ANNALES
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN—POLONIA
VOL. V. 5. SECTIO A 1951

Z Seminarium Matematycznego I Wydz. Mat.-Przyr. U. M. C. S.
Kierownik: prof. dr Mieczysław Biernacki.

FRANCISZEK JAKÓBCZYK

Les applications de la fonction $\lambda_g(n)$ à l'étude des fractions périodiques et de la congruence chinoise $2^n - 2 \equiv 0 \pmod{n}$

Zastosowanie funkcji $\lambda_g(n)$ do badania ułamków okresowych i kongruencji chińskiej $2^n - 2 \equiv 0 \pmod{n}$

О применении функции $\lambda_g(n)$ к исследованию периодических дробей и китайского сравнения: $2^n - 2 \equiv 0 \pmod{n}$.

Introduction.

Les étranges propriétés des fractions décimales périodiques ont attiré mon attention dès l'année 1940. Les plus intéressantes se manifestent dans la représentation de la fraction irréductible $\frac{l}{m}$ dans un système numérique arbitraire g, si $(g, m) = 1$. Une propriété particulièrement intéressante se présente lorsque les chiffres des périodes se complètent à $g - 1$ (les restes correspondants se complétant à m) — propriété à laquelle j'ai donné le nom de propriété D; — et lorsque les chiffres se complètent à un nombre constant arbitraire a. Parmi les autres propriétés qui méritent aussi l'attention, signalons celles des chiffres et des restes des périodes de la fraction $\frac{l}{m}$ représentée dans les systèmes g et $\bar{g}$, dont les bases satisfont à la relation $g\bar{g} - 1 = m$. Une regularité intéressante s'observe aussi dans les produits des restes, comme p. ex $r_{s-i} \cdot r_{s+i} \equiv r_s^2 \pmod{m}$, $i = 1, 2, \ldots; s$ étant un nombre donné, d'ailleurs susceptible de prendre les valeurs $1, 2, \ldots$

Cependant on constate que dans tous ces problèmes le role fondamental appartient à la longueur de la période, c'est-à-dire un nombre de chiffres dans la période fondamentale simple. Je l'ai désigné par le symbole $\lambda_g(m)$.

Il est étonnant que cette fonction, si bien étudiée par différents mathematiciens du XIX-e siècle, n'ai pas encore trouvé place dans les manueles de Théorie des nombres. Ainsi p. ex. le professeur W. Sierpiński, dans son remarquable livre *„Teoria liczb"*, publié en 1950, se contente de montrer que la longueur de la période est l'exposant, auquel appartient le nombre g mod. m. G. H. Hardy et E. M. Wright, auteurs du volumineux livre *„An Introduction to the Theory of Numbers"*, paru en 1945, et Winogradow, dans son livre *„Osnowy tieorii czisel"* (1949), n'en font pas mention.

Pourtant cette fonction mérite d'être étudiée en méme temps que les fonctions d'Euler $\varphi(m)$, de Möbius $\mu(m)$, la fonction $\Theta(m)$, désignant le nombre des diviseurs de m, etc.

Dans le présent travail j'expose certains resultats nouveau (autant que j'aie pu le vérifier) sur la propriété D, obtenus principalement au moyen de la fonction $\lambda_g(m)$, ainsi que les résultats obtenus en appliquant cette fonction à l'étude de la congruence chinoise.

Le travail se compose de 3 parties.

Dans la première, j'énumère les propriétés fondamentales de la fonction $\lambda_g(m)$ en me servant du symbole de cette fonction, introduit par moi. Ces propriétés étant connues, je les ai indiquées sans démonstration.

Dans la seconde partie j'énonce quelques propositions et conséquences nouvelles sur la propriété D des nombres naturels m dans le système g. En profitant du théorème, bien connu, de Midy, j'établis les conditions nécessaires et suffisantes pour que les nombres suivants jouissent de la propriété D: $2m$ (m impair); p^a (p — nombre premier > 2) et 2^a; m, lorsque g en est une racine primitive; m^n (m impair); $m = [m_1, m_2, \ldots m_n]$, et aussi $2^a m$.

En appliquant ensuite le théorème de Jenkins, que je déduis comme corollaire des théorèmes précédents, j'établis encore quelques conséquences sur la propriété D du nombre $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, en tenant compte des types $4k + 1$, $4k - 1$, auxquels appartiennent les nombres premiers p_i, $i = 1, 2, \ldots n$, et de la circonstance que g est, ou non, racine primitive de ces nombres.

Dans la troisième partie j'expose les résultats obtenus en appliquant la fonction $\lambda_g(n)$ à l'étude de la congruence chinoise $2^n - 2 \equiv$

$\equiv 0 \pmod{n}$: je démontre ques les nombres impairs du type $n = 2^m + 1$, satisfaisant á la congruence chinoise, sont des nombres de Fermat et que les nombres impairs $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, solutions de cette congruence, doivent remplir la condition $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$, $i = 1, 2, \dots, k$, où ν_i est le plus grand nombre naturel t_i satisfaisant à la congruence $2^{\lambda_i} - 1 \equiv 0 \pmod{p_i^{t_i}}$ où $\lambda_i = \lambda_2(p_i)$, enfin, que pour les nombres pairs $2n$, racines de la même congruence chinoise, l'on a encore la condition $k \geqslant 2$.

Une intéressante propriété, jusqu'ici inconnue, se manifeste pour les nombres de Fermat et de Mersenne, impairs, qui, on le sait, satisfont à la congruence chinoise; tous ces nombres doivent être du type $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, avec les conditions mentionnées plus haut, de plus, il est assez probable qu'ils sont tous du type $n = p_1 p_2 \dots p_k$, $k \geqslant 1$.

En terminant cette introduction je tiens à exprimer à M. le Professeur M. Biernacki ma profonde gratitude pour l'intérét qu'il a prété à ce travail, en le relisant plusieurs fois, pour ses remarques critiques qui m'ont permis d'éviter certaines erreurs et d'améliorer quelques démonstrations, enfin pour ses précieux conseiles au cours de la rédaction.

Je remercie aussi sincèrement M. le Professeur A. Bielecki qui a bien voulu s'intéresser à mon travail et en a relu le manuscrit.

Je voudrais exprimer ma particulière reconnaissance à M. le Professeur W. Sierpiński pour les encouragements et le bienveillant intérét qu'il a prêtés aux résultats de mon travail et pour les avoir estimés positivement. C'est lui qui, en 1947, a attiré mon attention sur le problème de la congruence chinoise $2^n - 2 \equiv 0 \pmod{n}$. Cela m'a donné l'occasion d'y appliquer la fonction $\lambda_g(n)$ et de mieux l'étudier.

Je remercie enfin cordialement M. le Professeur A. Mostowski, qui s'est intéressé aux résultats de mon travail et les a estimés positivement; ses encouragements ont été pour moi une forte impulsion qui m'a permis de le mener à bout.

I

La fonction $\lambda_g(m)$

Dans le présent travail je me sers constamment du symbole $\lambda_g(m)$. Il désigne la longueurs de la période (nombre de chiffres de la

période) de la fraction proprement dite irréductible $\frac{l}{m}$ dans le système numérique dans la base g (pour simplifier nous écrirons désormais: système g), les nombres m et g étant premiers entre eux; car nous admettons, dans la suite, que la période de la fraction $\frac{l}{m}$ est simple, c'est-à-dire qu'elle ne contient que des termes réguliers de la représentation systématique dans la base g.

Remarque. — Les symboles (a, b) et $[a, b]$ représentent respectivement le plus grand commun diviseur et le plus petit commun multiple des nombres a et b.

Le nombre [1]) $\lambda_g(m) = \lambda$ n'étant autre que l'exposant[2]), auquel appartient le nombre g *mod.* m, on a la congruence $g^\lambda - 1 \equiv 0 \pmod{m}$, et λ est le plus petit nombre naturel qui satisfasse à cette congruence.

La fonction $\lambda_g(m)$ a des propriétés bien connues, que je vais énumérer sans les démontrer.

Propriété I. Si $g \equiv g \pmod{m}$, alors $\lambda_{\bar{g}}(m) = \lambda_g(m)$.

Propriété II. Si $g\bar{g} \equiv 1 \pmod{m}$, alors $\lambda_{\bar{g}}(m) = \lambda_g(m)$.

Propriété III. [3]) Si $m_i \neq m_j$, $i, j = 1, 2, \ldots, n$

alors $\lambda_g([m_1, m_2, \ldots, m_n]) = [\lambda_g(m_1), \lambda_g(m_2), \ldots, \lambda_g(m_n)]$

Propriété IIIa.[4]) Si $m_i \neq m_j$ et $(m_i, m_j) = 1$, $i, j = 1, 2, \ldots, n$,

alors $\lambda_g(m_1 m_2 \ldots m_n) = [\lambda_g(m_1), \lambda_g(m_2), \ldots, \lambda_g(m_n)]$.

Propriété IIIb. Si $(m, 2) = 1$ et $(g, 2) = 1$, alors $\lambda_g(2m) = \lambda_g(m)$.

Propriété IIIc.[5]) Si $m = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$, où p_i $(i = 1, 2, \ldots n)$

[1]) Le symbole $\lambda_g(m)$ a été introduit par moi. Il permet de donner une grande clarté aux théorèmes et aux démonstrations concernant la longueur de la période. De plus, il s'accorde bien avec le nombre $\lambda(m)$ qui désigne le plus petit exposant universel mod. m.

Cf. O. Ore: *Number Theory and its History*, New York, 1948, 1st ed., pp. 290—4.

[2]) Cf. W. Sierpiński: *Teoria liczb*, Waszawa-Wrocław, 1950, p. 222. Dans sa *Théorie des nombres*, Paris 1891, t. I, p. 439, Lucas appelle cet exposant *gaussien*.

[3]) Cf. F. J. Lionnet: *Algèbre élém.*, 3-e éd., 1868. Nouv. Ann. Math., (2), 7, 1868, 239; pour les démonstrations de Morel et Pellet cf 2, 10, 1871, 39—42, 92—95. Cf. aussi F. Meyer, Archiv Math. Phys., 49, 1869, 168—178.

[4]) Cf. J. Wallis: *Treatise of Algebra both Historical and Practical*, London, 1865, ch. 89, 326—8 (manuscrit, 1676). — J. Bernoulli: Nouv. mém. Acad. Roy., Berlin, année 1771 (1773), 273—317. — Thibault: Nouv. Ann. Math., 1, 1842, 464—5, 467—9. — A. Lugli: Periodico di Mat., 2, 1887, 161—174. — J. E. Oliver: Math. Monthly, (ed. Runkle) Cambridge, Mars, 1, 1859, 345—9.

[5]) Cf. E. Midy: *De quelques propriétés des nombres et des fractions décimales périodiques*, Nantes, 1836, 21 pp.

sont des nombres premiers, alors $\lambda_g(m) = [\lambda_g(p_1^{a_1}), \lambda_g(p_2^{a_2}), \ldots, \lambda_g(p_n^{a_n})]$.

Propriété IVa.[6]) Si p désigne un nombre premier > 2, $(p, g) = 1$ et ν désigne la plus grande valeur du nombre naturel t satisfaisant à la congruence $g^\lambda - 1 \equiv 0 \pmod{p^t}$, où $\lambda = \lambda_g(p)$ alors

$\lambda_g(p^a) = \lambda_g(p)$ lorsque $1 \leqslant a \leqslant \nu = \nu_g(p)$

et $\lambda_g(p^a) = p^{a-\nu}\lambda_g(p)$ „ $a > \nu$.

Propriété IVb.[7]) Si $g = 4k \pm 1 = 2^{2+h} \cdot k' \pm 1$, où $(k', 2) = 1$, on a $\lambda_g(2^a) = 1$ pour $1 = a$,

$\lambda_g(2^a) = \lambda_g(2^2)$ pour $1 < a \leqslant \nu = 2 + h$,

$\lambda_g(2^a) = 2^{a-\nu}$ pour $a > \nu$,

de plus, $\lambda_g(2^2) = 1$ ou 2 suivant que g est du type $4k + 1$ ou $4k - 1$.

Propriété V.[8]) Si $m = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ et $m' = p_1\ p_2\ \ldots\ p_n$, p_i étant un nombre premier > 2, $i = 1, 2, \ldots, n$, on a les relations

A. $\lambda_g(m) = \lambda_g(m')$ lorsque $1 \leqslant a_i \leqslant \nu_i = \nu_g(p_i)$, $i = 1, 2, \ldots n$

B. $\lambda_g(m) = \left[p_1^{a_1-\nu_1} \cdot \lambda_g(p_1), p_2^{a_2-\nu_2} \cdot \lambda_g(p_2), \ldots, p_k^{a_k-\nu_k} \cdot \lambda_g(p_k), \lambda_g(p_{k+1}), \ldots, \lambda_g(p_n)\right]$.

lorsque l'inégalité $a_i > \nu_i$ a lieu pour les indices $i = 1, 2, \ldots, k$, où $1 \leqslant k \leqslant n$ et où l'on suppose que dans la décomposition de m en facteurs premiers on a placé au commencement tous les facteurs p_i pour lesquels $a_i > \nu_i$.

C. $\lambda_g(2^a m) = [\lambda_g 2^a), \lambda_g(m)]$

si g et m sont impairs, $\lambda_g(2^a)$ étant défini par la propriété IVb.

Remarque. La propriété V est un énoncé plus détaillé de la propriété IIIc.

Définition. Nous appellerons degré de parité du nombre $\overline{m} = 2^a m$, où $(m, 2) = 1$, le nombre a.

---

[6]) Cf. Thibault: Nouv. Ann. Math., 1, 1842, 464—5, 467—9. — E. Desmarest: *Théorie des nombres*, Paris, 1852, 308, (pour $a = 2$). — F. J. Lionnet: op. cit. — G. Barillari: Giornale di Mat., 9, 1871, 125—135. — W. Shanks: Messenger Math., 3, 1874, 52—55. — J. W. L. Glaisher: Report British Assoc., 1878, 190—1.

[7]) Cf. F. Schuh: Nieuw Archief Wiskunde, (2), 9, 1911, 408—439.

[8]) Cf. Sanio: *Ueber die periodischen Decimalbrüche*, Progr., Memel, 1866. — G. Barillari: Giornale di Mat., 9, 1871, 125—135. — T. Muir: Messenger Math., 4, 1875, 1—5. — F. Stasi: Il Boll. Mat. Giorn., 11, 1912, 226—246.

Cette définition permet de formuler encore une propriété de la fonction $\lambda_g(m)$, résultant des propriétés IVa et V.

Propriété VIa. p désignant un nombre premier > 2, les nombres $\lambda_g(p^a)$ et $\lambda_g(p)$ ont le même degré de parité.

Propriété VIb. Si $m = p_1^{a_1} \cdot p_2^{a_2} \ldots p_k^{a_k}$, $m' = p_1 p_2 \ldots p_k$, p_i désignant un nombre premier > 2, $i = 1, 2, \ldots, k$, alors les nombres $\lambda_g(m^n)$, $\lambda_g(m)$ et $\lambda_g(m')$, ont le même degré de parité.

II

Chiffres et restes complémentaires dans la période (propriété D)

§ 1. Certains nombres entiers m possèdent l'étrange propriété suivante: si l'on représente la fraction proprement dite irréductible $\frac{l}{m}$ comme fraction périodique dans le système g, les chiffres de la période, à partir de la moitié de la période, se complètent à $g - 1$ avec les chiffres correspondants de la première moitié de la période, et, d'une façon analogue, dans la période des restes, les restes correspondants se complètent à m.

Appelons cette propriété du nombre m *propriété D*. Elle ne dépend nullement du numérateur de la fraction $\frac{l}{m}$ mais seulement des nombres m et g. Nous n'allons considérer que des périodes simples [9]). Nous supposerons désormais $(m, g) = 1$ et, évidement, $(l, m) = 1$.

Désignons les chiffres de la période par c_i, les restes correspondants par r_i $(i = 1, 2, \ldots, n)$; si la longueur $\lambda_g(m)$ compte $2a$ termes, la propriété D s'exprime par les égalités

$$c_i + c_{a+i} = g - 1 \tag{1}$$

$$r_i + r_{a+i} = m \tag{2}$$

$$i = 1, 2, \ldots, a$$

Nous désignerons par $C_g\left(\frac{l}{m}\right)$ la période des chiffres de la fraction $\frac{l}{m}$, représentée dans le système g et par $R_g\left(\frac{l}{m}\right)$ le période des restes correspondants dans le même système.

[9]) Cf. W. Sierpiński: *Teoria liczb*, Warszawa—Wrocław, 3-e éd., 1950, pp. 219, 222.

Exemple. — $C_{10}\left(\frac{1}{7}\right) = 142|857$; $R_{10}\left(\frac{1}{7}\right) = 3, 2, 6, |4, 5, 1$. Pour la période $C_{10}\left(\frac{1}{7}\right)$ on a les égalités: $1 + 8 = 4 + 5 = 2 + 7 = 9$, pour $R_{10}\left(\frac{1}{7}\right)$ on a: $3 + 4 = 2 + 5 = 6 + 1 = 7$.

§ 2. On peut se poser la question suivante: quels sont les nombres m qui ont la propriété D et dans quels systèmes numériques?

Remarquons d'abord que la *condition nécessaire* pour que le nombre m possède cette propriété est que la longueur de la période, c'est-à-dire le nombre $\lambda_g(m)$, soit paire. On voit pourtant aisément que cette condition n'est pas suffisante.

D'autre part, E. Catalan (1842) [10]) a démontré que si l'égalité (2) a lieu pour un indice i, elle a lieu aussi pour l'indice $i + 1$, elle est donc vraie pour tous les indices suivants; on peut aussi montrer qu'elle a lieu encore pour l'indice $i - 1$, donc elle est vraie pour tous les indices inférieurs.

En profitant de cette propriété de l'égalité (2), il est facile de démontrer que l'égalité (2) entraîne l'égalité (1).

En effet, supposons que l'égalité $r_i + r_{a+i} = m$ ait lieu pour un indice i dans la période $R_g\left(\frac{l}{m}\right)$ alors, il résulte du théorème de Catalan que l'on a aussi: $r_{i+1} + r_{a+i+1} = m$. Or, entre les restes r_i et les chiffres c_i des périodes $C_g\left(\frac{l}{m}\right)$ et $R_g\left(\frac{l}{m}\right)$ il y a la relation simple: $gr_i = mc_i + r_{i+1}$, $i = 1, 2, \ldots$. De même, $gr_{a+i} = mc_{a+i} + r_{a+i+1}$. En ajoutant ces égalités membre à membre, nous obtenons:

$$g(r_i + r_{a+i}) = m(c_i + c_{a+i}) + (r_{i+1} + r_{a+i+1}),$$

d'où, en tenant compte des égalités $r_i + r_{a+i} = r_{i+1} + r_{a+i+1} = m$,

il résulte $$gm = m(c_i + c_{a+i}) + m,$$

c'est-à-dire $$c_i + c_{a+i} = g - 1.$$

Quant à la question si, inversement, l'égalité (2) résulte de l'égalité (1), on peut démontrer que cette circonstance n'a lieu que lorsque l'égalité (1) est vraie pour *tous* les indices $i = 1, 2, \ldots a$.

[10]) Nouv. Ann. Math., 1, 1842, 464—5, 467—9.

Nous ommettons la démonstration, reposante sur le théorème de Midy, que nous allons énoncer plus loin.

En 1836 E. Midy[11]) et, en 1864, W. H. H. Hudson[12]) ont démontré que si $\lambda_{10}(m) = 2n$, $(m, 10) = 1$ et $(m, 10^n - 1) = 1$, alors le nombre m possède la propriété D dans le système $g = 10$.

En 1880 O. Schlömilch[13]) a trouvé que la condition nécessaire, pour que le nombre m possède la propriété D dans le système $g = 10$, est qu'il soit diviseur du nombre $10^n + 1$, où $2n = \lambda_{10}(m)$ et $(m, 10) = 1$.

G. R. Perkins (1841)[13a]) a démontré que si dans la période $R_g\left(\frac{1}{m}\right)$ on a l'égalité $r_n = m - 1$, alors le nombre m possède la propriété D. On démontre aisément que cette proposition résulte du theorème de Schlömilch. En effet, comme $r_n \equiv g^n \pmod{m}$, l'égalité ci-dessus donne la congruence $g^n \equiv m - 1 \equiv -1 \pmod{m}$.

On peut montrer que les théorèmes de Midy et de Schlömilch sont equivalents; en effet, si $\lambda_g(m) = 2n$, $(m, g) = 1$ et $(m, 2) = 1$, on a la congruence

$g^{2n} - 1 = (g^n - 1)(g^n + 1) \equiv 0 \pmod{m}$, où $(g^n - 1, g^n + 1) \leqslant 2$. Donc, si $(m, g^n - 1) = 1$, alors $g^n + 1 \equiv 0 \pmod{m}$. D'autre part, $g^n + 1 \equiv 0 \pmod{m}$ entraîne $(m, g^n - 1) = 1$.

Ce théorème est *fondamental* pour le problème considéré. Nous l'énoncerons sous la forme suivante, comme

Théorème de Midy. Pour que le nombre m posséde la propriéte D dans le systeme g, il faut et il suffit qu'il existe un nombre naturel a satisfaisant à la congruence: $g^a + 1 \equiv 0 \pmod{m}$.
De plus, si a est le plus petit nombre ayant cette propriété, alors $\lambda_g(m) = 2a$. Le théorème est connu, je ne vais pas le démontrer.

§ 3. De ce théorème, ainsi que des propriétés de la fonction $\lambda_g(m)$ je vais déduire quelques propositions, nouvelles ou peu connues, et quelques conséquences.

Théorème I. — *Si le nombre m possède la propriété D dans le système g et si $g \equiv g \pmod{m}$, alors il la possède aussi dans le système g.*

Démonstration. — Supposons que le nombre m possède la

[11]) *De quelques propriétés des nombres et des fractions décimales périodiques*, Nantes, 1836, 21 pp.

[12]) Oxford, Cambridge and Dublin Messenger of Math., 2, 1864, 1—6.

[13]) Zeitschrift Math. Phys., 25, 1880, 416.

[13a]) Amer. Journ. Sc. Arts, 40, 1841, 112-7.

propriété D dans le système g. En vertu du théorème de Midy, il existe un nombre a tel que la congruence

$$g^a + 1 \equiv 0 \ (mod.\ m) \tag{3}$$

ait lieu. Comme

$$\bar{g} \equiv g \ (mod.\ m) \tag{4}$$

on a aussi: $\bar{g}^a \equiv g^a \ (mod.\ m)$,

d'où, en tenant compte de (3), nous obtenons immédiatement la congruence

$$\bar{g}^a + 1 \equiv g^a + 1 \equiv 0 \ (mod.\ m),$$

ce qui prouve que m possède la propriété D aussi dans le système g.

Désignons par $\bar{r}_i$ $(i = 1, 2, \ldots)$ les restes de la période $R_{\bar{g}}\left(\frac{l}{m}\right)$. Nous avons donc

$$\bar{r}_i \equiv l\bar{g}^i \ (mod.\ m), \tag{5}$$

de même, pour $R_g\left(\frac{l}{m}\right)$, nous avons: $r_i \equiv lg^i \ (mod.\ m)$. (6)

La congruence (4) donne

$$\bar{g}^i \equiv g^i \ (mod.\ m) \tag{7}$$

pour $i = 1, 2, 3, \ldots$, donc il résulte de (5) et (6) que $\bar{r}_i \equiv r_i \ (mod.\ m)$, d'où, au moyen des inégalités: $0 < \bar{r}_i < m$, $0 < r_i < m$, nous obtenons immédiatement

$$\bar{r}_i = r_i. \tag{8}$$

En désignant par $\bar{c}_i$ $(i = 1, 2, \ldots)$ les chiffres de la période $C_{\bar{g}}\left(\frac{l}{m}\right)$ nous avons, pour les périodes des chifres et des restes dans les systèmes $\bar{g}$ et g, les égalités

$$\bar{g}\bar{r}_i = m\bar{c}_i + \bar{r}_{i+1} \tag{9}$$

$$gr_i = mc_i + r_{i+1} \tag{10}$$

Mais, d'après (8), l'égalité (9) prend la forme

$$\bar{g}r_i = m\bar{c}_i + r_{i+1} \tag{11}$$

En retranchant (10) de (11) on a

$$(\bar{g} - g)\, r_i = m\,(\bar{c}_i - c_i) \tag{12}$$

Mais (4) entraine $\bar{g} = g + km$, où k est un nombre naturel. De l'égalité (12), après avoir divisé les deux membres par m, nous obtenons

$$\bar{c}_i = c_i + kr_i, \quad i = 1, 2, 3, \ldots \tag{13}$$

Les égalités (8) et (13) permettent de déterminer les périodes $R_{\bar{g}}\left(\frac{l}{m}\right)$ et $C_{\bar{g}}\left(\frac{l}{m}\right)$ au moyen des périodes $R_g\left(\frac{l}{m}\right)$ et $C_g\left(\frac{l}{m}\right)$ lorsque $\bar{g} = g + km$, de plus, elles confirment le théorème I, car $\bar{c}_l + \bar{c}_{\alpha+l} = c_l + c_{\alpha+l} + k(r_l + r_{\alpha+l}) = g - 1 + km = \bar{g} - 1$.

§ 4. **Théorème II.** *Si le nombre m possède la propriété D dans le système g et si $g\bar{g} \equiv 1$ (mod. m), alors il la possède aussi dans le système $\bar{g}$.*

Démonstration. Si le nombre m possède la propriété D dans le système g, en vertu du théorème de Midy nous avons la congruence

$$g^{\alpha} + 1 \equiv 0 \ (mod.\ m). \tag{14}$$

Puisque $g\bar{g} \equiv 1$ (mod. m), la congruence

$$(g\bar{g})^{\alpha} = \bar{g}^{\alpha} g^{\alpha} \equiv 1 \ (mod.\ m) \tag{15}$$

est aussi vraie.

Mais (14) entraîne $g^{\alpha} \equiv -1$ (mod. m), de la congruence (15) il résulte donc

$$-\bar{g}^{\alpha} \equiv 1 \ (\text{mod. } m) \quad \text{ou} \quad \bar{g}^{\alpha} + 1 \equiv 0 \ (\text{mod. } m).$$

Le nombre m possède donc la propriété D aussi dans le système $\bar{g}$.

On démontre aisément que l'on a

$$r_i = \bar{r}_{\lambda-i}, \ i = 1, 2, 3, \ldots; \ \lambda = 2\alpha = \lambda_g(m). \tag{16}$$

En effet, si $1 \equiv g\bar{g}$ (mod. m), on a aussi

$$1 \equiv g^{\lambda-i}\bar{g}^{\lambda-i} \ (\text{mod. } m), \ i = 1, 2, \ldots$$

En multipliant membre à membre cette congruence avec la congruence $r_i \equiv lg^i$ (mod. m), nous obtenons

$$r_i \equiv lg^{\lambda} \cdot \bar{g}^{\lambda-i} = g^{\lambda} \cdot l\bar{g}^{\lambda-i} \equiv l\bar{g}^{\lambda-i} \equiv \bar{r}_{\lambda-i} \ (\text{mod. } m)$$

car $g^{\lambda} \equiv 1$ (mod. m), en vertu de la définition du nombre λ. L'égalité (16) en résulte immédiatement. Elle constitue aussi une vérification du théorème II.

§ 5. **Théorème III.** *Pour que le nombre pair $m = 2m$, où $(m, 2) = 1$, possède la propriété D dans le système g, où $(g, 2) = 1$, il faut et il suffit que le nombre m la possède dans le même système.*

Démonstration. Si le nombre impair m possède la propriété D dans le système g, la congruence $g^{\alpha} + 1 \equiv 0$ (mod. m) a lieu. Le nombre g étant impair, le membre gauche de cette congruence est pair, m étant aussi impair, nous avons $g^{\alpha} + 1 \equiv 0$ (mod. $2m$), ce qui

prouve que le nombre $\overline{m} = 2m$ possède la propriété D. La condition est donc *suffisante.*

Inversement, si le nombre pair $\overline{m} = 2m$, où $(m, 2) = 1$, possède la propriété D dans le système g, et si $(g, 2) = 1$, nous avons $g^a + 1 \equiv 0 \pmod{2m}$.

On a donc les congruences

$$g^a + 1 \equiv 0 \pmod{2} \text{ et } g^a + 1 \equiv 0 \pmod{m}.$$

La dernière prouve que m possède la propriété D, c'est—à—dire que la condition est aussi *nécessaire.*

§ 6. Pour les nombres premiers $p > 2$ la propriété D a été étiudé par Goodwyn [14]) (1802), F. T. Poselger [15]) (1827, P. Lafitte [16]) (1851), W. H. H. Hudson [17]) (1864), J. W. L. Glaisher [18]) (1878); ces auteurs ont trouvé que si la longueur de la période, c'est-à-dire $\lambda_g(p)$ est un nombre pair alors, le nombre p possède la propriété D.

Pourtant on peut démontrer un théorème plus général.

Théorème IV. — *Pour que le nombre p^a où p désigne un nombre premier > 2 et a un nombre naturel, possède la propriété D dans le système g, il faut et il suffit que le nombre $\lambda_g(p)$ soit pair. Évidemment $(g, p) = 1$.*

Démonstration. — En vertu de la propriété IVa de la fonction $\lambda_g(m)$, la parité du nombre $\lambda_g(p^a)$, donc aussi celle du nombre $\lambda_g(p)$, est la condition *nécessaire* pour que le nombre p^a possède la propriété D. Cela est évident, sinon celle-ci n'aurait pas lieu. Il nous reste donc à démontrer que cette condition est *suffisante.*

En effet, si $\lambda_g(p)$ est pair, il résulte de la propriété IVa de la fonction $\lambda_g(m)$ que $\lambda_g(p^a) = \lambda$ est aussi pair. On a donc, par définition du nombre λ, la congruence

$$g^{\lambda} - 1 \equiv 0 \pmod{p^a} \qquad (16')$$

ou

$$\left(g^{\frac{\lambda}{2}} - 1\right)\left(g^{\frac{\lambda}{2}} + 1\right) \equiv 0 \pmod{p^a}.$$

Mais $\left(g^{\frac{\lambda}{2}} - 1,\ g^{\frac{\lambda}{2}} + 1\right) \leqslant 2$, donc le nombre $p > 2$ ne peut être com-

[14]) Journ. Nat. Phil. Chem. Arts, (ed. Nicholson), London, New Series, 1, 1802, 314—6. — Cf. R. Law: Ladies'Diary, 1824, 44—45, Quest. 1418.

[15]) Abhand. Ak. Wiss. Berlin, (Math.), 1827, 21—36.

[16]) Nouv. Ann. Math., 3, 1851, 147—152. Cf. Amer. Math. Monthly, 19, 1912, 130—2.

[17]) Oxford, Cambridge and Dublin Messenger of Math., 2, 1864, 1—6.

[18]) Report British Assoc., 1878, 190—1.

mun diviseur des nombres $g^{\frac{\lambda}{2}} - 1$ et $g^{\frac{\lambda}{2}} + 1$. Donc un seul des nombres $g^{\frac{\lambda}{2}} - 1$ et $g^{\frac{\lambda}{2}} + 1$ est divisible par p et p^α. Mais, le nombre λ étant par définition le plus petit nombre naturel, satisfaisant à la congruence (16'), le nombre $g^{\frac{\lambda}{2}} - 1$ ne peut être divisible ni par p^α, ni par p. On a donc la congruence $g^{\frac{\lambda}{2}} + 1 \equiv 0 \pmod{p^\alpha}$, ce qui prouve, d'après le théorème de Midy, que le nombre p^α a la propriété D dans le système g. Ainsi nous avons trouvé que la condition du théorème IV est aussi suffisante. Le théorème IV est donc démontré complètement.

§ 7. **Théorème V.** — *Si le nombre g est une racine primitive du nombre m, m possède la propriété D dans le système g.*

Démonstration. — Le nombre g n'est une racine primitive de m que dans le cas où l'on à l'égalité $\lambda_g(m) = \varphi(m)$ [19]).

On sait [20]) que les seuls nombres qui possèdent des racines primitives sont les nombres 2, 4, p^α, $2p^\alpha$, où p désigne un nombre premier > 2, α un nombre naturel. Nous avons donc à démontrer que si g est une racine primitive de l'un quelconque des nombres 2, 4, p^α, $2p^\alpha$, alors m possède la propriété D dans le système g.

a) Pour le nombre $m = 2$ tout nombre impair $g = 2k + 1$ (k — naturel) — et aucun autre — est une racine primitive. Mais, alors, on a $\lambda_g(2) = \varphi(2) = 1$; on pourrait donc supposer que, le nombre $\lambda_g(2)$ étant impair, la propriété D est en défaut. Pourtant, la congruence $g + 1 \equiv 0 \pmod 2$ est vraie pour tous les nombres g impairs, donc, en vertu du théorème de Midy, le nombre 2 possède la propriété D. Y aurait-il alors contradiction? Non, mais, dans ce cas, pour la propriété D il faut doubler la longueur de la période $C_g\left(\frac{1}{2}\right)$ En effet, on a alors (pour $g = 2k + 1$):

$$C_g\left(\frac{1}{2}\right) = kk \quad \text{ce qui donne} \quad c_1 + c_2 = 2k = g - 1$$

$$R_g\left(\frac{1}{2}\right) = 1{,}1 \quad „ \quad „ \quad „ \quad r_1 + r_2 = 2 = m.$$

[19]) $\varphi(m)$ désigne la fonction, bien connue, d'Euler, qui exprime le nombre des nombres premiers par rapport à m et plus petits que lui. Cf. p. ex. G. H. Hardy et E. M. Wright. *An Introduction to the Theory of Numbers*, Oxford, 1945, p. 52, Winogradow: *Osnowy tieorii cziseł* (en russe). W. Sierpiński appelle cette fonction „fonction de Gauss". Cf. Sierpiński: *Teoria liczb*, Warszawa—Wrocław, 1950, p. 140.

[20]) Cf. p. ex. W. Sierpiński, op. cit., p. 193.

Une circonstance pareille ne se présente pas parmi les périodes à un chiffre $R_g\left(\frac{l}{m}\right)$ de longueur doublée, si $m > 2$. Pour que l'on ait $\lambda_g(m) = 1$, il faut que $g = km + 1$, (k — naturel). Nous avons alors les périodes:

$$C_g\left(\frac{l}{m}\right) = lk,\ lk \quad \text{ce qui donne} \quad c_1 + c_2 = 2lk$$

$$R_g\left(\frac{l}{m}\right) = l,\ l \quad \text{„ „ „} \quad r_1 + r_2 = 2l.$$

Pour que l'égalité $r_1 + r_2 = m$ ait lieu, il faudrait donc que l'égalité $2l = m$ soit vérifiée; comme $(l, m) = 1$ ceci n'est possible que lorsque $l = 1$, $m = 2$.

b) Pour le nombre $m = 4$ toutes les racines primitives sont données par la formule $g = 4k - 1$ ($k = 1, 2, \ldots$). Or, ces nombres g vérifient la congruence $g + 1 \equiv$ (mod. 4), ce qui prouve, d'après le théorème de M i d y, que le nombre 4 possède alors la propriété D.

c) Si g est une racine primitive de p^a (p — nombre premier > 2), alors $\lambda_g(p^a) = \varphi(p^a) = p^{a-1}(p - 1$. Donc, d'après la propriété IVa de le fonction $\lambda_g(m)$, on a $\lambda_g(p) = p - 1$. Le nombre $\lambda_g(p)$ est donc pair, ce qui prouve, en vertu du théorème IV, que le nombre p^a possède la propriété D dans le système g,

d) Si g est une racine primitive de $2p^a$, alors g est impair. De plus, on a $\lambda_g(2p^a) = \varphi(2p^a) = \varphi(p^a)$. Mais il résulte de l'égalité $(g, 2) = 1$ et de la propriété IIIb de la fonction $\lambda_g(m)$ que l'on a aussi $\lambda_g(2p^a) = \lambda_g(p^a)$. L'égalité $\lambda_g(p^a) = \varphi(p^a)$ est donc vérifiée, ce qui prouve que g est aussi une racine primitive de p^a. D'après ce qui a été dit sous c), le nombre p^a possède alors la propriété D dans le système g; des égalités $(g, 2) = 1$, $(p^a, 2) = 1$, et du théorème III il résulte enfin que le nombre $2p^a$ possède aussi la propriété D dans le système g.

§ 8. Les propriétés de la fonction $\lambda_g(m)$ permettent de dèmontrer le théorème suivant.

Théorème VI. — *Le nombre 2 possède la propriété D dans tout système, dont la base g est impaire; le nombre* 2^a, *a désignant un nombre naturel* > 1, *ne la possède que dans le cas où* $g = 4k - 1 = 2^{2+h}k' - 1 = 2^{\nu}k' - 1$, $(k', 2) = 1$, $h \geqslant 0$, $\nu = 2 + h$ *et a satisfait à la condition* $1 <$

Démonstration. — 1) La première partie du théorème resulte immédiatement d'apres le théorème de M i d y, de la congruence $g + 1 \equiv 0$ (mod. 2), qui est vérifiée pour tout nombre g impair.

Pour ce qui concerne le nombre 2^a, $a > 1$, remarquons d'abord que le nombre impair g ne peut avoir que l'une des deux formes suivantes:

a) $g = 4k + 1 = 2^{2+h} k' + 1 = 2^\nu \cdot k' + 1$ où $(k', 2) = 1, \nu = 2 + h$

b) $g = 4k - 1 = 2^{2+h} k' - 1 = 2^\nu \cdot k' - 1$ $h \geqslant 0$.

2) Or, d'après la propriété IVb de la fonctions $\lambda_g(m)$, nous avons alors pour $1 < a \leqslant \nu$:

dans le cas a):

$\lambda_g(2^a) = 1$; le nombre 2^a ne peut avoir la propriété D, car celle-ci exige que le nombre $\lambda_g(2^a)$ soit pair. D'ailleurs, même si l'on doublait la période du nombre 2^a dans le système g, on aurait $g + 1 = 2^\nu k' + 2 = 2(2^{\nu-1} k' + 1) \not\equiv 0 \pmod{2^a}$ pour $a = 2, 3, \ldots \nu$, ce qui montre, d'après le théorème de Midy, que le nombre 2^a ne peut avoir la propriété D.

Dans le cas b) on a: $\lambda_g(2^a) = 2$ et alors la congruence

$$g + 1 = 2^\nu k' \equiv 0 \pmod{2^a}$$

est vérifiée; dans ce cas le théorème de Midy montre que le nombre 2^a possède la propriété D.

3) Dans le cas $a = \nu + 1 = 3 + h$, nous avons, pour les deux types du nombre g: $\lambda_g(2^a) = 2^{a-\nu} = 2$. Mais alors, dans le cas a), nous avons: $g + 1 = 2^\nu k' + 2 = 2(2^{\nu-1} \cdot k' + 1) \not\equiv 0 \pmod{2^{\nu+1}}$, car $\nu > 2$; dans le cas b), de même, $g + 1 = 2^\nu k' \not\equiv 0 \pmod{2^{\nu+1}}$, car $(k', 2) = 1$. Cela prouve, en vertu du théorème de Midy, que le nombre 2^a, $a = \nu + 1$, ne possède pas la propriété D.

4) Considerons maitenant le cas $a > \nu + 1 = 3 + h$. Pour les deux types du nombre g nous avons alors $\lambda_g(2^a) = 2^{a-\nu} > 2$. Posons, pour abréger, $\lambda_g(2^a) = \lambda$. Pour que le nombre 2^a possède la propriété D, il faudrait, en vertu du théorème de Midy et de la définition du nombre λ, que la congruence

$$g^{\frac{\lambda}{2}} + 1 = g^{2^{a-\nu-1}} + 1 \equiv 0 \pmod{2^a}$$

fût vérifiée. Nous montrerons pourtant qu'elle ne l'est pas. En effet, d'après la définition du nombre λ et la propriété IVb de la fonction $\lambda_g(m)$, nous avons les relations

$$(1') \qquad g^\lambda - 1 = g^{2^{a-\nu}} - 1 \equiv 0 \pmod{2^a}$$

$$(2') \qquad g^\lambda - 1 = g^{2^{a-\nu}} - 1 \not\equiv 0 \pmod{2^{a+1}}$$

Puisque le nombre λ est pair, il résulte de (1')

$$(3') \qquad (g^{2^{a-\nu-1}} + 1)(g^{2^{a-\nu-1}} - 1) \equiv 0 \pmod{2^a}$$

où, g étant impair, les deux nombres $g^{2^{a-\nu-1}} + 1$ et $g^{2^{a-\nu-1}} - 1$

sont pairs, et $(g^{2^{a-\nu-1}}+1,\ g^{2^{a-\nu-1}}-1)=2$. Nous pouvons donc écrire

$$g^{2^{a-\nu-1}}+1=2m_1\ ;\ g^{2^{a-\nu-1}}-1=2m_2,$$

où m_1, m_2 sont des nombres naturels et $(m_1,\ m_2)=1$, car $m_1-m_2=1$. La congruence (3') prend la forme $4\,m_1\,m_2\equiv 0\ (\mathrm{mod.}\ 2^a)$, d'où il vient

$$(4') \qquad m_1\,m_2\equiv 0\ (\mathrm{mod.}\ 2^{a-2}),\quad a\geqslant 3$$

Comme $(m_1,\ m_2)=1$, il en résulte que :

A) ou bien m_1 est impair, m_2 pair et divisible par 2^{a-2}; mais alors

$$g^{\frac{\lambda}{2}}+1=g^{2^{a-\nu-1}}+1=2m_1\not\equiv 0\ (\mathrm{mod.}\ 2^a),\ \text{car}\ a>2,$$

B) ou bien m_1 est pair, m_2 impair. La congruence (4') entraîne donc $m_1\equiv 0\ (\mathrm{mod.}\ 2^{a-2})$, d'où $m_1=l\cdot 2^{a-2}$, l étant un nombre naturel. Si l était pair, soit $l=2l'$, on aurait:

$$2m_1=2l\cdot 2^{a-2}=2\cdot 2l'\cdot 2^{a-2}=l'\cdot 2^a$$

et

$$2m_1\cdot 2m_2=l'\,m_2\cdot 2^{a+1}$$

La congruence $g^{\frac{\lambda}{2}}-1=g^{2^{a-\nu}}-1=l'\,m_2\cdot 2^{a+1}\equiv 0\ (\mathrm{mod.}\ 2^{a+1})$ serait alors vérifiée, en contradiction avec (2'). Le nombre l doit donc être impair. On a $2m_1=2l\cdot 2^{a-2}=l\cdot 2^{a-1}$, mais alors $g^{2^{a-\nu-1}}+1=2m_1=l\cdot 2^{a-1}\not\equiv 0\ (\mathrm{mod}\ 2^a)$ car $(l\cdot 2)=1$.

La congruence $g^{\frac{\lambda}{2}}+1\equiv 0\ (\mathrm{mod.}\ 2^a)$ ne peut donc être vraie si $a>\nu+1$.

Notre théorème est ainsi démontré complétement.

§ 9. **Théorème VII.** — *Pour que le nombre m^n (m impair, n naturel) ait la propriété D dans le système g, $(g,\ m)=1$, il faut et il suffit que le nombre m l'ait aussi dans le même système.*

Démonstration. — Si le nombre naturel impair m possède la propriété D dans le système g, on a la congruence $g^a+1\equiv 0$ (mod. m), où a est un nombre naturel. Cette congruence peut s'écrire

$$g^a=-1+km, \qquad (17)$$

k étant un nombre naturel. En élévant les deux membres de l'égalité (17) à la puissance impaire m, nous obtenons l'égalité

$$g^{am}=-1+\frac{m}{1}km-\frac{m(m-1)}{1\cdot 2}k^2m^2+\frac{m(m-1)(m-2)}{1\cdot 2\cdot 3}k^3m^3\ldots.$$

où tous le termes du membre droit, à partir du troisième, sont divisibles par m^3. On peut donc l'écrire ainsi:

$$g^{am} = -1 + km^2 + k'm^3 = -1 + (k + k'm)\, m^2$$

ou encore

$$g^{am} = -1 + k_1 m^2, \tag{18}$$

où $k_1 = k + k'm$ est un nombre entier. Par conséquent, on a la congruence $g^{am} + 1 \equiv 0 \pmod{m^2}$, ce qui prouve que le nombre m^2 possède aussi la propriété D dans le système g.

En élevant maintenant les deux membres de l'égalité (18) à la puissance impaire m, nous obtiendrons, d'une façon analogue l'égalité

$$g^{am^2} = -1 + k_2 m^3,$$

où k_2 est un nombre entier, il en résulte que le nombre m^3 possède la propriété D dans le système g. De même, nous aurons les égalités

$$g^{am^3} = -1 + k_3 m^4; \quad g^{am^4} = -1 + k_4 m^5; \ldots.$$

Par induction, nous arrivons ainsi à la conclusion que la congruence

$$g^{am^{n-1}} + 1 \equiv 0 \pmod{m^n}$$

a lieu pour tous les nombres naturels $n \geqslant 1$.

Naus avons démontré que la condition du théorème est *suffisante.*

Supposons maintenant que le nombre m^n, où m et n sont naturels, ait la propriété D dans le système g; par consèquent, il existe, en vertu du théorème de Midy, un nombre naturel a tel que la congruence $g^a + 1 \equiv 0 \pmod{m^n}$, et a fortiori, la congruence $g^a + 1 \equiv 0 \pmod{m}$ soit vérifiée, ce qui prouve que le nombre m possède aussi la propriété D. Nous avons donc prouvé que la condition du théorème est aussi *nécessaire.* Notre théorème est ainsi démontré complètement.

Exemples. — Nous avons vu que le nombre impair 7 possède la propriété D dans le système $g = 10$; il résulte du théorème IV que les nombres 7^n doivent aussi l'avoir. En effet, si l'on représente p. ex. la fraction $\frac{1}{7^2} = \frac{1}{49}$ comme fraction décimale périodique, on voit aisément que la propriété D a lieu. Nous avons

$$C_{10}\left(\frac{1}{49}\right) = 020408163265306122448\,979591836734693877551$$

$$R_{10}\left(\frac{1}{49}\right) = 10,2,20,4,40,8,31,16,13,32,26,15,3,30,6,11,12,22,24,44,48,$$
$$|39,47,29,45,9,41,18,33,36,17,23,34,46,19,43,38,37,27,25,5,1$$

De même, nous avons:

$$C_3\left(\frac{1}{5}\right) = 01|21\,; \qquad R_3\left(\frac{1}{5}\right) = 3,4,|2,1$$

$$C_3\left(\frac{1}{25}\right) = 0010020110\,|\,2212202112$$

$$R_3\left(\frac{1}{25}\right) = 3,9,2,6,18,4,12,11,8,24,|22,16,23,19,7,21,13,14,17,1$$

§ 10. Nous allons établir l'important théorème que voici.

Théorème VIII. — *Si les nombres naturels $m_1, m_2, \ldots, m_n$ sont tous différents, la condition nécessaire et suffisante pour que le nombre $m = [m_1, m_2, \ldots, m_n]$ possède la propriété D dans le système g, $(g, m) = 1$, est que les deux conditions suivantes soient vérifiées simultanément:*

1) *tous les nombres $m_1, m_2, \ldots, m_n$ ont la propriété D dans le système g;*
2) *tous les nombres $\lambda_g(m_1), \lambda_g(m_2), \ldots, \lambda_g(m_n)$ ont le même degré de parité > 0. Le nombre $\lambda_g(m)$ a alors le même degré de parité que chacun des nombres $\lambda_g(m_i)$, $i = 1, 2, \ldots, n$.*

Remarque. — Nous appelons degré de parité du nombre pair $m = 2^a m$, où $(m, 2) = 1$, le nombre a.

Démonstration. — Nous montrerons, en premier lieu, que le théorème est vrai dans le cas $n = 2$.

a) Nous allons d'abord prouver que les conditions 1) et 2) constituent une condition suffisante pour que le nombre $m = [m_1, m_2]$ possède la propriété D. En effet, soit d'après 2):

$$\lambda_g(m_1) = \lambda_1 = 2^\delta a_1\,; \quad \lambda_g(m_2) = \lambda_2 = 2^\delta a_2\,,$$

où a_1, a_2, δ sont des nombres naturels et a_1, a_2 sont impairs En vertu de 1) et du théorème de Midy, on a les congruences.

$$g^{2^{\delta-1}a_1} + 1 \equiv 0 \pmod{m_1}; \quad g^{2^{\delta-1}a_2} + 1 \equiv 0 \pmod{m_2}$$

c'est-à-dire

$$\gamma^{a_1} + 1 \equiv 0 \pmod{m_1}; \quad \gamma^{a_2} + 1 \equiv 0 \pmod{m_2},$$

où l'on a posé $\gamma = g^{2^{\delta-1}}$. En désignant par t un nombre impair, on a aussi les congruences

$$\gamma^{a_1 t} + 1 \equiv 0 \pmod{m_1}; \quad \gamma^{a_2 t} + 1 \equiv 0 \pmod{m_2}$$

La congruence $\gamma^a + 1 \equiv 0 \pmod{m}$, où $a = [a_1, a_2]$, $m = [m_1, m_2]$ est donc également vérifiée, c'st-à-dire que l'on a

$$g^{2^{\delta-1}a} + 1 \equiv 0 \pmod{m}.$$

Cela prouve que m possède la propriété D dans le système g. D'après la propriété III de la fonction $\lambda_g(m)$, on a alors la relation

$$\lambda_g(m) = [\lambda_g(m_1), \lambda_g(m_2)] = 2^\delta \cdot [a_1, a_2] = 2^\delta a.$$

Le nombre $\lambda_g(m)$ a donc le même degré de parité que chacun des nombres $\lambda_g(m_1)$ et $\lambda_g(m_2)$, car, les nombres a_1 et a_2 étant impairs, a l'est aussi.

Ainsi nous avons démontré que les conditions 1) et 2) sont *suffisantes*.

b) Afin de montrer qu'elles sont *nécessaires*, supposons d'abord que la condition 1) soit remplie, alors que la condition 2) ne le soit pas. Posons donc $\lambda_g(m_1) = \lambda_1 = 2^{\delta_1} a_1$; $\lambda_g(m_2) = \lambda_2 = 2^{\delta_2} a_2$, où δ_1, δ_2, a_1, a_2 sont des nombres naturels, $\delta_1 - \delta_2 = \mu > 0$ et a_1, a_2 sont impairs.

Puisque la condition 1) est remplie, nous pouvons écrire les congruences

$$g^{2^{\delta_1-1}a_1} + 1 \equiv 0 \pmod{m_1}; \quad g^{2^{\delta_2-1}a_2} + 1 \equiv 0 \pmod{m_2},$$

c'st-à-dire

$$\gamma^{2^{\mu}a_1} + 1 \equiv 0 \pmod{m_1}; \quad \gamma^{a_2} + 1 \equiv 0 \pmod{m_2},$$

où l'on a posé $\gamma = g^{2^{\delta_2-1}}$.

Or, puisque $\mu > 0$, il n'existe pas de nombre du type $\gamma^a + 1$, qui soit le p. p. c. m. des nombres $\gamma^{2^{\mu}a_1} + 1$ et $\gamma^{a_2} + 1$, donc aussi le p. p. c.m. des nombres m_1, m_2, sinon, le nombre a devrait être[21]) pair, comme multiple impair du nombre pair $2^\mu a_1$, et en même temps impair, comme multiple impair du nombre impair a_2, ce qui est impossible.

La congruence $g^a + 1 \equiv 0 \pmod{m}$ n'est donc vraie pour aucune valeur naturelle de a; par conséquent le nombre m ne peut avoir la propriété D.

c) Supposons maintenant que la condition 1) ne soit pas remplie, ne faisant aucune hypothèse au sujet de la condition 2). Alors, au moins l'un des nombres m_1, m_2 ne possède pas la propriété D.

---

[21]) Le nombre $a^n + 1$ (a, n naturels) ne peut etre diviseur du nombre $a^{2ln} + 1$ (a, n naturel); cela résulte immediatement de la congruence

$$a^{2ln} + 1 = a^{2ln} - 1 + 2 = (a^n)^{2l} - 1 + 2 \equiv 2 \pmod{a^n + 1}$$

Admettons p. ex. que ce soit le nombres m_1, ne faisant aucune hypothèse sur m_2. On a donc la congruence $g^{\lambda_1} - 1 \equiv 0 \pmod{m_1}$, alors que d'après le théorème de Midy, $g^a + 1 \not\equiv 0 \pmod{m_1}$ pour tout nombre naturel a. Si t désigne un nombre naturel, la congruence $g^a + 1 \equiv 0 \pmod{m_1 t}$ n'est donc vérifiée pour aucun a naturel; il en résulte que la congruence $g^a + 1 \equiv 0 \pmod{m}$, où $m = [m_1, m_2]$, n'est vraie pour aucune valeur naturelle de a. Le nombre m ne possède donc pas la propriété D.

A fortiori, la congruence $g^a + 1 \equiv 0 \pmod{m}$ n'est pas vérifiée, lorsque les deux nombres m_1 et m_2 n'ont pas la propriété D. Par conséquent, le nombre D ne la possède pas non plus.

Nous avons donc montré que si la condition 1) n'est pas remplie, le nombre m ne possède pas la propriété D, indépendamment des hypothéses faites sur la condition 2).

De toutes les hypothèses possibles (en tout 4), que l'on peut faire au sujet des conditions 1) et 2), il en reste une, pour laquelle m possède la propriété D. Cette circonstance se présente lorsque les deux conditions sont vérifiées *simultanément*.

Nous avons donc prouvé que les conditions 1) et 2) sont *nécessaires* et, ainsi, le théorème est démontré pour $n = 2$.

On peut montrer qu'il est aussi vrai pour $n > 2$. En effet, soient 3 nombres naturels differents m_1, m_2, m_3 et posons $m = [m_1, m_2, m_3]$. Puisque $m = [m_1, m_2, m_3] = [[m_1, m_2], m_3] = [\overline{m}, m_3]$ où $\overline{m} = [m_1, m_2]$, le nombre m possède la propriété D dans le système g, ainsi qui nous venons de le prouver, seulement dans le cas, où les deux nombres $\overline{m}$ et m_3 la possèdent aussi, et où les nombres $\lambda_g(\overline{m})$ et $\lambda_g(m_3)$ ont le même degré de parité > 0. Mais le même raisonnement, apliqué au nombre $\overline{m} = [m_1, m_2]$, montre que celui-ci ne possède la propriété D que lorsque les deux nombres m_1, m_2 l'ont aussi et que les deux nombres $\lambda_g(m_1)$ et $\lambda_g(m_2)$ ont le même degré de parité > 0.

Puisque $\lambda_g(\overline{m})$ doit avoir le même degré de parité que $\lambda_g(m_1)$ et $\lambda_g(m_2)$, et $\lambda_g(\overline{m})$ — le même degré de parité que $\lambda_g(\overline{m})$ et $\lambda_g(m_3)$, le nombre m ne possédera la propriété D dans le système g que si tous les nombres m_1, m_2, m_3, la possèdent aussi et si tous les nombres $\lambda_g(m_1)$, $\lambda_g(m_2)$, $\lambda_g(m_3)$ ont le même degré de parité > 0 et $\lambda_g(m) = [\lambda_g(m_1), \lambda_g(m_2), \lambda_g(m_3)]$ conserve le même degré de parité.

On peut ainsi étendre le théorème VIII à une quantité quelconque de nombres différents $m_1, m_2, \ldots, m_n$. Le théorème est donc démontré.

§ 11. Les théorèmes VII et VIII, ainsi que la propriété VIb de la fonction $\lambda_g(m)$ permettent d'énoncer le corollaire suivant.

Corollaire I. — *Si les nombres impairs* $m_1, m_2, \ldots, m_k$ *sont tous differents, la condition nécessaire et suffisante pour que le nombre* $m = [m_1^{n_1}, m_2^{n_2}, \ldots, m_k^{n_k}]$ *possède la propriété D dans le système g, est que tous les nombres* $m_1, m_2, \ldots, m_k$ *l'aient aussi dans le même système et que tous les nombres* $\lambda_g(m_1), \lambda_g(m_2), \ldots, \lambda_g(m_k)$ *aient le même degré de parité* > 0.

En particulier, si $(m_i, m_j) = 1$ pour $i, j = 1, 2, \ldots, k$, alors

$$m = m_1^{n_1} m_2^{n_2} \ldots m_k^{n_k} \tag{19}$$

Admettons, en outre, que $m_i = p_i$, où p_i $(i = 1, 2 \ldots, k)$ est un nombre premier > 2, et remplaçons n, par a, l'expression (19) prendra la forme

$$m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k},$$

qui n'est autre que la décomposition du nombre impair m en facteurs premiers. Du corollaire I et du théorème IV on déduit comme conséquence le théorème suivant, trés important pour notre problème.

Théorème de Jenkins[22]). — La condition nécessaire et suffisante pour que le nombre impair $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ possède la propriété D dans le système g est que tous les nombres $\lambda_g(p_i)$, $i = 1, 2, \ldots k$, aient le même degré de parité > 0.

Pour la démonstration il suffit de remarquer que, d'après le corollaire I, la condition nécessaire et suffisante pour que le nombre impair $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ possède la propriété D dans le système g, est que tous les nombres p_i, $i = 1, 2, \ldots k$, la possèdent aussi et que tous les nombres $\lambda_g(p_i)$ aient le même degré de parité > 0. Mais, en vertu du théorème IV, pour que les nombres p_i possèdent la propriété D, il faut et il suffit que les nombres $\lambda_g(p_i)$ soient pairs. Le problème se ramène donc au degré de parité des nombres $\lambda_g(p_i)$.

Quant au nombre pair $m = 2^a m$, $(m, 2) = 1$, on déduit des théorèmes VI et VIII le

Corollaire II. — *Pour que le nombre pair* $m = 2^a m$, $(m, 2) = 1$, $a > 1$, *posséde la propriété D dans le systéme g,* $(g, 2) \quad 1$, *il faut et*

---

[22]) Cf. Math. Quest. Educ. Times, 7, 1867, 31—2. Jenkins a établi ce théorème pour $g = 10$ et $(m. 10) = 1$, mais il est évident qu'il est aussi vrai pour toute base naturelle g pourvu que $(m, g) = 1$.

il suffit que toutes les conditions suivantes soient remplies simultanément:

1) $g = 4k - 1 = 2^{2+h}k' - 1 = 2^{\nu}k' - 1$ où $\nu = 2 + h$, $h \geqslant 0$, $(k', 2) = 1$,
2) $1 < a \leqslant \nu$,
3) *m possède la propriété D dans le système g,*
4) *le degré de parité du nombre $\lambda_g(m)$ est 1.*

Le cas $m = 2m$, $(m, 2) = 1$ a été étudié au théorème III.

§ 12. En profitant des propriétés de la fonction $\lambda_g(m)$ nous pouvons déduire du théorème de Jenkins quelques nouvelles conséquences.

Tout nombre premier $p > 2$ peut être mis sous l'une des deux formes $4k - 1$ ou $4k + 1$.

1) Si $p = 4k - 1$, alors $\varphi(p) = p - 1 = 4k - 2 = 2(2k - 1)$, donc $\varphi(p)$ est alors un nombre pair de degré 1. Par conséquent le degré de parité de chacun des diviseurs pairs du nombre $\varphi(p)$ est 1.

2) Si $p = 4k + 1$, alors $\varphi(p) = p - 1 = 4k = 2^2k$; dans ce cas $\varphi(p)$ est un nombre pair de degré au moins 2 (k peut être pair ou non). Il existe donc des diviseurs pairs du nombre $\varphi(p)$, dont le degré de parité est arbitraire, mais ne surpasse pas celui du nombre $4k$.

$\lambda_g(p)$ étant toujours diviseurs de $\varphi(p)$, le raisonnement indiqué sous 1) permet de tirer du théorème IV la conclusion suivante: si p^a, où p est un nombre premier de la forme $4k - 1$, possède la propriété D dans le système g, alors $\lambda_g(p)$ est un nombre pair de degré 1; si p est de la forme $4k + 1$, il résulte de la remarque 2) que $\lambda_g(p)$ est un nombre pair, dont le degré de parité peut être arbitraire > 0, mais ne surpasse pas celui du nombre $4k$.

Du théorème de Jenkins résulte donc le

Corollaire III [22a]. — *Si les nombres premiers impairs $p_1, p_2, \ldots, p_n$ sont tous de la forme $4k - 1$ et possèdent tous la propriété D dans le système g, alors le nombre $m = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ la possède aussi dans le même système.*

Pourtant le nombre $m = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$ où p_i ($i = 1, 2, \ldots n$) sont des nombres premiers > 2 de la forme $4k + 1$, qui ont la pro-

[22a] Dans une lettre adressée à M. Sierpiński (que celui-ci a bien voulu mettre à ma disposition), M. Warmus (Wrocław) a communiqué le 14. XI. 1947 qu'il a établi la proposition suivante: le nombre $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ possède la propriété D dans le système $g = 10$, $(g, n) = 1$, si aucun des nombres p_i (i = 1, 2, ..., k) n'est de la forme $4s + 1$ et si le nombre 10 est non-reste quadratique pour chacun d'eux.

priété D dans le système g, peut ne pas l'avoir dans le même système, si les nombres $\lambda_g(p_i)$ n'ont pas tous le même degré de parité > 0.

Si l'on a l'égalité $\lambda_g(m) = \varphi(m)$, le nombre g est, comme on le sait, racine primitive du nombre m. Dans le cas $m = p$ cette égalité prend la forme $\lambda_g(p) = p - 1$. Le nombre $\lambda_g(p)$ est alors pair de degré 1 si $p = 4k-1$, de degré au moins 2 si $p = 4k+1$.

Du théorème de Jenkins on déduit encore le

Corollaire IV. — *Si g est une racine primitive de tous les nombres $p_1, p_2, \ldots, p_n$ premiers > 2 de la forme $4k-1$, alors le nombre $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ possède la propriété D dans le système g.*

Pourtant cette conclusion peut ne pas être vraie dans le cas, où les nombres p_i $(i = 1, 2, \ldots n)$ sont tous du type $4k+1$ et g est une racine primitive de tous ces nombres.

Théorème IX. — *Si dans le nombre impair $m = p^{\alpha_1} \cdot p^{\alpha_2} \ldots p_n^{\alpha_n}$ au moins deux nombres premiers p_r, p_s sont de types différents $4k-1$ et $4k+1$, et ont tous les deux g comme racine primitive, alors le nombre m ne possède pas la propriété D dans le système g.*

Démonstration. —Si $p_r = 4k-1$ et $p_s = 4k'+1$, g étant racine primitive de ces deux nombres, on a

$$\lambda_g(p_r) = \varphi(p_r) = 4k - 2 = 2(2k-1),$$

et

$$\lambda_g(p_s) = \varphi(p_s) = 4k' = 2^2 \cdot k'.$$

Alors les nombres $\lambda_g(p_r)$ et $\lambda_g(p)$ n'ont pas le même degré de parité. D'après le théorème de Jenkins, le nombre m ne peut donc avoir la propriété D dans le système g, c. q. f. d.

Ainsi p. ex. le nombre $119 = 7 \cdot 17$ n'a pas la propriété D dans le système $g = 10$, bien que les nombres 7 et 17 la possèdent et que 10 soit racine primitive de chacun d'eux. C'est parce que le nombre 7 est du type $4k-1$ et 17 du type $4k+1$. Nous avons donc: $\lambda_{10}(7) = 6 = 2 \cdot 3$; $\lambda_{10}(17) = 16 = 2^4$; les nombres $2 \cdot 3$ et 2^4 ont différents degrés de parité.

§ 13. Afin de savoir si le nombre $m = 2^\alpha p^{\alpha_1} \cdot p^{\alpha_2} \ldots p_n^{\alpha_n}$, où $\alpha > 1$ et $p_i > 2$, $(i = 1, 2, \ldots n)$ possède la propriété D dans le système g, où $(g, 2) = 1$, il faut et il suffit de calculer les nombres

$$\lambda_g(2^\alpha),\ \lambda_g(p_1),\ \lambda_g(p_2), \ldots,\ \lambda_g(p_n)$$

et de déterminer leur degré de parité. Si celui-ci est le même pour tous, le nombre m possède la propriété D, sinon la propriété D n'a pas lieu.

Dans le cas $\alpha = 1$ il est superflu d'étudier le nombre $\lambda_g(2)$.

Exemples.

I. $g = 10,\ p = 11,\ \lambda_{10}(11^a) = 11^{a-1} \cdot 2.$

Puisque $\lambda_{10}(11) = 2$, le nombre 11^a possède la propriété D dans le système $g = 10$. En effet, nous avons $C_{10}\left(\frac{1}{11}\right) = 09$, $R_{10}\left(\frac{1}{11}\right) = 10{,}1$.

$C_{10}\left(\frac{1}{121}\right) = 0\,0\,8\,2\,6\,4\,4\,6\,2\,8\,0 \mid 9\,9\,1\,7\,3\,5\,5\,3\,7\,1\,9$

$R_{10}\left(\frac{1}{121}\right) = 10,\ 100,\ 32,\ 78,\ 54,\ 56,\ 76,\ 34,\ 98,\ 12,\ 120, \mid 111,\ 21,\ 89,\ 43,\ 67,\ 65,\ 45,\ 87,\ 23,\ 109,\ 1.$

On voit que la propriété D a lieu. Signalons encore les intéressantes propriéts des périodes $C_{10}\left(\frac{1}{211}\right)$ et $R_{10}\left(\frac{1}{121}\right)$, en particulier la curieuse symétrie des termes équidistants des 2 extrémités de la période $R_{10}\left(\frac{1}{121}\right)$, p. ex. les nombres 32 et 23, 78 et 87, etc. où les chiffres des unités et des dizaines sont échangés.

Les nombres 10 et 1, 100 et 109, 120 et 111 semblent échapper à cette symétrie Pourtant une petite transformation permet de la rétablir. En effet, nous avons

$$\begin{aligned} 10 &= \quad\quad = 10, & 1 &= \quad\quad = \overline{0}\ 1, \\ 100 &= 9 \cdot 10 + 10 = \overline{9}\ \overline{10}, & 109 &= 10 \cdot 10 + 9 = \overline{10}\ \overline{9}, \\ 120 &= 11 \cdot 10 + 10 = \overline{11}\ \overline{10}, & 111 &= 10 \cdot 10 + 11 = \overline{10}\ \overline{11}. \end{aligned}$$

Remarque. — Lest nombres $\overline{10}$ et $\overline{11}$ doivent être considérés comme „chiffres".

II. $g = 10,\ m = 11011 = 7 \cdot 11^2 \cdot 13.$

Le nombre 11011 possède la propriété D, car $\lambda_{10}(7) = 6$, $\lambda_{10}(11) = 2$, $\lambda_{10}(13) = 6$, et les nombres 2 et 6 ont le même degré de parité 1. En effet, nous avons

$C_{10}\left(\frac{1}{11011}\right) = 000\ 090\ 818\ 272\ 636\ 454\ 454\ 636\ 272\ 818\ 090 \mid 999\ 909\ 181\ 727\ 363\ 545\ 545 \ldots$

III. $g = 10,\ m = 1309 = 7 \cdot 11 \cdot 17.$

On voit aisément que le nombre 1309 ne possède pas la propriété D dans le système 10, car $\lambda_{10}(7) = 6$, $\lambda_{10}(11) = 2$, $\lambda_{10}(17) = 16$ et les nombres 6, 2 et 16 ont différents degrés de parité

III.

Application de la fonction $\lambda_g(n)$ a l'étude de la congruence chinoise $2^n - 2 \equiv 0 \pmod{n}$.

§1 4. Les Chinois supposaient que le nombre $2^n - 2$ n'est divisible par n que lorsque n est un nombre premier. Or, M. Banachiewicz[23]) a trouvé 7 nombres naturels composés $n \leqslant 2000$, pour lesquels l'hypothèse des Chinois est en défaut. Ce sont les nombres

(19) $341 = 11 \cdot 31$; $561 = 3 \cdot 11 \cdot 17$; $645 = 3 \cdot 5 \cdot 43$; $1105 = 5 \cdot 13 \cdot 17$; $1387 = 19 \cdot 73$; $1729 = 7 \cdot 13 \cdot 19$; $1905 = 3 \cdot 5 \cdot 127$.

On voit qu'ils sont tous impairs.

M. Sierpiński[24]) a démontré le théorème suivant:

Théorème. Si nombre impair n est tel que le nombre $2^n - 2$ soit divisible par n, le nombre impair $k = 2^n - 1$ possède aussi cette propriété. De plus, si n est composé, le nombre k l'est aussi.

Il en résulte qu'il existe une *infinité* de nombres impairs composés n, pour lesquels l'hypothèse des Chinois est en défaut

§. 15. Appliquons la fonction $\lambda_g(n)$ à l'étude de ce problème. Puis que $\lambda_g(n) = \lambda$ n'est autre que l'exposant, auquel appartient le nombre g modulo n, on a la congruence

$$g^{\lambda} - 1 \equiv 0 \pmod{n}, \tag{20}$$

où λ est le plus petit nombre naturel, pour lequel cette congruence est vraie. La congruence $g^a - 1 \equiv 0 \pmod{n}$ entraîne donc la congruence $a \equiv 0 \pmod{\lambda_g(n)}$ et réciproquement[25]).

L'hypothese de Chinois sur la divisibilité du nombre $2^n - 2$ par n équivaut évidemment à la congruence

$$2^n - 2 \equiv 0 \pmod{n}. \tag{21}$$

Il faut distinguer ici 2 cas, selon que n est impair ou pair.

---

[23]) T. Banachiewicz: Comptes Rendus de la Soc. des Sciences et des Lettres de Varsovie, Classe III, Année 2 (1909), p. 9. Je cite d'après W. Sierpiński: *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n-2)/n$. Colloquium Math., vol. I, fasc. 1, p. 9, Wrocław 1947.

[24]) W. Sierpiński: *Remarque* citée plus haut et aussi du même auteur *Teoria liczb*, Warszawa—Wrocław, 3-e éd., 1950, p. 61 et p. 66 exercice 15. **Remarque.** — En vue des applications j'ai énoncé le théorème sous une forme un peu différente, pourtant sans en changer la teneur.

[25]) Cf. W. Sierpiński, *Teoria liczb*, 1950, p. 173.

1) Si n est impair, posons $n = m$; la congruence (21) se réduit alors à la congruence

(22) $$2^{n-1} - 1 \equiv 0 \pmod{m},$$

2) Si n est pair, posons $n = 2m$, la congruence (21) prend alors la forme

(23) $$2^{2m-1} - 1 \equiv 0 \pmod{m},$$

d'où il résulte que m doit être impair

Dans les 2 congruences (22) et (23) le nombre m est donc impair.

Ces remarques permettent d'énoncer le lemme suivant.

Lemme. — *Pour que la congruence chinoise* $2^n - 2 \equiv 0 \pmod{n}$ *soit satisfaite, il faut et il suffit que l'une des 2 congruences suivantes soit vraie:*

1) $n = m, \quad m - 1 \equiv 0 \pmod{\lambda_2(m)},$

2) $n = 2m, \quad 2m - 1 \equiv 0 \pmod{\lambda_2(m)},$

où m *désigne un nombre impair.*

§ 16. Il est possible maintenant de donner une démonstration du théorème de M. Sierpiński, utilisant les propriétés de la fonction $\lambda_g(n)$.

Supposons que le nombre impair n vérifie la congruence chinoise

(24) $$2^n - 2 \equiv 0 \pmod{n}.$$

D'aprés le lemme précédent, la congruence

(25) $$n - 1 \equiv 0 \pmod{\lambda_2(n)}$$

est donc vraie. En prenant le nombre impair $k = 2^n - 1$, pour lequel on a evidement

(26) $$\lambda_2(k) = n,$$

nous avons $k - 1 = 2^n - 2$. Donc, en tenant compte de (24) et (26), il vient: $k - 1 \equiv 0 \pmod{\lambda_2(k)}$, ce qui prouve, d'après le lemme précédent, que le nombre k satisfait à la congruence chinoise.

Supposons maitenant que le nombre impair n est composé, p. ex. $n = pq$; le nombre impair $k = 2^{pq} - 1$ est aussi composé, car il est divisible par $2^p - 1$ et $2^q - 1$. Il en résulte immédiatement le théorème de M. Sierpiński.

§ 17. En appliquant encore les propriétés de la fonction $\lambda_g(n)$, il sera facile de démontrer le théorème suivant, bien connu.

Théorème A[26]). — Tous les nombres premiers, tous les nombres de Mersenne, de Fermat et tous les nombres pseudo-premiers satisfont à la congruence chinoise.

[26]) Cf. W. Sierpiński: *Teoria liczb*, 1950, p. 61 et p. 66, ex. 14, cf. aussi p. 60 (nombres pseudo-premiers).

Démonstration. — a) Les nombres premiers $p > 2$ vérifient la congruence chinoise $2^p - 2 \equiv 0 \pmod{p}$ c'est-à-dire la congruence $2^{p-1} - 1 \equiv 0 \pmod{p}$ donc aussi la congruence $p - 1 \equiv 0 \pmod{\lambda_2(p)}$, (d'après le lemme), car cela résulte immediatement du petit théorème de Fermat; d'ailleurs $p-1 = \varphi(p)$ et $\lambda_2(p)$ est diviseur de $\varphi(p)$. Le théorème étant vrai pour le nombre 2, nous voyons qu'il est vrai pour tous les nombres premiers.

b) Les nombres de Mersenne sont les nombres impairs du type $M_p = 2^p - 1$ où p est premier. Or, il résulte de a) et du théorème de Sierpiński qu'ils vérifient la congruence chinoise lorsqe $p > 2$. Le théorème étant vrai pour le nombre $M_2 = 2^2 - 1 = 3$ (nombre premier, cf. a), il est vrai pour tous les nombres de Mersenne.

c) On appelle nombres de Fermat les nombres impairs du type $F_k = 2^{2^k} + 1$, k naturel. Puisque

$$\lambda_2(F_k) = 2 \cdot 2^k = 2^{k+1} \tag{27}$$

et que la congruence

$$F_k - 1 = 2^{2^k} \equiv 0 \pmod{2^{k+1}} \tag{28}$$

est vérifée pour tout nombre naturel $k \geqslant 0$, (27) et (28) permettent de conclure que la congruence $F_k - 1 \equiv 0 \pmod{\lambda_2(F_k)}$ a aussi lieu, ce qui prouve, en vertu du lemme, que le théorème est vrai pour tous les nombres de Fermat.

d) Les nombres pseudo-premiers[27]) sont les nombres impairs n satisfaisant à la congruence

$$g^{n-1} - 1 \equiv 0 \pmod{n} \tag{29}$$

pour **toute** valeur de g, première à n. Pour $g = 2$, cette congruence prend la forme

$$2^{n-1} - 1 \equiv 0 \pmod{n};$$

le nombre n étant impair, on a donc aussi $2^n - 2 \equiv 0 \pmod{n}$.

Ainsi notre théorème se trouve complètement établi.

§ 18. On démontre aussi aisément le théorème suivant.

Théorème X. — *Si un nombre impair de la forme $n = 2^m + 1$ où m désigne un nombre entier non négatif, satisfait à la congruence chinoise $2^n - 2 \equiv 0 \pmod{n}$ alors il est un nombre de Fermat.*

Démonstration. — Pour le nombre $n = 2^m + 1$ on a $\lambda_2(n) = 2m$; la congruence $n - 1 \equiv 0 \pmod{\lambda_2(n)}$ (cf. le lemme) prend

[27]) S. Sispanow: Bolletino di Matematica 14, (1941), pp. 99—106.

la forme: $2^m \equiv 0 \pmod{2m}$, c'est-à-dire $2^{m-1} \equiv 0 \pmod{m}$, d'où il résulte que $m = 2^h$, h étant un nombre entier non négatif, verifiant l'inégalité

$$h \leqslant m - 1 = 2^h - 1$$

Pourtant cette inégalité est vraie pour tout nombre entier non négatif. Donc $n = 2^{2^h} + 1$, $n = F_h$, c. g. f. d.

Dans de nombreux cas, les nombres de Mersenne[28]) et de Fermat[29]) sont composés. Ains: $M_{11} = 2^{11} - 1 = 2048 - 1 = 23 \cdot 89$; $M_{23} = 2^{23} - 1 = 8388608 - 1 = 47 \cdot 178481$; $M_{29} = 2^{29} - 1 = 536870912 - 1 = 233 \cdot 2304167$; $F^5 = 2^{2^5} + 1 = 641 \cdot 6700417$; $F_6 = 2^{2^6} + 1 = 274177 \cdot 67280421310721$.

Les nombres pseudo-premiers[30]) sont tous des nombres composés impairs du type $n = p_1 p_2 \ldots p_k$, où $k \geqslant 3$. P. ex. $561 = 3 \cdot 11 \cdot 17$; $1105 = 5 \cdot 13 \cdot 17$; $1729 = 7 \cdot 13 \cdot 19$; $2821 = 7 \cdot 13 \cdot 31$; $63973 = 7 \cdot 13 \cdot 19 \cdot 37$; $294409 = 37 \cdot 73 \cdot 109$; $509033161 = 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109$.

Ces exemples montrent à quel point l'hypothèse des Chinois était fausse.

Remarquons encore que parmi les 7 nombres, trouvés par T. Banachiewicz, 3 sont pseudo-premiers: 561, 1105, 1729.

§ 19. Dans la suite nous aurons besoin des propriétés IV et V de la fonction $\lambda_g(n)$, pour cela, nous y poserons $g = 2$.

Considerons maintenant un nombre impair arbitraire $m = p_1^{\alpha_1} p_1^{\alpha_2} \ldots p_k^{\alpha_k}$, et posons $m' = p_1 p_2 \ldots p_k$.

Quand existe-t-il des racines de la congruence

$$m - 1 \equiv 0 \ [\text{mod. } \lambda_2(m)] \tag{30}$$

ou encore de la congruence

$$2m - 1 \equiv 0 \ [\text{mod. } \lambda_2(m)], \tag{31}$$

donc aussi, d'après le lemme, des racines de la congruence chinoise? A. Supposons d'abord que $m = p^\alpha$, c'est-à-dire que l'indice $k = 1$. Les congruences (30) et (31) prennent alors la forme

$$p^\alpha - 1 \equiv 0 \ [\text{mod. } \lambda_2(p^\alpha)] \tag{32}$$

$$2p^\alpha - 1 \equiv 0 \ [\text{mod. } \lambda_2(p^\alpha)]. \tag{33}$$

---

[28]) Je cite les nombres M_{11}, M_{23}, M_{29} d' après W. Sierpiński: *Teoria liczb*, 1950, 3-e éd., pp. 120—1.

[29]) Pour les nombres F_5, F_6 cf. G. H. Hardy et E. M. Wright: *An Introduction to the Theory of Numbers*, Oxford, 2nd ed., 1945, p. 14.

[30]) Les nombres pseudo-premiers sont cités d'après O. Ore: *Numbers Theory and its History*, New York, 1948, 1 ed., pp. 331—9.

Nous allons distinguer 2 cas: 1) $1 \leqslant a \leqslant \nu = \nu_2(p)$
2) $a > \nu$.

Dans le cas 1) les congruences (32) et (33) deviennent

(34) $$p^a - 1 \equiv 0 \ [\text{mod. } \lambda_2(p)]$$

(35) $$2p^a - 1 \equiv 0 \ [\text{mod. } \lambda_2(p)]$$

Puisque $\lambda_2(p)$ est diviseur du nombre $\varphi(p) = p - 1$, est celui-ci est diviseur de $p^a - 1$, alors il est évident que la congruence (34) est vérifiée, alors que (35) ne l'est pas

Remarque. — Il est clair que tous les nombres premiers $p > 2$ sont contenus dans le cas 1). Quant au nombre 2, il est évident qu'il satisfait à la congruence chinoise, comme nous l'avons remarqué plus haut.

Dans le cas 2), les congruences (32) et (33) prennnent, d'après la propriété IVa de la fonction $\lambda_g(n)$, la forme

$$p^a - 1 \equiv 0 \ [\text{mod. } p^{a-\nu} \cdot \lambda_2(p)]; \quad 2p^a - 1 \equiv 0 \ [\text{mod. } p^{a-\nu} \cdot \lambda_2(p)].$$

Il est clair qu'aucune de ces congruences n'est vérifiée, car aucune des 2 congruences

$$p^a - 1 \equiv 0 \ (\text{mod. } p^{a-\nu})$$
$$2p^a - 1 \equiv 0 \ (\text{mod. } p^{a-\nu})$$

n'a lieu.

B. Admettons maintenant que $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, où $k > 1$. Nous distinguerons encore 2 cas: 1) $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ pour tous les $i = 1, 2, \dots, k$, 2) $a_i > \nu_i$, pour un indice $i = j$ au moins. Dans le cas 1), en vertu de la propriété V A de la fonction $\lambda_g(n)$, les congruences (30) et (31) prennent le forme

$$m - 1 \equiv 0 \ [\text{mod. } \lambda_2(m')]$$
$$2m - 1 \equiv 0 \ [\text{mod. } \lambda_2(m')].$$

Dans le cas 2), les mêmes congruences (30) et (31) prendront, d'après la propriété V B de la fonction $\lambda_g'n)$, la forme

(36) $$m - 1 \equiv 0 \ \left(\text{mod.} \left[p_1^{a_1-\nu_1}\lambda_2(p_1), p_2^{a_2-\nu_2}\lambda_2(p_2), \dots p_j^{a_j-\nu_j}\lambda_2(p_j), \lambda_2(p_{j+1}), \lambda_2(p_{j+2}), \dots \lambda_2(p_k)\right]\right)$$

(37) $$2m - 1 \equiv 0 \ \left(\text{mod.} \left[p_1^{a_1-\nu_1}\lambda_2(p_1), p_2^{a_2-\nu_2}\lambda_2(p_2), \dots p_j^{a_j-\nu_j}\lambda_2(p_j), \lambda_2(p_{j+1}), \lambda_2(p_{j+2}), \dots, \lambda_2(p_k)\right]\right)$$

lorsque l' inégalité $a_i > \nu_i$ a lieu pour tous les indices $i = 1, 2, \dots, j$, où $1 \leqslant j \leqslant k$ et où l' on admet que, dans la décomposition du nombre m en facteurs premiers, on a écrit d'abord tous les facteurs p pour lesquels $a_i > \nu_i$.

Or, les congruence (36) et (37) ne peuvent être vérifiées, car les congruences

$$m - 1 \equiv 0 \pmod{p_i^{a_i - \nu_i}}$$

$$2m - 1 \equiv 0 \pmod{p_i^{a_i - \nu_i}}$$

ne sont jamais satisfaites.

En rassemblant ces résultats nous obtenons le théorème suivant:

Théorème XI. *Les seuls nombres qui satisfont à la congruence chinoise* $2^n - 2 \equiv 0 \pmod{n}$ *sont les suivants:*

1) *tous les nombres premiers* $n = p$,
2) *tous les nombres impairs* $n = p^a$, *où* $1 \leqslant a \leqslant \nu = \nu_2(p)$,
3) *tous les nombres impairs* $n = m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, *où* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ *pour* $i = 1, 2, \dots k$, *pourvu que la congruence*

$$m - 1 \equiv 0 \pmod{\lambda_2(m')}, \quad m' = p_1 p_2 \dots p_k$$

ait lieu,

4) *tous les nombres pairs* $n = 2m = 2 p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, *où* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ *pour* $i = 1, 2, \dots k \geqslant 2$, *à condition que la congruence*

$$2m - 1 \equiv 0 \pmod{\lambda_2(m')}, \quad m' = p_1 p_2 \dots p_k$$

soit vérifiée.

Remarque. — Il est facile de voir que le No 1 du théorème XI est un cas particulier du No 2, sauf pour le cas $p = 2$, et que le No 2 est un cas particulier du No 3.

§ 20. Les nombres impairs $n = p^a$, dont il est question dans le No 2 du théorème XI, pour lesquels $1 < a \leqslant \nu$, doivent être très rares. Autant que je le sache, on ne connait actuellement qu'un seul de ce genre, $n = 1093^2$, pour lequel on a la congruence[31]) $2^{1092} - 1 \equiv 0 \pmod{1093^2}$. En vertu de la définition du nombre $\lambda_g(n)$, il résulte de cette congruence que $\lambda_2(1093^2)$ est diviseur du nombre $1092 = 1093 - 1 = \varphi(1093)$. On sait que le nombre $\lambda_2(1093)$ est aussi diviseur de $\varphi(1093)$. Or, d'après le propriété IVa de la fonction $\lambda_g(n)$, la suite $\lambda_g(p^a)$, $a = 1, 2, 3, \dots$ ne contient jamais 2 diviseurs d i f f é r e n t s du nombre $\varphi(p)$. On a donc l'égalité $\lambda_2(1093) = \lambda_2(1093^2)$; de là, en vertu de la propriété IVa de la fonction $\lambda_g(n)$, il résulte immédiatement que $\nu_2(1093) \geqslant 2$.

Pourtant, pour les nombres premiers $p > 2$, on a, en général, l'égalité $\nu_2(p) = 1$.

31) Cf. G. H. H a r d y et E. M. W r i g h t : *An Introduction to the Theory of Numbers*, Oxford, 1945, 2-e éd., p. 73.

§ 21. On ignore, jusqu'à présent[31a] s'il existe des nombres pairs composés, dont il est question au No 4 du théorème XI, qui satisfassent à la congruence chinoise. On peut établir le corollaire suivant.

Corollaire V. — *Le nombre impair $n > 1$ et le nombre pair $2n$ ne peuvent vérifier tous les deux la congruence chinoise $2^n - 2 \equiv 0$ (mod. n).*

Démonstration[32]). — Si ces nombres vérifiaient la congruence chinoise, les 2 congruences

(38) $\qquad 2^n - 2 \equiv 0 \pmod{n}$ et $2^{2n} - 2 \equiv 0 \pmod{2n}$,

donc a fortiori aussi la congruence

(39) $\qquad 2^{2n} - 2 \equiv 0 \pmod{n}$.

devraient être simultanément vraies. En retranchant (38) de (39) nous aurions

$$2^{2n} - 2^n = 2^n (2^n - 1) \equiv 0 \pmod{n},$$

donc, puisque $(n, 2) = 1$, nous aurions aussi

(40) $\qquad 2^n - 1 \equiv 0 \pmod{n}$.

En retranchant ensuite (38) de (40) nous aurions alors $1 \equiv 0 \pmod{n}$, ce qui est impossible, car $n > 1$. Les nombres n et $2n$, où $(n, 2) = 1$, ne peuvent donc simultanément vérifier la congruence chinoise.

§ 22. D'après la remarque du § 19 il est clair que le No 3 du théorème XI est vrai pour tous les nombres impairs (premiers et composés), qui satisfont à la congruence chinoise. On peut donc énoncer le.

Corollaire VI. — *Tous les nombres impairs n, verifiant la congruence chinoise $2^n - 2 \equiv 0$ (mod. n), sont du type $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, où $1 \leqslant a_i \leqslant \nu_i = \nu_2 (p_i)$, $i = 1, 2, \dots, k$, ν_i étant le plus grand nombre, naturel satisfaisant à la congruence $2^{\lambda_i} - 1 \equiv 0$ (mod. $p_i^{\nu_i}$), où $\lambda_i = \lambda_2 (p_i)$.*

Les nombres pairs composés, vérifiant la congruence chinoise, s'ils existent, sont tous du type $n = 2 p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, où $1 \leqslant a_i \leqslant \nu_i = \nu_2 (p_i)$, $i = 1, 2, \dots k$ et $k \geqslant 2$.

De ce corollaire ainsi que du théorème A on déduit immédiatement le

---

[31a]) N. G. W. H. Beeger a démontré récemment qu'il existe une infinité de nombres paires satisfaisants à la congruence chinoise: le plus petit d'eux, trouvé par Lehmer, est 2. 73. 1103. Cfr. Beeger N. G. W. H: *On even numbers m dividing $2^m - 2$.* Amer. Math. Montly, 58, 1951, 553—555. et Mathematical Reviews, Vol. 13, No 4, April 1952, p. 320.

[32]) Je dois cette courte démonstration à M. le Professeur Bernacki, alors que la mienne, beaucoup plus longue, procédait par induction.

Corollaire VII. — *Tous les nombres des* Fermat *et de* Mersenne *sont des nombres impairs du type* $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, *où* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$, $i = 1, 2, \dots, k$.

Les nombres pseudo-premiers sont tous, nous l'avons vu, des nombres impairs du type $n = p_1 p_2 \dots\dots p_k$ *où* $k \geqslant 3$. Les nombres de Fermat et de Mersenne, cités à titre d'exemples, ainsi que la remarque du § 20 suggèrent l'hypothèse suivante:

Hypothèse. — *Les nombres de* Fermat *et de* Mersenne *sont des nombres impairs du type* $n = p_1 p_2 \dots p_k$ *où* $k \geqslant 1$.

La question reste ouverte. Aucun couple de nombres de Fermat ne pouvant avoir de p. g. c. d. supérieur à 1, si l'hypothèse était vraie, nous aurions une preuve immédiate du fait qu'il existe une infinité de nombres premiers [33]).

§ 23. En appliquant la fonction $\lambda_g(n)$ à l'étude de la congruence chinoise, nous obtenons un moyen simple et facile de vérifier si un nombre donné n satisfait à cette congruence ou non.

Ainsi, prenons les nombres de Banachiewicz et quelques des nombres pseudo-premiers. Tous ces nombres étant impairs, il suffit, en vertu du lemme, de faire la preuve avec la congruence $n - 1 \equiv 0 \pmod{\lambda_2(n)}$.

En effet, pour les nombres de Banachiewicz, nous avons, en vertu de la propriété IIIa de la fonction $\lambda_g(n)$:

1) $\lambda_2(341) = [\lambda_2(11), \lambda_2(31)] = [10; 5] = 10$; $\quad 341 - 1 \equiv 0 \pmod{10}$
2) $\lambda_2(561) = [\lambda_2(3), \lambda_2(11), \lambda_2(17)] = [2; 10; 8] = 40$; $\quad 561 - 1 \equiv 0 \pmod{40}$
3) $\lambda_2(645) = [\lambda_2(3), \lambda_2(5), \lambda_2(43)] = [2; 4; 14] = 28$; $\quad 645 - 1 \equiv 0 \pmod{28}$
4) $\lambda_2(1105) = [\lambda_2(5), \lambda_2(13), \lambda_2(17)] = [4; 12; 8] = 24$; $\quad 1105 - 1 \equiv 0 \pmod{24}$
5) $\lambda_2(1387) = [\lambda_2(19), \lambda_2(73)] = [18; 9] = 18$; $\quad 1387 - 1 \equiv 0 \pmod{18}$
6) $\lambda_2(1729) = [\lambda_2(7), \lambda_2(13), \lambda_2(19)] = [3; 12; 18] = 36$; $\quad 1729 - 1 \equiv 0 \pmod{36}$
7) $\lambda_2(1905) = [\lambda_2(3), \lambda_2(5), \lambda_2(127)] = [2; 4; 7] = 28$; $\quad 1905 - 1 \equiv 0 \pmod{28}$

Prenons maintenant un nombre pseudo-premier, p. ex. $2821 = 7 \cdot 13 \cdot 31$. En vertu de la propriété IIIa de la fonction $\lambda_g(n)$ nous avons

$$\lambda_2(2821) = [\lambda_2(7), \lambda_2(13), \lambda_2(31)]. \tag{41}$$

Le symbole $a \mid b$ indiquant, comme d'habitude, que a est diviseur de b, remarquons que pour tous les nombres premiers p et g premiers à p, l'on a $\lambda_g(p) \mid \varphi(p)$, donc aussi $\lambda_2(p) \mid \varphi(p)$. Nous avons donc $\lambda_2(7) \mid 6$;

[33]) Cf. la démonstration de Pólya pour l'existence d'une infinité de nombres premiers, citée par G. H. Hardy et E. M. Wright dans *An Introduction to the Theory of Numbers*, Oxford, 1945, p. 14.

$\lambda_2(13) \mid 12$; $\lambda_2(31) \mid 30$. Il en resulte que $[\lambda_2(7), \lambda_2(13), \lambda_2(31)] \mid [6; 12; 30]$. Puisque $[6; 12; 30] = 60$, en vertu de (41) l'on a $\lambda_2(2821) \mid 60$. On verifie aisement que $60 \mid 2820$, donc $\lambda_2(2821) \mid 2820$; ainsi la congruence $2821 - 1 \equiv 0 \pmod{\lambda_2(2821)}$ est vraie, ce qui prouve que le nombre 2821 satisfait à la congruence chinoise.

Streszczenie

W pracy tej podaję rezultaty zastosowania funkcji $\lambda_g(m)$, której własności omawiam w cz. I, do badania ułamków okresowych (cz. II) i kongruencji chińskiej $2^n \equiv 2 \pmod{n}$ (cz. III).

Spośród wielu własności ułamków okresowych rozpatruję tu tylko tzw. własność D, polegającą na tym, że cyfry w okresie cyfr ułamka nieprzywiedlnego $\frac{l}{m}$, rozwiniętego w układzie pozycyjnym o podstawie g, począwszy od połowy okresu, dopełniają się z odpowiednimi cyframi od początku okresu do liczby $g-1$, analogiczne zaś reszty w okresie reszt dopełniają się do liczby m.

Omawiam więc własność D liczby m w układach g i $\bar{g}$, gdy zachodzą zależności: $g \equiv g \pmod{m}$ (Tw. I), lub $g\bar{g} \equiv 1 \pmod{m}$ (Tw. II), oraz w układzie g, gdy g jest pierwiastkiem pierwotnym liczby m (Tw. V). Podaję warunki konieczne i dostateczne istnienia własności D dla liczb p^a (p — liczba pierwsza > 2) (Tw. IV), 2^a, (Tw. VI), m^n (m — liczba nieparzysta), (Tw. VII), $m = [m_1, m_2, \ldots, m_k]$, (Tw. VIII) $2^a m$, (m — liczba nieparzysta), (Tw. III i Wn. II), $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ (Tw. Jenkinsa — podane tu jako wniosek). W końcu, opierając się na własnościach funkcji $\lambda_g(m)$, wyprowadzam z tzw. Jenkinsa wnioski dotyczące istnienia własności D dla liczby $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ w zależności od tego, czy liczby p_i ($i = 1, 2, \ldots k$) są liczbami typu $4k + 1$ czy typu $4k - 1$, oraz w zależności od tego, czy podstawa układu g jest, czy nie jest pierwiastkiem pierwotnym liczb p_i. (Wn. III i IV, Tw. IX).

W zastosowaniu funkcji $\lambda_g(m)$ do badania kongruencji chińskiej $2^n \equiv 2 \pmod{n}$ otrzymuję jako główny wynik warunki konieczne i dostateczne na to, by liczba nieparzysta $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ lub parzysta $n = 2 p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ spełniała tę kongruencję (Tw. XI), z którego jako prosty już wniosek wynika pewna interesująca, przy tym nowa własność liczb Mersenne'a i Fermata, które, jak wiadomo spełniają także kongruencją chińską.

W końcu cz. III — podaję metodę sprawdzania, czy liczba dana n spełnia, czy nie, kongruencję chińską, metoda ta opiera się na własnościach funkcji $\lambda_g(m)$.

Spełniając miły obowiązek wdzięczności, wyrażam serdeczne podziękowanie prof. W. Sierpińskiemu i prof. A. Mostowskiemu za życzliwe odniesienie się do wyników mej pracy, prof. M. Biernackiemu za cenne wskazówki i krytyczne uwagi przy ostatecznej redakcji tej pracy, oraz prof. A. Bieleckiemu za przejrzenie i przychylną ocenę.

Część I

Funkcja $\lambda_g(m)$.

W pracy niniejszej stale posługuję się symbolem $\lambda_g(m)$. Oznacza on długość okresu ułamka nieprzywiedlnego $\frac{l}{m}$ rozwiniętego w układzie pozycyjnym o podstawie g, przy czym liczby g, m są względem siebie pierwsze; zakładamy bowiem, że okres ułamka $\frac{l}{m}$ jest okresem czystym, tzn. posiada same tylko wyrazy regularne rozwinięcia systematycznego przy zasadzie g.

Liczba $\lambda_g(m)$ jest niczym innym, jak tylko wykładnikiem, do którego należy liczba g według modułu m. Zachodzi więc kongruencja $g^{\lambda} \equiv 1 \pmod{m}$, gdzie $\lambda = \lambda_g(m)$, przy czym λ, jest najmniejszą liczb a, b, zaś symbolem $[a, b]$ — najmniejszą wspólną wielokrotną

Funkcja $\lambda_g(m)$ posiada szereg interesujących własności, które jednak jako znane, podaję bez dowodów.

Oznaczając symbolem (a, b) — największy wspólny podzielnik liczb a, b, zaś symbolem $[a, b]$ — najmniejszą wspólną wielokrotną tych liczb, własności funkcji $\lambda_g(m)$ wyrażamy w postaci następującej:

Własność I. Jeśli $\bar{g} \equiv g \pmod{m}$, to $\lambda_{\bar{g}}(m) = \lambda_g(m)$.

Własność II. Jeśli $g\bar{g} \equiv 1 \pmod{m}$, to $\lambda_{\bar{g}}(m) = \lambda_g(m)$.

Własność III. Jeśli $m_i \neq m_j$ dla $i, j = 1, 2, 3, \ldots, n$,
to $\lambda_g([m_1, m_2, \ldots, m_n]) = [\lambda_g(m_1), \lambda_g(m_2), \ldots, \lambda_g(m_n)]$.

Jako szczególne przypadki tej własności mamy tu:

Własność IIIa. Jeśli $m_i \neq m_j$, $(m_i, m_j) = 1$ dla $i, j = 1, 2, 3, \ldots, n$,
to $\lambda_g(m_1 m_2 m_3 \ldots m_n) = [\lambda_g(m_1), \lambda_g(m_2), \ldots \lambda_g(m_n)]$.

Własność IIIb. Jeśli $(m, 2) = 1$ i $(g, 2) = 1$, to $\lambda_g(2m) = \lambda_g(m)$.

Własność IIIc. Jeśli $m = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, gdzie p_i $(i = 1, 2, \dots, n)$ oznacza liczbę pierwszą, to $\lambda_g(m) = [\lambda_g(p_1^{a_1}), \lambda_g(p_2^{a_2}), \dots, \lambda_g(p_n^{a_n})]$.

Własność IVa. Jeśli p oznacza liczbę pierwszą > 2, $(p, g) = 1$, zaś ν oznacza największą wartość liczby naturalnej t, spełniającej kongruencję $g^{\lambda} \equiv 1 \pmod{p^t}$, gdzie $\lambda = \lambda_g(p)$, to

$$\begin{aligned} \lambda_g(p^a) &= \lambda_g(p) && \text{dla } 1 \leqslant a \leqslant \nu = \nu_g(p) \\ \lambda_g(p^a) &= p^{a-\nu} \cdot \lambda_g(p) && a > \nu \end{aligned}$$

Własność IVb. Jeśli $g = 4k \pm 1 = 2^{2+h} k' \pm 1 = 2^{\nu} k' \pm 1$, gdzie $(k', 2) = 1$, $h \geqslant 0$.

$$\begin{aligned} \text{to } \lambda_g(2^a) &= 1 && \text{dla } 1 = a \\ \lambda_g(2^a) &= \lambda_g(2^2) && 1 < a \leqslant \nu = 2 + h \\ \lambda_g(2^a) &= 2^{a-\nu} && a > \nu \end{aligned}$$

przy czym $\lambda_g(2^2) = 1$ lub 2 zależnie od tego ,czy g jest liczbą typu $4k + 1$, czy typu $4k - 1$.

Własność V. Jeśli $m = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$, zaś $m' = p_1 p_2 \dots p_n$, przy czym p_i $(i = 1, 2, \dots, n)$ oznacza liczbę pierwszą > 2, to zachodzą związki

A. $\lambda_g(m) = \lambda_g(m')$ gdy $1 \leqslant a_i \leqslant \nu_i = \nu_g(p_i)$ dla $i = 1, 2, 3, \dots, n$.

B. $\lambda_g(m) = [p_1^{a_1-\nu_1} \lambda_g(p_1), p_2^{a_2-\nu_2} \lambda_g(p_2), \dots, p_k^{a_k-\nu_k} \lambda_g(p_k), \lambda_g(p_{k+1}), \dots, \lambda_g(p_n)]$ gdy nierówność $a_i > \nu_i$ zachodzi dla wskaźników $i = 1, 2, \dots, k$, gdzie $1 \leqslant k \leqslant n$, przy czym zakładamy, że w rozwinięciu liczby m na czynniki pierwsze umieszczono na początku wszystkie te czynniki p_i, dla których jest $a_i > \nu_i$.

C. $\lambda_g(2^a m) = [\lambda_g(2^a), \lambda_g(m)]$ gdy $(g, 2) = 1$, $(m, 2) = 1$.

Można tu zauważyć, że własność V jest bardziej szczególnym rozwinięciem własności IIIc (po uwzględnieniu własności IVa i IVb).

Nazywając stopniem parzystości liczby $m = 2^a m$, gdzie $(m, 2) = 1$, liczbę a, mamy jeszcze

Własność VIa. Liczby $\lambda_g(p^a)$ i $\lambda_g(p)$, gdzie p oznacza liczbę pierwszą > 2, mają ten sam stopień parzystości.

Własność VIb. Liczby $\lambda_g(m^n)$, $\lambda_g(m)$ i $\lambda_g(m')$ gdzie $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ $m' = p_1 p_2 \dots p_k$, zaś p_i $(i = 1, 2, \dots, k)$ oznacza liczbę pierwszą > 2, mają ten sam stopień parzystości.

Część II.

Dopełnianie się cyfr i reszt w okresie czyli własność *D*.

Niektóre liczby całkowite m posiadają osobliwą własność: jeśli ułamek właściwy nieprzywiedlny $\frac{l}{m}$ rozwinąć na ułamek okresowy w układzie pozycyjnym o podstawie g, to cyfry w okresie cyfr począwszy od połowy okresu dopełniają się z odpowiednimi cyframi od jego początku do liczby $g-1$, analogiczne zaś reszty w okresie reszt dopełniają się do liczby m.

Własność tę liczby m nazywamy własnością *D*. Jest ona niezależna od liczby l, zależy zaś tylko od liczb m i g.

W dalszym ciągu pracy zakładam stale, że mamy do czynienia z okresem czystym, tzn. że w rozwinięciu systematycznym ułamka $\frac{l}{m}$ przy zasadzie g występują tylko wyrazy regularne rozwinięcia. Zakładamy więc stale, że $(m, g) = 1$, $(m, l) = 1$.

Jeśli długość okresu $\lambda_g(m)$ wynosi $2a$, to oznaczając przez c_i $(i = 1, 2, \ldots,)$ cyfry w okresie cyfr, zaś przez r_i odpowiednie reszty w okresie reszt, własność *D* wyrażamy dwoma następującymi równościami:

$$c_i + c_{a+i} = g - 1 \tag{1}$$

$$r_i + r_{a+i} = m \qquad i = 1, 2, \ldots, a. \tag{2}$$

Oznaczając jeszcze przez $C_g\left(\frac{l}{m}\right)$ okres cyfr ułamka $\frac{l}{m}$ w układzie g, zaś przez $R_g\left(\frac{l}{m}\right)$ analogiczny okres reszt, własność *D* ilustrujemy następującym przykładem:

$$C_{10}\left(\frac{1}{7}\right) = 1\ 4\ 2\ |\ 8\ 5\ 7 \quad \text{gdzie} \quad 1+8 = 4+5 = 2+7 = 9$$

$$R_{10}\left(\frac{1}{7}\right) = 3, 2, 6, |\ 4, 5, 1, \qquad 3+4 = 2+5 = 6+1 = 7$$

Jak widać liczba 7 posiada własność *D* w układzie $g = 10$.

Powstaje zagadnienie. *Jakie liczby m i w jakich układach g posiadają własność D?*

Zagadnieniu temu poświęcam całą część II tej pracy.

Zwracając uwagę na równości (1) i (2), przypominam, co już

wykazał Catalan (1842), że jeśli równość (2) zachodzi dla pewnego wskaźnika i, to zachodzi także dla wskaźnika $i+1$. Stwierdzam również, że można wykazać, że wtedy równość (2) zachodzi także dla wskaźnika $i-1$.

Opierając się na tej własności równości (2), wykazuję, że równość (2) pociąga za sobą równość (1). Odwrotna zaś zależność istnieje tylko wtedy, gdy równość (1) słuszna jest dla wszystkich wskaźników $i = 1, 2, \ldots, a$.

E. Midy (1836) i W. H. H. Hudson (1864) podali twierdzenie, że jeśli $\lambda_{10}(m) = 2n$, $(m, 10) = 1$ i $(m, 10^n - 1) = 1$, to liczba m posiada własność D w układzie $g = 10$.

O. Schlömilch (1880) podał twierdzenie, że na to by liczba m posiadała własność D w układzie $g = 10$, potrzeba, by była ona dzielnikiem liczby $10^n + 1$, gdzie $2n = \lambda_{10}(m)$, przy czym $(m, 10) = 1$.

G. R. Perkins (1841) stwierdził, że jeśli w okresie $R_g\left(\frac{1}{m}\right)$ zachodzi równość $r_n = m - 1$ to liczba m posiada własność D w układzie g.

Wykazuję, że twierdzenie Perkinsa wynika z twierdzenia Schlömilcha, to zaś ostatnie jest równoważne twierdzeniu podanemu najpierw przez Midy'ego, które, jako podstawowe dla postawionego tu problemu. formułuję w sposób następujący:

Twierdzenie Midy'ego. Warunkiem koniecznym i dostatecznym na to, by liczba m posiadała własność D w układzie g, jest by istniała liczba naturalna a, spełniająca kongruencję $g^a + 1 \equiv 0 \pmod{m}$. Jeśli przy tym a jest najmniejszą taką liczbą, to wtedy $\lambda_g(m) = 2a$.

Opierając się na tym twierdzeniu i na własnościach funkcji $\lambda_g(m)$ wyprowadzam kilka nowych lub mało znanych twierdzeń i wniosków, dotyczących omawianego tu problemu Oto one:

Twierdzenie I. *Jeśli liczba m posiada własność D w układzie g i $\bar{g} \equiv g \pmod{m}$, to liczba m posiada tę własność także w układzie $\bar{g}$.*

Zwraca się przy tym uwagę na związki: $\bar{r}_i = r_i$; $\bar{c}_i = c_i + kr_i$, gdzie $\bar{c}_i$, $\bar{r}_i$ oznaczają cyfry i reszty okresów ułamka $\frac{1}{m}$ w układzie $\bar{g} = g + km$. $(i = 1, 2, \ldots)$.

Twierdzenie II. *Jeśli liczba m posiada własność D w układzie g i $g\bar{g} \equiv 1 \pmod{m}$, to liczba m posiada tę własność także w układzie $\bar{g}$.*

Zwraca się przy tym uwagę na związek $\overline{r_i} = r_{\lambda-i}$ $(i = 1, 2, \ldots,)$ gdzie $\lambda = \lambda_g(m)$.

T w i e r d z e n i e III. *Liczba parzysta* $\overline{m} = 2m$, *gdzie* $(m, 2) = 1$, *posiada własność D w układzie g, gdzie* $(g, 2) = 1$, *wtedy i tylko wtedy, gdy liczba m posiada tę własność w tym układzie.*

Zagadnieniem własności D dla liczb pierwszych $p > 2$ zajmowali się G o o d w y n (1802), F. T. P o s e l g e r (1827), P. L a f i t t e (1851), W. H. H. H u d s o n (1864), J. W. L. G l a i s h e r (1878), stwierdzając, że jeśli $\lambda_g(p)$ jest liczbą parzystą, to liczba p posiada własność D. W pracy niniejszej wykazuję, że słuszne jest także ogólniejsze

T w i e r d z e n i e IV. *Liczba* p^a, *gdzie p oznacza liczbę pierwszą* > 2, *a zaś liczbę naturalną, posiada własność D w układzie g wtedy i tylko wtedy, gdy* $\lambda_g(p)$ *jest liczbą parzystą, przy tym oczywiście* $(g, p) = 1$.

W dowodzie korzystam z twierdzenia M i d y'e g o i z własności funkcji $\lambda_g(m)$. Podobnie, opierając się na twierdzeniu M i d y'e g o i własnościach funkcji $\lambda_g(m)$, wyprowadzam dwa następujące twierdzenia:

T w i e r d z e n i e V. *Jeśli g jest pierwiastkiem pierwotnym liczby m, to liczba m posiada własność D w układzie g.*

T w i e r d z e n i e VI. *Liczba 2 posiada własność D w każdym układzie o nieparzystej podstawie g. Liczba zaś* 2^a, *a — liczba naturalna* > 1, *posiada tę własność tylko w przypadku* $g = 4k - 1 = 2^{2+h}k' - 1 = 2^\nu k' - 1$, *gdzie* $\nu = 2 + h$, $h \geqslant 0$, $(k', 2) = 1$, *gdy a spełnia nierówność* $1 < a \leqslant \nu$.

Następujące zaś

T w i e r d z e n i e VII. *Jeśli m oznacza liczbę nieparzystą, zaś n oznacza liczbę naturalną, to liczba* m^n *posiada własność D w układzie g,* $(g, m) = 1$, *wtedy i tylko wtedy, gdy liczba m ją posiada w tym układzie,*

dowodzę przy pomocy indukcji matematycznej. Mianowicie, jeśli liczba m posiada własność D w układzie g, to w myśl twierdzenia M i d y'e g o zachodzi kongruencja $g^a + 1 \equiv 0 \pmod{m}$, czyli równość $g^a = -1 + km$, gdzie k jest pewną liczbą całkowitą. Podnosząc obie strony tej równości do potęgi m (m — z założenia nieparzyste), otrzymujemy równość $g^{am} = -1 + k_1 m^2$, gdzie k_1 jest pewną liczbą całkowitą, czyli kongruencję $g^{am} + 1 \equiv 0 \pmod{m^2}$, co dowodzi, w myśl twierdzenia M i d y'e g o, że liczba m^2 również

posiada własność D w układzie g. W podobny sposób wykazujemy, że mają własność D w układzie g także liczby m^3, m^4, ..., m^n. Dowód zależności odwrotnej jest bardzo prosty. Jeśli bowiem liczba m^n posiada własność D w układzie g, to istnieje taka liczba naturalna α, że słuszna jest kongruencja $g^\alpha + 1 \equiv 0 \pmod{m^n}$, tym bardziej jest wtedy słuszna kongruencja $g^\alpha + 1 \equiv 0 \pmod{m}$, co dowodzi, że liczba m też posiada własność D w układzie g.

Inny już charakter ma następujące

T w i e r d z e n i e VIII. *Jeśli liczby naturalne* $m_1, m_2, \ldots, m_n$ *są od siebie różne, to liczba* $m = [m_1, m_2, \ldots, m_n]$ *posiada własność* D *w układzie* g, $(g, m) = 1$, *wtedy i tylko wtedy, gdy jednocześnie spełnione są oba następujące warunki:*

1) *wszystkie liczby* $m_1, m_2, \ldots, m_n$ *mają własność* D *w układzie* g,
2) *wszystkie liczby* $\lambda_g(m_1), \lambda_g(m_2), \ldots, \lambda_g(m_n)$ mają ten sam *stopień parzystości* > 0.

Liczba zaś $\lambda_g(m)$ zachowuje wtedy stopień parzystości wspólny liczbom $\lambda_g(m_i)$, $(i = 1, 2, \ldots, n)$.

Przez stopień parzystości liczby $2^\alpha m$, gdzie $(m, 2) = 1$, rozumiemy liczbę naturalną α.

W dowodzie wykazuję najpierw słuszność tego twierdzenia dla przypadku $n = 2$, następnie uogólniam je na n dowolne. W przypadku $n = 2$ wykazuję najpierw a) dostateczność podanego warunku. Dla wykazania zaś jego konieczności zakładam b), że zachowany jest warunek 1) twierdzenia, ale warunek 2) nie jest zachowany, oraz c), że warunek 1) twierdzenia nie jest spełniony, natomiast o warunku 2) nic nie zakładamy. Wykazuję, że w przypadkach b) i c) własność D nie ma miejsca. Pozostaje więc tylko przypadek a), w którym mamy własność D.

Z twierdzeń VIII i VII wobec własności VIb funkcji $\lambda_g(m)$ wyprowadzam.

W n i o s e k I. *Jeśli liczby nieparzyste* $m_1, m_2, \ldots m_k$ *są od siebie różne, to liczba* $m = [m_1^{n_1}, m_2^{n_2}, m_k^{n_k}]$, *gdzie liczby* n_1, n_2, n_k *są liczbami naturalnymi, posiada własność* D *w układzie* g *wtedy i tylko wtedy, gdy wszystkie liczby* m_i $(i = 1, 2, \ldots k)$ *posiadają tę własność w układzie* g, *oraz gdy wszystkie liczby* $\lambda_g(m_i)$ *mają ten sam stopień parzystości* > 0.

Z wniosku tego i twierdzenia IV wynika już natychmiast bardzo ważne dla postawionego tu problemu, podane już w 1867 r.:

Twierdzenie Jenkinsa. Liczba nieparzysta $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ posiada własność D w układzie g wtedy, i tylko wtedy gdy wszystkie *liczby* $\lambda_g(p_i)$ $(i = 1, 2, \dots k)$ mają ten sam stopień parzystości > 0.

a także (wobec twierdzenia VI)

Wniosek II. *Liczba parzysta* $m = 2^a m$, *gdzie* $(m, 2) = 1$, $a > 1$, *posiada własność* D *w układzie* g, $(g, 2) = 1$ *wtedy i tylko wtedy, gdy równocześnie spełnione są wszystkie następujące warunki*

1) $g = 4k - 1 = 2^{2+h} k' - 1 = 2^\nu k' - 1$, *gdzie* $\nu = 2 + h$, $h \geqslant 0$, $(k', 2) = 1$.
2) $1 < a \leqslant \nu$;
3) *liczba* m *posiada własność* D *w układzie* g,
4) *stopień parzystości liczby* $\lambda_g(m)$ *wynosi 1,*

Opierając się teraz na twierdzeniu Jenkinsa i wykorzystując własności funkcji $\lambda_g(m)$ wyprowadzam następujące wnioski:

Wniosek III. *Jeśli liczby pierwsze nieparzyste* $p_1, p_2 \dots, p_n$ *są wszystkie formy* $4k - 1$ *i wszystkie mają własność* D *w układzie* g, *to tę własność ma w tymże układzie także liczba* $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$

Wniosek IV. *Jeśli* g *jest pierwiastkiem pierwotnym dla wszystkich liczb* $p_1, p_2, \dots p_n$, *pierwszych* > 2, *typu* $4k - 1$, *to liczba* $m = p_1^{\alpha_1} p_2^{\alpha_2} p_n^{\alpha_n}$ *posiada własność* D *w układzie* g.

a także

Twierdzenie IX. *Jeśli w liczbie nieparzystej* $m = p_1^{\alpha_1} p_2^{\alpha_2} \dots, p_n^{\alpha_n}$ *przynajmniej dwie liczby pierwsze* p_r, p_s *należą do odmiennych typów* $4k - 1$ *i* $4k + 1$, *zaś* g *jest dla obu tych liczb pierwiastkiem pierwotnym, to liczba* m *nie posiada własności* D *w układzie* g.

Część III.

Zastosowanie funkcji $\lambda_g(m)$ do badania chińskiej kongruencji $2^n - 2 \equiv 0 \pmod{n}$

Chińczycy sądzili, że liczba $2^n - 2$ jest podzielna całkowicie przez n tylko wtedy, gdy n jest liczbą pierwszą. Tymczasem T. Banachiewicz (1909) znalazł 7 liczb naturalnych złożonych $n \leqslant 2\,000$, dla których przypuszczenie Chińczyków okazało się błędne. W. Sierpiński (1947) zaś wykazał, że istnieje nieskończenie wiele liczb nieparzystych złożonych n, dla których hipoteza Chińczyków jest błędna. Udowodnił on mianowicie następujące

Twierdzenie. Jeśli liczba nieparzysta n ma tę własność, że liczba $2^n - 2$ dzieli się całkowicie przez n, to liczba nieparzysta $k = 2^n - 1$ ma tę własność również: jeśli przy tym liczba n jest

złożona, to liczba k jest też złożona.

Do zagadnienia tego stosuję funkcję $\lambda_g(m)$ i ustalam przede wszystkim następujący

Lemmat. *Kongruencja chińska* $2^n - 2 \equiv 0 \,(mod.\, n)$ *może być spełniona wtedy i tylko wtedy, gdy będzie spełniona jedna z dwu następujących kongruencji:*

1) $n = m, \quad m - 1 \equiv 0 \,[mod.\, \lambda_2(m)]$

2) $n = 2m, \quad 2m - 1 \equiv 0 \,[mod.\, \lambda_2(m)]$

gdzie m *oznacza liczbę nieparzystą.*

Opierając się na tym lemmacie daję krótki dowód twierdzenia W. Sierpińskiego, podanego wyżej, następnie korzystając z własności funkcji $\lambda_g(m)$, udowadniam, znane zresztą

Twierdzenie A. Wszystkie liczby pierwsze, wszystkie liczby Mersenne'a, Fermat'a i tzw. pseudo-pierwsze spełniają kongruencję chińską,

oraz nowe (lub mało znane)

Twierdzenie X. *Jeśli liczba nieparzysta postaci* $n = 2^m + 1$, *gdzie* m *oznacza liczbę całkowitą nieujemną, spełnia kongruencję chińską* $2^n - 2 \equiv 0 \,(mod.\, n)$, *to jest ona liczbą* Fermata.

po czym stawiam następujące zagadnienie:

Jakim warunkom winna podlegać liczba nieparzysta $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, *by liczba* m *lub* $2m$ *spełniała kongruencję chińską?*

Jako odpowiedź na to zagadnienie otrzymuję

Twierdzenie XI. *Kongruencja chińska* $2^n - 2 \equiv 0 \,(mod\ n)$ *jest spełniona tylko i wyłącznie przez następujące liczby:*

1) *wszystkie liczby pierwsze* $n = p$,

2) *wszystkie liczby nieparzyste* $n = p^a$, *gdzie* $1 \leqslant a \leqslant \nu = \nu_2(p)$

3) *wszystkie liczby nieparzyste* $n = m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, *gdzie* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ *dla* $i = 1, 2, \ldots k$, *pod warunkiem, że jest spełniona kongruencja:* $m - 1 \equiv 0 \,[mod.\, \lambda_2(m')]$, *przy czym* $m' = p_1 p_2 \ldots p_k$.

4) *wszystkie liczby parzyste* $n = 2m = 2 p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, *gdzie* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ *dla* $i = 1, 2, \ldots k \geqslant 2$, *o ile jest spełniona kongruencja:* $2m - 1 \equiv 0 \,[mod.\, \lambda_2(m')]$.

Odnośnie liczb złożonych parzystych, spełniających omawianą kongruencję chińską, to nie wiadomo dotąd, czy takie istnieją*) w pewnym jednak związku z tym zagadnieniem jest

*) N. G. W. H. Beeger udowodnił ostatnio (gdy praca niniejsza była oddana do druku), że istnieje nieskończenie wiele liczb parzystych, spełniających omawianą kongruencję.

W n i o s e k V. *Liczby nieparzyste n i parzyste $2n$ nie mogą jednocześnie spełniać kongruencji chińskiej* $2^n - 2 \equiv 0 \pmod{n}$.

Bezpośrednio z twierdzenia XI wypływają następujące wnioski:

W n i o s e k VI. *Wszystkie liczby nieparzyste n, spełniające kongruencję chińską* $2^n - 2 \equiv 0 \pmod{n}$ *są liczbami typu* $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, *gdzie* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ *dla* $i = 1, 2, \dots k$, *przy czym* ν_i *jest największą liczbą naturalną, spełniającą kongruencję* $2^{\lambda_i} - 1 \equiv 0 \pmod{p_i^{\nu_i}}$, *gdzie* $\lambda_i = \lambda_2(p_i)$.

Liczby zaś parzyste złożone, spełniające powyższą kongruencję chińską, o ile istnieją, są wszystkie typu $n = 2 p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, *gdzie* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ *dla* $i = 1, 2, \dots k$, *przy czym* $k \geqslant 2$.

W n i o s e k VII. *Wszystkie liczby* F e r m a t a i M e r s e n n e ' a *są liczbami nieparzystymi typu* $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, *gdzie* $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$ *dla* $i = 1, 2, \dots k$.

Wobec tego, że liczba $\nu_2(p)$ rzadko przekracza wartość 1, nasuwa się dość prawdopodobna

H i p o t e z a. *Liczby* F e r m a t a i M e r s e n n e ' a *są liczbami nieparzystymi typu* $n = p_1 p_2 p_3 \dots p_k$, gdzie $k \geqslant 1$

W zakończeniu części III-ej podaję metodę sprawdzania, czy liczba n spełnia kongruencję chińską, czy nie, opartą na własnościach funkcji $\lambda_g(m)$. Metodę tę stosuję do liczb znalezionych przez T. B a n a c h i e w i c z a oraz do niektórych liczb pseudo-pierwszych.

Р е з ю м е

В этой работе излагаю результаты применения функции $\lambda_g(m)$, которой свойства разбираю в ч. 1, к исследованию периодических дробей (ч. 2) и китайского сравнения $2^n \equiv 2 \pmod{n}$ (ч. 3).

Из многих свойств периодических дробей рассматриваю здесь только т. н. свойство D. Состоит оно в том, что цифры в периоде цифр несократимой дроби $\frac{l}{m}$ разложенной в позиционной системе с основанием g, начиная от половины периода дополняются с соответвующими цифрами от начала периода к числу $g - 1$, а аналогичные остатки в периоде остатков дополняются к числу m.

Разбираю, следовательно, свойство D числа m в системах g и g, когда имеет место зависимость: $g \equiv g \pmod{m}$ (Т. 1) или $gg \equiv 1 \pmod{m}$ (Т. 2), и в системе g, когда g первообразный

корень числа m (Т. 5). Изгагаю необходимые и достаточные условия существования свойства D для чисел p^a (p — простое число > 2) (Т. 4). 2^a, (Т. 6), m^n (m — число нечётное), (Т. 7), $m = [m_1, m_2, \ldots m_k]$, (Т. 8), $2^a m$, (m — число нечётное) (Т. 3 и Сл. 2), $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ (Т. Дженкинса-данное здесь как следствие). Наконец, основываясь на свойствах функции $\lambda_g(m)$, делаю выводы из теоремы Дженкинса, касающиеся существования свойства D для числа $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, в зависимости от того, являются-ли числа p_i ($i = 1, 2, \ldots k$) числами типа $4k + 1$ или типа $4k - 1$, и в зависимости от того, есть-ли основание системы g или нет, первообразный корень чисел p_i. (Сл. 3 и 4, Т. 9).

Применяя функцию $\lambda_g(m)$ к исследованию китайского сравнения $2^n \equiv 2 \pmod{n}$ получаю как основной результат необходимые и достаточные условия для того, чтобы нечётное число $n = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, или чётное $n = 2 p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$, удовлетворяло этому сравнению (Т. 11). Это являются 1^0 неравенства $1 \leqslant a_i \leqslant \nu_i = \nu_2(p_i)$, $i = 1, 2, 3, \ldots k$, где $\nu_i = \nu_2(p_i)$ обозначает самое большое значение натурального числа t_i, удовлетворяющего сравнению $2^{\lambda_i} - 1 \equiv 0 \pmod{p_i^{t_i}}$, где $\lambda_i = \lambda_2(p_i)$, и 2^0 сравнение $n - 1 \equiv 0 \pmod{\lambda_2(n')}$ или сравнение $n - 1 \equiv 0 \left[\mathrm{mod.}\ \lambda_2\left(\frac{n'}{2}\right)\right]$ в зависимости от того, есть-ли n — нечётное или чётное число, причем $n' = p_1 p_2 \ldots p_k$, когда n — нечётное, а $n' = 2 p_1 p_2 \ldots p_k$ когда n — чётное. Кроме этого для n — чётного прибавляется условие $k \geqslant 2$.

Из этого результата, как прямое следствие, получается интересное, притом новое свойство чисел Ферма и Мерсена, удовлетворяющих, как известно, рассматриваемому китайскому сравнению, что они обязательно должны удовлетворять выше изложеным условиям. Возникает здесь обоснованное предположение, что числа эти имеют прямо вид $n = p_1 p_2 p_3 \ldots p_k$, $k \geqslant 1$.

Другой результат здесь теорема: если число $n = 2^m + 1$ удовлетворяет китайскому сравнению, то является оно числом Ферма (Т. 10), и следствие, что числа: нечётное n и чётное $2n$ не могут одновременно удовлетворять китайскому сравнению, что уменьшает вероятность существования чисел составных чётных, удовлетворяющих этому сравнению.

В конце ч. 3 — излагаю метод проверки, удовлетворяет-ли данное число n, или нет китайскому сравнению, метод этот основан на свойствах функции $\lambda_g(m)$.