résultat:

$$C(\delta) = P(\delta) = C_{\frac{m}{\delta}}^{\frac{i}{\delta}}$$

conformément à ce qui a déjà été trouvé comme conséquence du théorème 3.

Cas $d = 1$.

$$\begin{aligned} C(1) &= \sum_{d_k \mid \delta} P(d_k) \\ P(1) &= \sum_{d_k \mid \delta} \mu(d_k)\, C(d_k)\ . \end{aligned} \tag{4}$$

Il ne reste maintenant plus qu'à fixer en combien de *colonnes cycliques* différentes (§ 1) se répartissent les $P(d)$ ensembles $i$-uples propres à la division $d$ de $m$. Chacun de ces ensembles $i$-uples est reproduit pour la première fois par $\frac{m}{d}$ déplacements. Autrement dit la colonne cyclique issue de l'un quelconque d'entre eux par les substitutions du groupe $\{(0, 1, 2, \ldots, m-1)\}$ contient $\frac{m}{d}$ $i$-uples; le $\left(\frac{m}{d} + 1\right)^{\text{ième}}$ $i$-uple reproduit le premier. Le nombre des colonnes cycliques en lesquelles se répartissent ces $P(d)$ $i$-uples propres à la division $d$ est donc $N(d) = \frac{d \cdot P(d)}{m}$.

Le nombre total des colonnes cycliques différentes en lesquelles se répartissent les $C_m^i$ $i$-uples des $m$ éléments est donc:

---

La formule d'inversion ci-dessus donne alors:

$$P_1\left(\frac{\delta}{d}\right) = \sum_{d_k \mid \frac{\delta}{d}} \mu(d_k)\ C_1\left(\frac{\delta}{dd_k}\right)$$

et donc

$$P(d) = \sum_{d_k \mid \frac{\delta}{d}} \mu(d_k)\ C(dd_k) \quad \text{c. q. f. d.}$$

$$\sum_{d|\delta} N(d) = \frac{1}{m} \sum_{d|\delta} d \cdot P(d) \quad . \tag{5}$$

**7.** Nous calculerons comme application le cas $m = 96$, $i = 12$, $\delta = 12$. Les diviseurs de 12 sont 1, 2, 3, 4, 6, 12. Le nombre des colonnes cycliques différentes en lesquelles se répartissent les $P(d)$ ensembles 12-uples propres à chacun de ces diviseurs et par suite le nombre total des colonnes cycliques dans lesquelles se répartissent les combinaisons 12 à 12 de 96 éléments par les substitutions du groupe $\{(0, 1, 2, \ldots, 95)\}$ s'établissent donc de la manière suivante:

| | | |
|---|---|---|
| $d = \delta = 12$, | $d_k = 1$ | $P(12) = C(12) = C_8^1 = 8 \qquad N(12) = 1$ |
| $d = 6$ | , $d_k = 1, 2$ | $P(6) = C(6) - C(12) = C_{16}^2 - C_8^1 = 112$ <br> $N(6) = 7$ |
| $d = 4$ | , $d_k = 1, 3$ | $P(4) = C(4) - C(12) = C_{24}^3 - C_8^1 =$ <br> $2.016 \qquad N(4) = 84$ |
| $d = 3$ | , $d_k = 1, 2, 4$ | $P(3) = C(3) - C(6) = C_{32}^4 - C_{16}^2 =$ <br> $35.840 \qquad N(3) = 1120$ |
| $d = 2$ | , $d_k = 1, 2, 3, 6$ | $P(2) = C(2) - C(4) - C(6) + C(12) =$ <br> $12.269 \cdot 376 \qquad N(2) = 255.612$ |
| $d = 1$, | $d_k = 1,2,3,4,6,12$ | $P(1) = C(1) - C(2) - C(3) + C(6) =$ <br> $624.668.642.224.128$ <br> $N(1) = 6.506.965.023.168$ |

$$\sum_{d|12} N(d) = 6.506.965.279.992 \; .$$

**8.** Nous pouvons directement de nos formules donner quelques résultats généraux.

a) $P(d)$ et $N(d)$ ne dépendent que de $m$ et $\delta$. Donc la répartition en colonnes cycliques pour un $m$ fixé est *la même* pour tous les ensembles de $i$-uples où $i$ a avec $m$ le p. g. c. d. $\delta$. En particulier elle est la même pour les $i$-uples et les $(m - i)$-uples, $i$ et $m - i$, complément l'un de l'autre relativement à $m$, ayant avec $m$ le même p. g. c. d. $\delta$.

b) Lorsque $\delta = 1$, c'est-à-dire lorsque $i$ est *premier* avec $m$, le seul diviseur $d$ de $\delta$ est 1. Chaque colonne cyclique contient $m$ $i$-uples et le nombre des colonnes est $N(1) = \frac{1}{m} P(1) = \frac{1}{m} \mu(1)\, C(1) = \frac{1}{m} C_m^i$. Lorsque $m$ et $i$ sont premiers entre eux, le nombre $\frac{(m-1)\,(m-2)\ldots(m-i+1)}{i\,!}$ est donc un nombre entier.

c) Lorsque $\delta = i$, c'est-à-dire lorsque $i$ est *diviseur* de $m$, on a $N(\delta) = \frac{\delta P(\delta)}{m} = \frac{\delta}{m} C^1_{\frac{m}{\delta}} = 1$. Il n'y a qu'*une* colonne cyclique des $i$-uples propres à la division $i$ de $m$. Cette colonne d'après le tableau (1) est la suivante:

$$\begin{array}{cccc} 0 & \frac{m}{i} & \frac{2m}{i} & \dots \frac{(i-1)m}{i} \\ 1 & \frac{m}{i}+1 & \frac{2m}{i}+1 & \dots \frac{(i-1)m}{i}+1 \\ \dots & \dots & \dots & \dots \\ \frac{m}{i}-1 & \frac{2m}{i}-1 & \frac{3m}{i}-1 & \dots m-1 \end{array} \quad (6)$$

On voit immédiatement que les $i$-uples constitués par chaque ligne de ce tableau se reproduisent chacun après $\frac{m}{i}$ déplacements. Il n'y a pas d'autre $i$-uple des $m$ éléments ayant cette propriété et la colonne cyclique constituée par les $\frac{m}{i}$ $i$-uples du tableau est la seule de son espèce.

d) Lorsque $\delta = i$ et $i$ est diviseur *premier* de $m$, les seuls diviseurs $d$ de $\delta$ sont $i$ et 1. Il n'y a donc que la colonne cyclique (6) qui ait *moins* de $m$ $i$-uples. Toutes les autres colonnes ont $m$ $i$-uples et leur nombre est $N(1) = \frac{1}{m} P(1) = \frac{1}{m}\{\mu(1)\, C(1) + \mu(i)\, C(i)\} = \frac{1}{m}(C^i_m - C^1_{\frac{m}{i}}) = \frac{1}{m}\left(C^i_m - \frac{m}{i}\right)$.
Donc si $i$ est diviseur premier de $m$, le nombre suivant est un nombre entier:

$$\frac{(m-1)\,(m-2)\dots(m-i+1)}{i\,!} - \frac{1}{i}\,.$$

e) Lorsque $1 < \delta < i$, on a: $i = i'\delta$, $m = m'\delta$ avec $i'$ et $m' > 1$ et premiers entre eux. On a $N(\delta) = \frac{\delta P(\delta)}{m} = \frac{1}{m'} C^{i'}_{m'}$. Nous retrouvons la conclusion donnée déjà sous b).

f) D'une manière générale, il est intéressant de remarquer que le nombre $N(d) = \frac{d \cdot P(d)}{m} = \frac{1}{m}\, d \sum_{d_k \mid \frac{\delta}{d}} \mu(d_k)\, C(dd_k)$ est un nombre entier.

g) En faisant la sommation de la formule (3), étendue à tous les diviseurs $d$ de $\delta$, on obtient:

$$\sum_{d \mid \delta} P(d) = \sum_{d \mid \delta} \sum_{d_k \mid \frac{\delta}{d}} \mu(d_k)\, C(dd_k)$$

c'est-à-dire d'après (4), et en remarquant d'abord que l'on peut permuter la double sommation et ensuite qu'elle revient à une sommation simple dans laquelle $d$ et $d_k$ parcourent *indépendamment l'un de l'autre* tous les entiers positifs tels que $dd_k$ est diviseur de $\delta$:

$$C(1) = \sum_{d \mid \delta} \sum_{d_k \mid \frac{\delta}{d}} \mu(d_k)\, C(dd_k) = \sum_{d_k \mid \frac{\delta}{d}} \sum_{d \mid \delta} \mu(d_k)\, C(dd_k) = \sum_{dd_k \mid \delta} \mu(d_k)\, C(dd_k).$$

Nous écrirons mieux dans ce cas au lieu de $d$ et $d_k$, $d$ et $d'$, $d$ et $d'$ parcourant comme ci-dessus tous les entiers positifs tels que $dd'$ est diviseur de $\delta$, et on a évidemment par raison de symétrie:

$$C(1) = \sum_{dd' \mid \delta} \mu(d')\, C(dd') = \sum_{dd' \mid \delta} \mu(d)\, C(dd')$$

formule qui est probablement susceptible de généralisation.

h) Dans ce cas le nombre total (5) des colonnes cycliques différentes peut aussi s'écrire, directement en fonction des $C(dd')$, sous les formes suivantes:

$$\sum_{d \mid \delta} N(d) = \frac{1}{m} \sum_{d \mid \delta} d\, P(d) = \frac{1}{m} \sum_{d \mid \delta} \sum_{d' \mid \frac{\delta}{d}} d\, \mu(d')\, C(dd')$$

$$= \frac{1}{m} \sum_{dd' \mid \delta} d\, \mu(d')\, C(dd') = \frac{1}{m} \sum_{dd' \mid \delta} d'\, \mu(d)\, C(dd')$$

(Reçu le 2 avril 1940.)