INTRODUCTION A LA THÉORIE DES CONGRUENCES AU MOYEN DE LA THÉORIE DES GROUPES

Autor(en): **Miller, G.-A.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **29 (1930)**

Heft 1: **L'ENSEIGNEMENT MATHÉMATIQUE.**

PDF erstellt am: **26.09.2024**

Persistenter Link: https://doi.org/10.5169/seals-23246

INTRODUCTION A LA THÉORIE DES CONGRUENCES AU MOYEN DE LA THÉORIE DES GROUPES

PAR

M. G.-A. MILLER (Urbana, Ill.) [1].

Les nombres 0, 1, 2, ..., $m - 1$ sont dits constituer un *système résiduel complet*, relativement au module m, où m est un entier positif quelconque.

Ces nombres constituent un groupe cyclique G par rapport à l'addition, mod. m, groupe dont la transformation identique est représentée par *zéro* et dont l'ordre est m. Si n est un élément quelconque de G et si d est le plus grand facteur commun à m et n, alors n engendre un groupe d'ordre $m : d$. En particulier, G a autant d'éléments générateurs qu'il y a de nombres, dans le système résiduel, qui sont premiers avec m. Une condition nécessaire et suffisante pour que m soit premier est que chaque nombre du système, excepté zéro, puisse jouer le rôle d'élément générateur.

Le « totient » $\Phi(m)$ de m ou *indicateur* de m est le nombre de générateurs de G ou le nombre d'opérateurs, d'ordre m, en G. Si d est un diviseur entier quelconque de m, alors G contient un et seulement un sous-groupe d'ordre d et si $d_1, d_2, \ldots, d_n$, représentent tous les diviseurs entiers positifs de m, y compris m, alors

$$\Phi(d_1) + \Phi(d_2) + \ldots + \Phi(d_n) = m$$

puisque le nombre des opérateurs, de l'ordre le plus élevé, dans tous les sous-groupes cycliques d'un groupe quelconque est égal

---

[1] Traduit de l'anglais par A. BUHL.

à l'ordre de ce groupe. Soient d_1 et d_2 deux diviseurs entiers positifs de m tels que $m = d_1 d_2$, alors

$$\Phi(m) = \Phi(d_1)\,\Phi(d_2) \prod_{\lambda=1}^{\lambda} \frac{p_i}{p_i - 1}$$

où $p_1, p_2, \ldots, p_\lambda$ sont les facteurs premiers communs distincts et positifs de d_1 et d_2. En particulier, quand d_1 et d_2 sont premiers entre eux,

$$\Phi(m) = \Phi(d_1)\,\Phi(d_2) .$$

Ceci résulte directement du fait que G est alors le produit de ses sous-groupes cycliques, d'ordres d_1, d_2 respectivement, et que

$$\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

quand p est premier.

Les nombres d'un système résiduel complet qui sont premiers avec m sont dits constituer un *système résiduel réduit*, mod. m. Un système résiduel réduit constitue un groupe abélien par rapport à la multiplication, mod. m, et ce groupe θ est le groupe des isomorphismes de G, puisque ses éléments représentent les différents indices des puissances auxquelles les éléments de G peuvent correspondre dans un automorphisme de G. Quand tous les éléments de G sont multipliés par un élément de θ, il en résulte un automorphisme de G en vertu duquel ces produits, mod. m, représentent une permutation des éléments de G. En particulier, quand les éléments d'un système résiduel complet sont multipliés par un nombre qui est premier avec le module et que les produits sont réduits par rapport à ce module, il en résulte, à nouveau, ce système résiduel complet. Les résidus des nombres naturels, combinés par multiplication, ont été considérés comme le plus important exemple d'un groupe abélien d'ordre fini [1].

Si le groupe G est prolongé par le groupe θ, il en résulte un groupe dont l'ordre est le produit des ordres de G et θ. Ce groupe est l'*holomorphe* de G. Il est non abélien quand $m > 2$. Quand m est impair, il ne contient point d'élément invariant sauf l'élément identique et, quand m est pair, son seul élément invariant, hors

[1] H. WEBER, *Lehrbuch der Algebra*, vol. 2, seconde édition, 1899, p. 60.

l'élément identique, est l'élément d'ordre 2 contenu dans G. Si nous représentons chacun des nombres d'un système résiduel complet par une lettre différente, l'holomorphe de G apparaît comme un groupe de substitution transitif concernant ces m lettres. Il est clair que, dans un automorphisme de G, les automorphismes des sous-groupes maxima dont les ordres sont des puissances de nombres premiers sont indépendants l'un de l'autre; il suit de là que θ est le produit direct des groupes d'isomorphismes des sous-groupes de G dont les ordres sont des puissances de nombres premiers.

Tout opérateur d'un groupe fini engendre un sous-groupe cyclique de ce groupe. En particulier, chaque nombre du groupe θ engendre un sous-groupe cyclique. Puisque l'ordre d'un groupe est divisible par l'ordre de chacun de ses sous-groupes, on a, lorsque a est premier avec m

$$a^{\Phi(m)} \equiv 1 , \qquad \text{mod. } m .$$

On voit ainsi que le théorème de Fermat est un cas très particulier du théorème bien connu de Lagrange relatif à l'ordre de chaque sous-groupe d'un groupe. La démonstration de ce théorème étant ainsi rendue très élémentaire, la question peut être élargie, on le voit, quand il est nécessaire de retenir le théorème de Fermat comme théorème séparé se rapportant cependant aux éléments de la Théorie des groupes considérés d'un point de vue élevé. Sous tout rapport, il semble indésirable de démontrer le théorème de Fermat dans la Théorie des Nombres sans se soucier de le comprendre en quelque aspect élémentaire de la Théorie des Groupes. Des remarques similaires s'appliquent à nombre d'autres théorèmes fondamentaux de la Théorie élémentaire des Nombres et conduisent à conclure que c'est d'abord la Théorie des Groupes qui doit intervenir, dans les exposés mathématiques primordiaux, à cause de sa très grande généralité.

L'inverse d'un opérateur, de G, représenté par la lettre r dans le système résiduel complet, mod. m, est $m - r$. En fait, si tous les éléments de G sont multipliés par $m - 1$, il en résulte un automorphisme de G dans lequel chaque opérateur correspond à son inverse. Si r est premier avec m, il en est de même de $m - r$

et la somme de tous les nombres représentés, en I, comme ci-dessus est

$$\frac{1}{2} m \Phi(m) .$$

Si un opérateur de I est représenté par le nombre n_1, son inverse est représenté par le nombre n_2 si $n_1 n_2 \equiv 1$, mod. m.

Tout opérateur de I peut correspondre à son inverse dans un automorphisme de I mais non dans un automorphisme de l'holomorphe de G quand I concerne des opérateurs dont l'ordre excède 2. Le sous-groupe G est invariant dans cet holomorphe mais le sous-groupe I n'est jamais invariant à moins que I ne soit l'identité. Une condition nécessaire et suffisante pour que cet holomorphe contienne un second sous-groupe cyclique invariant d'ordre m est que m soit divisible par 8. Quand cette condition est satisfaite l'holomorphe de G est aussi l'holomorphe de ce second sous-groupe cyclique invariant d'ordre m puisque tout sous-groupe cyclique invariant d'un groupe transitif est composé de substitutions régulières et de l'identité. De là suit ce théorème:

Une condition nécessaire et suffisante pour qu'un groupe cyclique d'ordre m *soit un sous-groupe caractéristique de son holomorphe est que* m *ne soit pas divisible par* 8. Si m est divisible par 8, le groupe cyclique d'ordre m possède un *double holomorphe.*

De même que le symbole $\Phi(m)$ est employé pour représenter le nombre d'opérateurs, de l'ordre le plus élevé, dans le groupe cyclique d'ordre m, le symbole $\Phi_n(m)$ a été employé pour représenter le nombre d'opérateurs, de l'ordre le plus élevé, dans le produit direct de n groupes cycliques d'ordre m. Si p^{α} est la plus haute puissance de p qui divise m, ce produit direct contient le produit direct de n groupes cycliques d'ordre p^{α}. Le nombre d'opérateurs de l'ordre le plus élevé, en ce produit direct, est évidemment

$$p^{n\alpha} - p^{n(\alpha-1)} .$$

D'où il suit que le nombre d'opérateurs, de l'ordre le plus élevé, dans le produit direct de n groupes cycliques d'ordre m est

$$\Phi_n(m) = m^n \left(1 - \frac{1}{p_1^n}\right)\left(1 - \frac{1}{p_2^n}\right) \cdots \left(1 - \frac{1}{p_\lambda^n}\right)$$

si $p_1, p_2, \ldots, p_\lambda$ sont les facteurs premiers distincts de m. Par conséquent, cette formule représente aussi le nombre de séries ordonnées de n entiers d'un système résiduel complet, mod. m, de telle sorte que m soit premier avec le plus grand commun diviseur de chaque série.

Si nous considérons le double module $p, \Phi(\chi)$ où p est un nombre premier et $\Phi(\chi)$ un symbole polynominal, irréductible mod. p, de degré n, il est évident que les p^n polynomiaux qui forment un système résiduel complet, mod. $p, \Phi(\chi)$, constituent, par rapport à l'addition, le groupe abélien d'ordre p^n et du type (1, 1, 1, ...). En excluant zéro de ce système résiduel complet, nous obtenons un système résiduel réduit mod. $p, \Phi(\chi)$ et ceci constitue un groupe quand les éléments sont combinés par multiplication. Le dernier groupe est cyclique car si l'un de ses polynomiaux vérifie $t^d \equiv 1$, mod. p, mais nulle équation de plus faible degré et de même forme, il ne peut pas y avoir plus de d polynomiaux distincts, en ce système résiduel réduit, qui satisfont à cette équation. De là, on conclut que le groupe formé par ce système résiduel réduit a la propriété de ne pas contenir plus d'un sous-groupe cyclique d'un ordre donné quelconque qui soit un diviseur de $p^n - 1$; par suite, il doit être cyclique.

Si nous multiplions tous les éléments du système résiduel complet donné par un élément de ce système, il résulte une (1, 1) correspondance entre les éléments du système résiduel complet original. Ceci représente un automorphisme quand les éléments sont combinés par addition, mod. p. D'où il suit que les éléments du groupe formé par ce système résiduel réduit peuvent être regardés comme les opérateurs qui transformèrent en lui-même le groupe formé par les éléments du système résiduel complet. Ces deux groupes engendrent, de plus, un groupe d'ordre $p^n(p^n - 1)$ qui est toujours inclus en l'holomorphe du groupe formé par le système résiduel complet. Une condition nécessaire et suffisante pour qu'il coïncide avec cet holomorphe est $n = 1$, puisque le groupe des isomorphismes d'un groupe abélien non cyclique est toujours non abélien. Ceci met en lumière le fait que le groupe des isomorphismes du groupe abélien d'ordre p^n et du type (1, 1, 1, ...) implique toujours un opérateur d'ordre $p^n - 1$ et constitue, à ce sujet, une démonstration très élémentaire.

Le rang du groupe abélien formé par un système résiduel réduit, mod. m, est évidemment égal au nombre des générateurs indépendants de son sous-groupe maximum dont l'ordre est une puissance de 2. Une condition nécessaire et suffisante pour que m ait des racines primitives est, par suite, que ce groupe abélien ne concerne qu'un opérateur d'ordre 2. D'autre part le produit prolongé de tous les opérateurs d'un groupe abélien est d'ordre 2, ou revient à l'identité, suivant que ce groupe contient seulement un opérateur d'ordre 2 ou plus d'un tel opérateur. Puisqu'un nombre premier a des racines primitives, il résulte de ce théorème que $(p-1)! \equiv\equiv -1$, mod. p, l'opérateur d'ordre 2 dans le système résiduel réduit, mod. p, étant clairement $p-1$. Le théorème de Wilson peut alors être regardé comme un cas particulier du théorème relatif à l'ordre du produit prolongé de tous les opérateurs d'un groupe abélien quelconque.

Le groupe des isomorphismes d'un groupe abélien quelconque est évidemment le produit direct des groupes d'isomorphismes de ses plus grands sous-groupes de puissance première. Puisque chacun de ces derniers est d'ordre pair quand il n'est pas l'identité, il résulte que m ne peut pas avoir de racines primitives à moins qu'il ne soit puissance d'un nombre premier ou le double d'une puissance d'un nombre premier impair. Il est aisé de voir que lorsque m est de la forme 2^α, $\alpha > 2$, il ne peut pas avoir de racine primitive puisque les trois nombres $2^\alpha - 1$, $2^{\alpha-1} \pm 1$, de son système résiduel réduit représentent clairement des opérateurs distincts d'ordre 2.

Le fait que tout nombre impair p a des racines primitives résulte directement du théorème que la congruence $x^n \equiv 1$, mod. p, ne peut pas avoir plus de n racines distinctes en un système résiduel réduit, mod. p, puisque ce système résiduel réduit doit alors constituer un groupe cyclique.

Pour prouver que p^m, lorsque p est un nombre premier impair quelconque et m un entier positif quelconque, a des racines primitives, il est, maintenant, seulement nécessaire de montrer que, pourvu que $m > 1$, il doit y avoir des nombres dans le système résiduel réduit, mod. p^m, qui représentent des opérateurs d'ordre p^{m-1}.

Il est aisé de voir que $1 + p$ est un tel nombre puisque sa

puissance p est de la forme $1 + kp^2$, où k est premier avec p. Donc le nombre $1 + p$ correspond à un automorphisme du groupe cyclique d'ordre p^m, en lequel seulement p opérateurs correspondent à eux-mêmes cependant qu'exactement p^2 opérateurs correspondent à eux-mêmes dans la puissance p de cet automorphisme. De ceci suit directement que p^α, $\alpha \leq m$, correspondent à eux-mêmes dans la puissance $p^{\alpha-1}$ de cet automorphisme d'où il résulte encore que le système résiduel réduit, mod. p^m, p étant premier impair, représente un groupe cyclique par rapport à la multiplication. Puisque le groupe des isomorphismes du groupe d'ordre 2 est l'identité, il résulte que le système résiduel réduit, mod. p, représente le même groupe que le système résiduel réduit, mod. $2p^m$, si toutefois p est premier impair.

On peut donc noter que *une condition nécessaire et suffisante pour qu'un nombre* m $>$ 2 *possède des racines primitives est qu'il y ait seulement un sous-groupe de chaque ordre premier dans le système résiduel réduit de* m, et, de ceci, on conclut que les seuls tels nombres qui ont des racines primitives sont 2, 4, p^m et $2p^m$, si p est premier impair.

Le théorème mis en italique suggère une nouvelle méthode pour établir, comme suit, l'existence de racines primitives: Un nombre d'un système résiduel réduit, mod. p^m, ne peut évidemment pas correspondre à un opérateur d'ordre p^α, à moins qu'il ne soit de la forme $1 + kp$, puisqu'autrement il représenterait un automorphisme qui ne laisserait pas invariant un opérateur d'ordre p dans le système résiduel complet. Donc un nombre de ce système résiduel réduit ne peut pas correspondre à un opérateur d'ordre p, à moins qu'il ne soit de la forme $1+kp^{m-1}$. Ceci prouve qu'il y a seulement $p - 1$ tels nombres dans le système résiduel réduit, mod. p^m.

Une série d'opérateurs d'un groupe G est dite [1] *série complète pour les puissances n* si les puissances n de ces opérateurs donnent toutes les puissances n différentes des opérateurs de G et s'il n'y a pas deux opérateurs de la série ayant la même puissance n. Les produits obtenus en multipliant tous les opérateurs d'une série complète, pour les puissances n d'un groupe abélien H, par un opérateur quelconque de ce groupe, constituent une

[1] G. A. MILLER, *Bulletin of the Amer. Math. Society*, vol. 18,1912, p. 227.

série complète pour puissances n puisque les puissances n des opérateurs de H constituent un groupe. Les k séries complètes obtenues en multipliant une telle série complète quelconque, par les différents opérateurs de H dont les ordres divisent n ont été appelées *séries complémentaires.* Ces k séries complémentaires impliquent chaque opérateur de H une fois et une fois seulement. L'ordre du produit prolongé de tous les opérateurs d'une série complète pour puissances n de H est un diviseur de $2n$ puisque l'ordre du produit prolongé de tous les opérateurs d'un groupe abélien quelconque doit diviser $2n$. Une condition nécessaire et suffisante pour que cet ordre soit $2n$ est que le sous-groupe formé par les puissances n de H contienne une fois et une fois seulement un opérateur d'ordre 2. En particulier, *une condition nécessaire et suffisante pour que* $[(p-1):2]!$ *appartienne à l'exposant* 4, mod. p, *est que* $p-1$ *soit divisible par* 4; *quand* $p-1$ *n'est pas divisible par* 4, *une condition nécessaire et suffisante pour que*

$$\left(\frac{p-1}{2}\right)! \equiv 1 , \qquad \text{mod. } p$$

est qu'un nombre pair des carrés de ces nombres soient négatifs par réduction à leurs moindres valeurs absolues, mod. p, puisque

$$1, 2, \ldots, \frac{p-1}{2}$$

est évidemment une série complète pour carrés mod. p.

Si le produit prolongé d'une série complète pour carrés d'un système résiduel réduit, mod. m, est d'ordre 4, le produit prolongé de toute autre série complète pour carrés, eu égard au même module, doit aussi être d'ordre 4 et si un tel produit se réduit à l'ordre 2 ou à l'identité, tout autre tel produit est ou d'ordre 2 ou réduit à l'identité. En particulier, quand le système résiduel réduit, mod. m, est un groupe cyclique, deux tels produits prolongés ne peuvent différer que par le signe puisque l'opérateur d'ordre 2, en un tel groupe, est représenté par -1. Au surplus, une série complète pour carrés, d'un tel système, reste une telle série si le signe d'un quelconque de ses éléments est changé, et deux séries complètes pour carrés peuvent différer l'une de l'autre seulement eu égard à de tels changements de signes. D'où

il résulte que si nous multiplions, tous les nombres de la série 1, 2, ..., $(p - 1):2$, par un nombre m premier avec p et que si nous réduisons les produits à leurs moindres résidus absolus, mod. p, le nombre m est un résidu quadratique ou un résidu non quadratique de p suivant que le nombre des nombres négatifs parmi ces produits est pair ou impair, puisque les produits prolongés de ces deux résidus complets pour carrés diffèrent seulement par le facteur m à la puissance $(p - 1):2$. Ces considérations relatives à la Théorie des Groupes contiennent maintenant une démonstration du Lemme bien connu de Gauss. Le fait que -1 est un résidu quadratique de tous les nombres premiers de la forme $1 + 4k$ et un résidu non quadratique de tous les autres nombres premiers impairs est donc un cas très particulier d'un théorème de la Théorie des Groupes qui affirme que quand t est un élément d'un groupe quelconque, tel que t^m soit d'ordre n, si p^α et p^β, $\beta > 0$, sont les plus hautes puissances du nombre premier p qui divise m et n respectivement, l'ordre de t est $lp^{\alpha+\beta}$ où l est premier avec p.

Quand $\beta = 0$, l'ordre de t peut être divisible par une puissance quelconque de p qui n'excède pas p^α. D'où il résulte que, puisque -1 est un opérateur d'ordre 2 dans le système résiduel réduit, mod. p, il ne peut pas être le carré d'un opérateur de ce système, à moins que cet opérateur ne soit d'ordre 4, et quand ce système résiduel contient deux opérateurs d'ordre 4, il faut alors que -1 soit leur carré commun. C'est dire qu'une condition nécessaire et suffisante pour que -1 soit un résidu quadratique de p est que $p - 1$ soit divisible par 4.

Le fait que le groupe des isomorphismes du groupe cyclique d'ordre 2^m, $m > 2$, est du type $(m - 2, 1)$ et contient un opérateur d'ordre 2^{m-2} qui est commutatif avec les opérateurs d'ordre 4, en ce groupe cyclique, implique que les carrés de tous ses opérateurs sont commutatifs avec les opérateurs d'ordre 8 contenus en ce groupe cyclique et aussi que ces opérateurs carrés doivent correspondre aux nombres du système résiduel réduit qui sont de la forme $1 + 8k$. De là résulte de plus que tous les nombres de cette forme sont les résidus quadratiques, mod. 2^m, cependant que tous les autres nombres impairs sont non-résidus quadratiques. Quand $m = 2$, ce groupe d'isomorphismes est d'ordre 2

et de là suit qu'un nombre impair est un résidu quadratique ou un non-résidu quadratique de 4 suivant qu'il est de la forme $1 + 4k$ ou de la forme $3 + 4k$.

Puisque le groupe des isomorphismes du groupe cyclique d'ordre p^m, p étant un nombre premier impair, est le groupe cyclique d'ordre

$$p^m - p^{m-1}$$

les résidus quadratiques, en ce cas, sont les nombres, en le système résiduel réduit, mod. p^m, qui correspondent aux opérateurs du produit direct du groupe cyclique d'ordre p^{m-1} par le groupe cyclique d'ordre $(p - 1) : 2$. En particulier, un résidu quadratique quelconque, mod. p^α, $\alpha > 1$, est aussi un résidu quadratique, mod. p^β, où β est un entier positif arbitraire.

Puisque tout nombre de la forme $1 + kp$ correspond à un opérateur, en le groupe des isomorphismes dont l'ordre est une puissance de p, il résulte que tout nombre de cette forme est un résidu quadratique, mod. p^m. Si un nombre est de cette forme, son carré est de la même forme et la plus haute puissance de p qui divise le k de ce nombre est aussi la plus haute puissance de p qui divise le k de son carré, puisque tous les opérateurs d'ordre p^α, dans le groupe des isomorphismes, correspondent à un k qui est divisible par la puissance $m - \alpha - 1$ de p mais par nulle puissance de p plus élevée.

Du fait que le groupe du système résiduel réduit, mod. p^m, est le produit direct des groupes cycliques des ordres p^{m-1} et $p - 1$ respectivement, il résulte que si l_1, l_2 représentent respectivement un résidu quadratique et un non résidu quadratique de p, alors $l_1 + kp$, $l_2 + kp$, k étant un entier quelconque, positif ou nul, représentant respectivement un résidu quadratique et un non résidu quadratique de p^m.

Quand l_1, l_2, prennent successivement toutes leurs valeurs possibles de 1 à $p - 1$, cependant que k prend successivement toutes les valeurs de 1 à p^{m-1}, nous obtenons ainsi chaque résidu quadratique et chaque résidu non quadratique, mod. p^m, une fois et une fois seulement. Ces considérations montrent que si l est racine primitive de p, sans ainsi être racine primitive de p^2, alors $l + kp$, où k est premier avec p, est une racine primitive de p^m.

Ceci fournit une démonstration, par la Théorie des Groupes, du théorème suivant:

Chaque résidu quadratique et chaque non-résidu quadratique d'une puissance positive arbitraire de p *est aussi un résidu quadratique ou un non résidu quadratique de toute autre puissance positive de* p, *cependant que toute racine primitive, d'une puissance positive de* p, *au moins aussi grande que* p^2, *est aussi une racine primitive de toute autre puissance positive de* p.

Il y a $p^{m-2}\Phi(p-1)$ racines primitives distinctes de p qui sont moindres que p^m, $m > 1$, mais ne sont pas ainsi racines primitives de p^m. Les racines primitives distinctes de p^m qui sont moindres que p^m sont les produits des nombres qui correspondent à ces racines primitives de p et des nombres de la forme $1 + kp$ où k est premier avec p sans être plus grand que p. Une condition nécessaire et suffisante pour qu'un nombre soit une racine primitive de p, sans être aussi racine primitive de p^m, est que ses puissances p^{m-2} appartiennent à l'exposant $p - 1$, mod. p^m.

Quand $m = 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\lambda^{\alpha_\lambda}$, où $p_1, p_2, \ldots, p_\lambda$ sont des nombres premiers distincts, le groupe formé par le système résiduel réduit, mod. m, est de rang λ, $\lambda + 1$, $\lambda + 2$ suivant que α_0 est < 2, $= 2$, ou > 2, puisque le groupe des isomorphismes du groupe cyclique d'ordre m est le produit direct des groupes des isomorphismes de ses sous-groupes de Sylow. Par suite le nombre des nombres, en ce système résiduel réduit, qui sont des résidus quadratiques, est $\Phi(m)$ divisé par une puissance de 2 dont l'exposant est égal à λ, $\lambda + 1$, $\lambda + 2$ respectivement.

Une condition nécessaire et suffisante pour qu'un nombre de ce système résiduel soit un résidu quadratique, mod. m, est qu'il soit un résidu quadratique pour chacun des nombres $2^{\gamma_0}, p_1^{\alpha_1}, \ldots, p_\lambda^{\alpha_\lambda}$ puisque les carrés des opérateurs, dans le groupe donné d'ordre $\Phi(m)$, constituent un groupe qui est le produit direct des sous-groupes composés des carrés des opérateurs dans les groupes d'isomorphismes des sous-groupes cycliques des ordres 2^{γ_0}, $p_1^{\alpha_1}$, $p_2^{\alpha_2}$, ..., $p_\lambda^{\alpha_\lambda}$ respectivement.

Bien que le principal objet du présent article ait été de mettre en évidence l'utilité de la conception de groupe en l'étude des congruences élémentaires, ce même article peut aussi servir d'introduction aux éléments de la théorie abstraite des groupes considérée du point de vue de la Théorie des Nombres.
