SUR LES CONGRUENCES
$x^x \equiv c \pmod{m}$ et $a^x \equiv b \pmod{p}$

PAR

A. SCHINZEL et W. SIERPIŃSKI

THÉORÈME 1. *m étant un nombre naturel et c un entier premier avec m, la congruence*

$$x^x \equiv c \pmod{m} \tag{1}$$

a une infinité de solutions en nombres naturels x, telles que

$$(x, \varphi(m)) = 1 \tag{2}$$

($\varphi(m)$ désigne ici le nombre de nombres naturels $\leq m$ et premiers avec m, et (a, b) désigne le plus grand diviseur commun des nombres a et b).

LEMME. *r et s étant des entiers premiers entre eux et g un nombre naturel, il existe des nombres naturels k tels que $(rk + s, g) = 1$.*

DÉMONSTRATION DU LEMME. Le nombre

$$k = \frac{g}{(g, s^g)} \tag{3}$$

satisfait à notre lemme. En effet, soit p un diviseur premier du nombre g et soit p^h la plus haute puissance de p qui divise g. Si p ne divise pas s, p ne divise pas (g, s^g) et, d'après (3), divise k, donc aussi rk, et parsuite p ne divise pas $rk + s$ et on a $(rk + s, p) = 1$. Or, si p divise s, on a $h \leq p^h \leq g$ et p^h divise s^g, donc p^h divise (g, s^g), d'où (vu la définition du nombre h) on conclut, d'après (3), que p ne divise pas k, donc $(p, k) = 1$ et, comme p divise s et $(r, s) = 1$, on a $(p, r) = 1$, donc $(p, kr) = 1$ et, p divisant s, on trouve $(rk + s, p) = 1$. Nous

avons ainsi démontré que le nombre $rk + s$ est premier par rapport à tout diviseur premier du nombre g, d'où il résulte que $(rk + s, g) = 1$, c. q. f. d.

Notre lemme se trouve ainsi démontré.

DÉMONSTRATION DU THÉORÈME 1. Nous démontrerons le théorème 1 par l'induction par rapport à m. Pour $m = 1$ le théorème 1 est évidemment vrai. Soit maintenant m un entier > 1, $(c, m) = 1$, et supposons que le théorème 1 est vrai pour tous les modules naturels $< m$. En particulier, il est donc vrai pour le module $n = (m, \varphi(m))$ qui est $< m$, puisque pour $m > 1$ on a $\varphi(m) < m$. Le nombre n étant un diviseur de m, il résulte de $(c, m) = 1$ que $(c, n) = 1$ et, d'après notre hypothèse, il existe un nombre naturel a tel que

$$a^a \equiv c \pmod{n} \quad \text{et} \quad (a, \varphi(n)) = 1 \tag{4}$$

Vu que $(c, n) = 1$, la première des formules (4) prouve que $(a, n) = 1$, ce qui donne, vu la deuxième des formules (4) : $(a, n\varphi(n)) = 1$. Nous pouvons donc appliquer notre lemme pour $r = n\varphi(n)$, $s = a$, $g = \varphi(m)$. D'après ce lemme il existe donc un nombre naturel k tel que

$$(n\varphi(n)k + a, \varphi(m)) = 1 \tag{5}$$

Soit $b = n \cdot \varphi(n) k + a$: on aura évidemment, d'après (4) :

$$b^b \equiv a^a \equiv c \pmod{n} \tag{6}$$

et, d'après (5) : $(b, \varphi(m)) = 1$. Il en résulte qu'il existe un nombre naturel t tel que $bt \equiv 1 \pmod{\varphi(m)}$. Or, cela donne, d'après $(c, m) = 1$, $c^{bt} \equiv c \pmod{m}$ et, n étant un diviseur de m, aussi $c^{bt} \equiv c \pmod{n}$, donc, d'après (6) : $c^{bt} \equiv b^b \pmod{n}$. Il en résulte que $(c^t)^{bt} \equiv b^{bt} \pmod{n}$ et comme $bt \equiv 1 \pmod{\varphi(m)}$, et à plus forte raison $bt \equiv 1 \pmod{\varphi(n)}$ (puisque n divise m et parsuite $\varphi(n)$ divise $\varphi(m)$), on trouve $c^t \equiv b \pmod{n}$. Comme $n = (m, \varphi(m))$, on en déduit sans peine que le système de deux congruences

$$x \equiv c^t \pmod{m} \quad \text{et} \quad x \equiv b \pmod{\varphi(m)}$$

a une infinité de solutions en nombres naturels x.

Or, pour chaque telle solution on a

$$x^x \equiv (c^t)^b \equiv c^{tb} \equiv c \pmod{m}$$

et, d'après $(b, \varphi(m)) = 1$ on a $(x, \varphi(m)) = 1$.

Le théorème 1 se trouve donc démontré par l'induction. Il est à remarquer qu'il cessarait d'être vrai si l'on ommettrait la condition $(c, m) = 1$: par exemple, comme on le démontre sans peine, la congruence $x^x \equiv 2 \pmod 4$ ni la congruence $x^x \equiv 2 \pmod 6$ n'a pas de solutions en nombres naturels x.

Exemple. Pour $m = 15$ les nombres naturels $c < 15$ premiers avec 15 sont : 1, 2, 4, 7, 8, 11, 13 et 14. Pour tels c les plus petits nombres naturels x satisfaisant à la congruence (1) sont respectivement : 1, 17, 19, 37, 47, 11, 7 et 29.

Si $(x, m) = 1$ et si M désigne le plus petit multiple commun de nombres m et $\varphi(m)$, on a $(x + M)^{x+M} \equiv x^x \pmod m$. Il en résulte que dans le cas où $(c, m) = 1$, pour trouver toutes les solutions en nombres naturels x de la congruence (1), il suffit de trouver d'abord tous les nombres naturels $x < M$ pour lesquels le nombre x^x-c est divisible par m : si ce sont les nombres $x_1, x_2, \ldots, x_s$, toutes les solutions de la congruence (1) en nombres naturels x seront contenues dans les formules

$$x = x_i + kM, \quad \text{où} \quad i = 1, 2, \ldots, s \quad \text{et} \quad k = 0, 1, 2, \ldots$$

Du théorème 1 résulte tout de suite ce

Corollaire. *c étant un entier et p un nombre premier, la congruence*

$$x^x \equiv c \pmod p$$

a une infinité de solutions en nombres naturels x.

Voici une démonstration directe de cette proposition.

Soit p un nombre premier donné et c un entier donné. Comme $(p, p - 1) = 1$, il existe une infinité de nombres naturels x tels que $x \equiv c \pmod p$ et $x \equiv 1 \pmod{p-1}$, d'où, pour tout nombre k naturel, $x^k \equiv 1 \pmod{p-1}$. Si $c \equiv 0 \pmod p$, on a $x^{x^k} \equiv 0 \equiv c \pmod p$. Si $c \not\equiv 0 \pmod p$, on a $x \not\equiv 0 \pmod p$ et $x^{x^k} \equiv x^1 \equiv c \pmod p$. On a donc toujours $x^{x^k} \equiv c \pmod p$ pour $k = 1, 2, 3, \ldots$, donc on a non seulement $x^x \equiv c \pmod p$, ce qui démontre notre corollaire, mais aussi $x^{x^x} \equiv c \pmod p$, $x^{x^{x^x}} \equiv c \pmod p$, et ainsi de suite.

En modifiant la démonstration du théorème 1, on pourrait démontrer la proposition suivante :

m étant un nombre naturel et c un entier premier avec m, chacune des congruences

$$x^x \equiv c \pmod m, \quad x^{x^x} \equiv c \pmod m, \quad x^{x^{x^x}} \equiv c \pmod m, \ldots$$

a une infinité de solutions en nombres naturels x.

Exemple. Soit $p = 5$, $c = 3$. On a ici $M = 5.4 = 20$. Pour $x < 20$ les nombres $x^x - 3$ sont divisibles par 5 seulement pour $x = 7$ et $x = 13$. On en conclut que toutes les solutions en nombres naturels x de la congruence $x^x \equiv 3 \pmod 5$ sont contenues dans les formules $x = 7 + 20k$ et $x = 13 + 20k$, où $k = 0, 1, 2, \ldots$ Pareillement on trouve que toutes les solutions en nombres naturels x de la congruence $x^x \equiv 1 \pmod 5$ sont comprises dans la formule

$$x = t + 20k, \text{ où } t = 1, 4, 6, 8, 11, 12, 14 \text{ ou } 16 \text{ et } k = 0, 1, 2, \ldots$$

On trouve aussi que toutes les solutions en nombres naturels x de la congruence $x^{x^x} \equiv 3 \pmod 5$ sont les mêmes que de la congruence $x^x \equiv 3 \pmod 5$, et que toutes les solutions en nombres naturels x de la congruence $x^{x^x} \equiv 1 \pmod 5$ sont contenues dans la formule $x = t + 20k$, où $t = 1, 2, 4, 6, 8, 11, 12, 14, 16$ ou 18 et $k = 0, 1, 2, \ldots$

x étant un nombre naturel, désignons par x_n le n-ième terme de la suite infinie

$$x, \; x^x, \; x^{x^x}, \ldots$$

On peut démontrer que *pour tout module naturel m et tout entier c il existe un nombre naturel h tel que pour $n \geqslant h$ la congruence $x^{x_n} \equiv c \pmod m$ a les mêmes solutions que la congruence $x^{x_h} \equiv c \pmod m$.*

Cela est une conséquence immédiate de la proposition suivante : *Quels que soient les nombres naturels m et a, les restes de la division par m des nombres de la suite infinie $a, a^a, a^{a^a}, \ldots$ sont à partir d'une certaine place toutes égales.*

La proposition est évidemment vraie pour $a = 1$ et aussi pour les cas où tout diviseur premier de m est un diviseur de a, puisque dans ce cas tous les termes de notre suite sont, à partir d'une certaine place, divisibles par m.

La proposition est évidemment vraie pour le module $m = 1$. Soit maintenant m_0 un nombre naturel > 1 et supposons que la proposition est vraie pour tout module naturel $< m_0$. Nous pouvons écrire $m_0 = rs$, où tout diviseur premier de r est un diviseur de a et où $(a, s) = 1$. S'il était $s = 1$, tout diviseur premier de m_0 serait un diviseur de a et, comme nous avons remarqué plus haut, la proposition serait vraie pour m_0. Supposons donc que $s > 1$. Il existe évidemment un nombre naturel k tel que $r \mid a^k$ et il suffira de démontrer notre proposition pour le module $a^k s$ qui est un multiple de m_0. Comme $s > 1$, on a $\varphi(s) < s \leq m_0$ et, d'après l'hypothèse, notre proposition est vraie pour le module $m = \varphi(s)$. Vu notre notation,

il existe donc un nombre naturel $h \geqslant k$ tel que $a_n \equiv a_h \pmod m$ pour $n \geqslant h$ et, comme $m = \varphi(s)$, $(a, s) = 1$, d'après le théorème d'EULER on trouve $a^{a_n} - a^a \equiv 1 \pmod s$, ce qui prouve que $s \mid a^{a_n - a} - 1$. Or, on a

$$a_{n+1} - a_{h+1} = a^{a_n} - a^{a_h} = a^h (a^{a_n - a_h} - 1)$$

et, comme $h \geqslant k$, on a $a_h \geqslant k$, donc $a^k \mid a^{a_h}$. On a donc $m_0 = a^k s \mid a_{n+1} - a_{h+1}$ pour $n \geqslant h$, ce qui prouve que pour $n \geqslant h$ les nombres a_{n+1} et a_{h+1} donnent les mêmes restes mod. m_0. Notre proposition se trouve ainsi démontrée par l'induction.

Il est à remarquer que L. E. DICKSON dans son livre *History of the Theory of Numbers*, vol. I, p. 379 écrit que A. CUNNINGHAM dans les Proc. London Math. Soc. (2) 3 (1907), p. 257-274 a démontré que les restes de la suite infinie 2, 2^2, 2^{2^2}, ... forment pour tout module naturel m une suite périodique.

Passons maintenant à la congruence

$$a^x \equiv b \pmod p, \tag{7}$$

où a et b sont des entiers donnés et p un nombre premier donné. Les cas où $a = 0, 1, -1$ ou bien où $b = 0$ sont triviaux. Supposons donc que a et b sont des entiers donnés tels que $|a| > 1$ et $b \neq 0$. Si $b = a^h$, où $h = 0, 1, 2, \ldots$, la congruence (7) a pour tout nombre premier p qui ne divise pas a une infinité de solutions en nombres naturels x, par exemple les solutions $x = k(p-1) + h$, où $k = 0, 1, 2, \ldots$ Nous ne savons pas s'il y a d'autres cas, où la congruence $a^x \equiv b \pmod p$ a des solutions en nombres naturels x pour tous les nombres premiers p suffisamment grands.

Or, on a le théorème suivant :

THÉORÈME 2. *a et b étant des entiers donnés, tels que $|a| > 1$ et $b \neq 0$, il existe une infinité de nombres premiers p pour lesquels la congruence* (7) *a une infinité de solutions en nombres naturels x.* (1)

DÉMONSTRATION. Comme le cas $b = a^0 = 1$ a été traité plus haut, nous pouvons supposer que $b \neq 1$. Soit n un nombre naturel donné quelconque et soit, pour i naturel, p_i le i-ème nombre premier (donc $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_{10} = 29$). Soit $c = p_1 p_2 \ldots p_n$ et soit

$$|b| \cdot |b - 1| \cdot c = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s} \tag{8}$$

(1) Ce théorème est connu : sous une autre forme il se trouve comme Problème 107 dans le livre de G. PÓLYA et G. SZEGÖ, *Aufgaben und Lehrsätze aus der Analysis*, II. Cf. G. PÓLYA, Journ f. r. u. a. Math. 159 (1921) p. 19-21.

le développement du nombre $|b| \cdot |b-1| \cdot c$ en facteurs premiers. Soit

$$\theta = \varphi(q_1^{\alpha_1+1} q_2^{\alpha_2+1} \dots q_s^{\alpha_s+1}). \tag{9}$$

Comme $q_i^{\alpha_i} \geqslant \alpha_i + 1$ pour $i = 1, 2, \dots s$, nous aurons

$$\theta \geqslant \alpha_i + 1 \quad \text{pour} \quad i = 1, 2, \dots, s. \tag{10}$$

k étant un nombre pair suffisamment grand, nous aurons

$$a^{k\theta} - b > q_1^{\alpha_1} q_2^{\alpha_2} \dots q_s^{\alpha_s}. \tag{11}$$

Supposons que pour un nombre naturel $i \leqslant s$ le nombre $a^{k\theta} - b$ est divisible par $q_i^{\alpha_i+1}$. S'il était $q_i | a$, on aurait d'après (10), $q_i^{\alpha_i+1} | a^{k\theta}$, donc, d'après $q_i^{\alpha_i+1} | a^{k\theta} - b$, $q_i^{\alpha_i+1} | b$, ce qui contredit au développement (8). On a donc q_i non$|a$ et, d'après (9) et le théorème d'EULER : $q_i^{\alpha_i+1} | a^{k\theta} - 1$.

Or, comme $q_i^{\alpha_i+1} | a^{k\theta} - b$ et $a^{k\theta} - b = a^k - 1 - (b-1)$, on trouve $q_i^{\alpha_i+1} | b - 1$, ce qui est impossible, vu le développement (8).

Pour tout nombre naturel $i \leqslant s$ le nombre $a^{k\theta} - b$ est donc divisible au plus par la α_i-ème puissance du nombre premier q_i et il résulte de l'inégalité (11) que le nombre $a^{k\theta} - b$ a un diviseur premier p autre que $q_1, q_2, \dots q_s$, donc plus grand que p_n. Il existe donc des nombres premiers p aussi grands que l'on veut pour lesquels la congruence (7) a des solutions en nombres naturels x.

Il est à remarquer que si pour un nombre premier p la congruence (7) a une solution en nombres naturels x, elle a une infinité de telles solutions. En effet, si $p|a$, il résulte de (7) (x étant un nombre naturel) que $p|b$ et alors la congruence (7) a lieu quel que soit le nombre naturel x. Or, si p non a, il résulte de (7), d'après le théorème de FERMAT, $a^{k(p-1)+x} \equiv b \pmod{p}$ pour $k = 1, 2, \dots$, ce qui prouve que la congruence (7) a une infinité de solution en nombres naturels x.

Le théorème 2 se trouve ainsi démontré.

Il est à remarquer qu'en utilisant un résultat de M. G. PÓLYA qu'il a publié dans Mathematische Zeitschrift 1(1918), p. 143-148, en peut démontrer une proposition plus forte que le théorème 2, notamment la suivante :

a et b étant des entiers donnés, $a > 0$ et $b \neq 0$, il existe pour tout nombre naturel m un nombre naturel k_0 tel que pour tout nombre naturel $k > k_0$ le nombre $a^k - b$ a un diviseur premier $> m$.

En effet, M. G. PÓLYA a démontré l.c. que si A, B et C sont des entiers, $A \neq 0$, $B^2 - 4AC \neq 0$, le plus grand diviseur premier du

nombre $An^2 + Bn + C$ tend vers l'infinité avec n. Pour en obtenir notre proposition, il suffirait d'appliquer le théorème de G. PÓLYA aux polynomes $n^2 - b$ et $an^2 - b$ et de poser $n = a^k$.

a et b étant des entiers donnés et p un nombre premier donné, il est toujours possible de trouver tous les nombres naturels x qui satisfont à la congruence (7). En effet, si $p|a$ et $p|b$, tout nombre naturel x satisfait à la congruence (7), et si $p|a$ et p non $|\ b$, aucun nombre naturel x ne satisfait pas à la congruence (7). Si p non $|\ a$, on a $a^{p-1} \equiv 1 \pmod p$ et il suffit d'examiner pour lesquels de nombres naturels $x < p$ le nombre $a^x - b$ est divisible par p. S'il n'y a pas de tels nombres x, la congruence (7) n'a pas de solutions en nombres naturels x. Si $x_1, x_2, \ldots, x_s$ sont tous les nombres naturels $< p$ tels que $p|a^x - b$ pour $i = 1, 2, \ldots, s$, alors $x = x_i + k(p-1)$, où $i = 1, 2, \ldots, s$; $k = 0, 1, 2, \ldots$ — sont toutes les solutions de la congruence (7) en nombres naturels x.

Or, le problème de trouver, pour a et b donnés, tous les nombres premier p pour lesquels la congruence (7) a des solutions en nombres naturels x est difficile même pour les petites valeurs des entiers a et b.

En particulier, nous ne connaissons pas tous les nombres premiers p pour lesquels la congruence $2^x \equiv -1 \pmod p$ a des solutions en nombres naturels x. On sait démontrer que cette congruence a des solutions pour tous les nombres premiers p de la forme $8k \pm 3$ et n'a pas de solutions pour tous les nombres premiers de la forme $8k + 7$. On sait aussi qu'il existe une infinité de nombres premiers de la forme $8k + 1$ pour lesquels notre congruence a des solutions en nombres naturels x, et récenment M. A. AIGNER a démontré qu'il existe une infinité de nombres premiers p de la forme $8k + 1$ pour lesquels notre congruence n'a pas de solutions en nombres naturels x [1].

Quant à la congruence $3^x \equiv -1 \pmod p$, P. FERMAT affirmait que tous les nombres premiers p pour lesquels cette congruence a des solutions en nombres premiers x sont (sauf le nombre 2) les nombres premiers p de la forme $12n \pm 5$ [2]. Or, cette affirmation est fausse, puisque on a $61|3^5 + 1$, $73|3^6 + 1$, $241|3^{60} + 1$. On peut

---

[1] Voir W. SIERPIŃSKI, *Sur une décomposition des nombres premiers en deux classes*, Collectanea Mathematica, Vol. X (1958), p. 81-83, voir aussi Elemente der Mathematik 14 (1959), p. 60, probl. N.° 29.

[2] P. FERMAT, Oeuvres II, p. 220 (lettre au Mersenne du 15 juin, 1641), aussi L. E. DICKSON, *History of the theory of numbers*, vol. I, p. 257.

même démontrer qu'il existe une infinité de nombres premiers de la forme $p = 12k + 1$ pour lesquels la congruence $3^x \equiv -1 \pmod{p}$ a des solutions en nombres naturels x (1).

P. FERMAT affirmait aussi (l. c.) que la congruence $5^x \equiv -1 \pmod{p}$ n'a pas de solutions pour aucun nombre premier p de la forme $10k \pm 1$. A. SCHINZEL a démontré qu'il existe une infinité de nombres premiers p de la forme $10k + 1$ pour lesquels la congruence $5^x \equiv -1 \pmod{p}$ a des solutions en nombres naturels x : tel est par exemple, le nombre $x = 5$ pour $p = 521$. On peut aussi démontrer qu'il existe une infinité de nombres premiers de la forme $10k - 1$ pour lesquels la congruence $5^x \equiv -1 \pmod{p}$ a des solutions, par exemple $x = 7$ pour $p = 29$ (2).

Or, le problème se pose si, $a > 1$ et b étant des entiers premiers entre eux et b n'étant pas une puissance à l'exposant entier $\geqslant 0$ du nombre a, il existe une infinité de nombres premiers p pour lesquels la congruence (7) n'a pas de solutions (en nombres naturels x).

Nous démontrerons ici le

THÉORÈME 3. *a étant un nombre naturel et b un entier qui n'est pas la 12-éme puissance d'un entier, $(a, b) = 1$, il existe une infinité de nombres premiers p pour lesquels la congruence (7) n'a pas de solutions en entiers $x = 0, 1, 2, \ldots$*

LEMME 1. *a étant un nombre naturel et b un entier qui n'est pas un carré et $(a, b) = 1$, il existe une infinité de nombres premiers p pour lesquels a est un résidu et b est un non-résidu quadratique.* (3)

DÉMONSTRATION DU LEMME 1. Soit m^2 le plus grand carré qui divise a et n^2 le plus grand carré qui divise b et soit $a = a_1 m^2$, $b = b_1 n^2$: il suffira de démontrer qu'il existe une infinité de nombres naturels p pour lesquels a_1 est un résidu quadratique et b_1 ne l'est pas.

Soit d'abord $b_1 = -1$: il suffira de démontrer que a_1 est un résidu quadratique pour une infinité de nombres premiers p de la forme $4k + 3$ (puisque pour des tels nombres -1 est un non-résidu quadratique). Cela est évident si $a_1 = 1$; nous pouvons donc supposer que $a_1 > 1$, donc $a_1 = q_1 q_2 \ldots q_s$, où $q_1, q_2, \ldots, q_s$ sont des nombres premiers, $q_1 < q_2 < \ldots < q_s$.

---

(1) Voir la Note de A. SCHINZEL, *Sur quelques propositions fausses de P. Fermat*, Comptes rendus Acad. Paris, séance du 28 octobre, 1959, p. 1604.

(2) Voir la Note de A. SCHINZEL *Sur quelques propositions fausses de P. Fermat*, Comptes rendus Acad. Paris, séance du 28 octobre, 1959, p. 1605.

(3) Un théorème plus général est connu : voir E. HECKE, *Vorlesungen über algebraische Zahlen*, Satz 147, New York 1948, p. 199.

Il existe, comme on sait, un nombre naturel h tel que

$$h \equiv -1 \pmod 8, \quad h \equiv -1 \pmod{q_i} \quad \text{pour} \quad i = 1, 2, \ldots, s$$

(puisque, si $q_1 = 2$, la congruence $h \equiv -1 \pmod{q_1}$ est une conséquence de la congruence $h \equiv -1 \pmod 8$).

D'après le théorème de LEJEUNE-DIRICHLET, il existe une infinité de nombres premiers de la forme $p = 8q_1 q_2 \ldots q_2 t + h$.

Nous aurons ici $p \equiv h \equiv -1 \pmod 8$, donc p sera de la forme $4k + 3$ et si $q_1 = 2$, nous aurons $\left(\frac{q_1}{p}\right) = \left(\frac{2}{p}\right) = 1$.

Soit maintenant i un des nombres $1, 2, \ldots, s$. Si q_i est impair, de la forme $4k + 1$, on a

$$\left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right) = \left(\frac{8q_1 q_2 \ldots q_s^{t+h}}{q_i}\right) = \left(\frac{h}{q_i}\right) = \left(\frac{-1}{q_i}\right) = 1.$$

Soit maintenant $b_1 = \pm 2$. D'après $(a_1, b_1) = 1$ nous aurons $a_1 = q_1 q_2 \ldots q_r$ où $q_i\,(i = 1, 2, \ldots, r)$ sont des nombres premiers > 2. Il existe un nombre naturel h tel que $h \equiv 5 \pmod 8$ et $h \equiv 1 \pmod{q_i}$ pour $i = 1, 2, \ldots, r$. D'après le théorème de DIRICHLET il existe une infinité de nombres premiers de la forme $8q_1 q_2 \ldots q_r k + h$. Soit p un de tels nombres : en aura donc $p \equiv 5 \pmod 8$ et $p \equiv 1 \pmod{q_i}$ pour $i = 1, 2, \ldots, r$. Il en résulte que

$$\left(\frac{\pm 2}{p}\right) = -1, \qquad \left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right) = \left(\frac{1}{q_i}\right) = 1.$$

donc $\left(\frac{a_1}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)\ldots\left(\frac{q_r}{p}\right) = 1$ et a_1 est un résidu quadratique pour p et b_1 ne l'est pas.

Soit enfin b_1 un entier autre que -1 et ± 2 ; b_1 n'étant pas un carré (puisque b ne l'est pas), donc $b_1 \neq 1$, il existe au moins un diviseur impair q_1 de b_1 et on a $b_1 = \pm 2^\alpha q_1 q_2 \ldots q_{,,}$ $a_1 = 2^\beta q_{r+1} \ldots q_s$, où α et β sont des entiers non négatifs, $s \geqslant r \geqslant 1$ et $q_1, q_2, \ldots q_s$ sont des nombres premiers impairs. Il existe, comme on sait un nombre naturel n_1 qui est un non- résidu quadratique pour q_1. Il existe un nombre naturel h tel que

$$h \equiv 1 \pmod 8, \quad h \equiv n_1 \pmod{q_1} \quad \text{et} \quad h \equiv 1 \pmod{q_i} \quad \text{pour} \quad i = 2, 3, \ldots s.$$

D'après le théorème de DIRICHLET il existe une infinité de nombres premiers de la forme $8q_1q_2 \dots q_s k + h$; soit p un de ces nombres. On aura donc

$$p \equiv 1 \pmod 8, \quad p \equiv n_1 \pmod{q_1}, \quad p \equiv 1 \pmod{q_i} \quad \text{pour} \quad i = 2, 3, \dots s.$$

On en trouve

$$\left(\frac{-1}{p}\right) = 1, \quad \left(\frac{2}{p}\right) = 1, \quad \left(\frac{q_i}{p}\right) = \left(\frac{1}{q_i}\right) = 1 \quad \text{pour} \quad i = 2, 3, \dots, s,$$

$$\left(\frac{q_1}{p}\right) = \left(\frac{p}{q_1}\right) = \left(\frac{n}{q_1}\right) = -1.$$

On a donc

$$\left(\frac{a_1}{p}\right) = \left(\frac{2}{p}\right)^{\alpha} \left(\frac{q_{r+1}}{p}\right) \dots \left(\frac{q_s}{p}\right) = 1,$$

$$\left(\frac{b_1}{p}\right) = \left(\frac{\pm 1}{p}\right) \left(\frac{2}{p}\right)^{\beta} \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_r}{p}\right) = -1$$

et a_1 est un résidu quadratique pour p et b_1 ne l'est pas, c. q. f. d.

Le lemme 1 se trouve ainsi démontré.

LEMME 2. *Si a et b sont des entiers $(a, b) = 1$, et si b n'est pas un cube d'un entier, il existe une infinité de nombres premiers p pour lesquels a est un résidu cubique et b ne l'est pas.*

DÉMONSTRATION DU LEMME 2. D'après l'hypothèse un au moins nombre premier figure dans le développement du nombre b en facteures premiers avec un exposant qui n'est pas divisible par 3 : soit r un tel nombre premier et soient.

$$a = \pm q_1^{h_1} q_2^{h_2} \dots q_k^{h_k}, \qquad b = \pm q_{k+1}^{h_{k+1}} q_{k+2}^{h_{k+2}} \dots q_l^{h_l} r^g$$

les développements de a et b en facteurs premiers.

Il suffira évidemment de prouver que pour une infinité de nombres premiers p les nombres q_i $(i = 1, 2, \dots, l)$ sont des résidus cubiques et le nombre r n'est pas un résidu cubique.

Considérons les nombres premiers p de la forme $u^2 - uv + v^2$ (Tels sont, comme on sait, tous les nombres premiers de la forme $3t + 1$). Il résulte de la loi de reciprocité pour les résidus cubiques (voir T. J. STIELTJES, *Contribution à la théorie des résidus cubiques et biquadratiques*. Oeuvres complètes, t. I, p. 210-275) que

1.° si $v \equiv 0 \pmod{3q_i}$, q_i est résidu cubique pour p,

2.° il existe un entier c tel que

$$1 - 3c + 9c^2 \not\equiv 0 \pmod r \tag{12}$$

et, si $v \equiv 3cu \pmod{3r}$, r n'est pas un residu cubique pour p.

Le système des congruences

$$z \equiv 0 \pmod{q_i} \quad \text{et} \quad z \equiv c \pmod r \qquad (1 \leqslant i \leqslant l) \tag{13}$$

a des solutions d'après le théorème chinois sur les restes. d désignant une de ces solutions, si l'on pose

$$v = 3du + 6wq_1q_2 \dots q_1r, \quad \text{on aura}$$
$$v \equiv 0 \pmod{3q_i} \text{ et } v \equiv 3cu \pmod{3r},$$

donc tout nombre premier

$$p = u^2 - u(3du + 6wq_1q_2 \dots q_1r) + (3du + 6uq_1q_2 \dots q_1r)^2 = f(u, w)$$

jouit des propriétés désirées. En transformant nous obtenons

$$f(u, w) = u^2(1 - 3d + 9d^2) + 2uw(-3q_1q_2 \dots q_1r + 18dq_1 \dots q_1r) + \\ + w^2(36q_1^2q_2^2 \dots q_1^2r^2).$$

D'après (12) et (13) on a

$$(1 - 3d + 9d^2, \quad 36q_1^2q_2^2 \dots q_1^2r^2) = 1,$$

donc la forme $f(u, w)$ est proprement primitive et en vertu du théorème de DIRICHLET, démontré par H. WEBER (*Beweis des Satzes das jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Annalen Bd. 20, p. 301) elle représente une infinité de nombres premiers. Le lemme 2 se trouve ainsi démontré.

Pareillement, en se basant sur la loi de reciprocité des résidus biquadratiques on peut démontrer le

LEMME 3. *Si a est un nombre naturel et b un entier qui n'est pas un bicarré d'un entier, et si $(a, b) = 1$, il existe une infinité de nombres premiers p pour lesquels a est un résidu biquadratique et b ne l'est pas.*

Le théorème 3 est une conséquence immédiate des lemmes 1, 2 et 3.

A. Schinzel a démontré à l'aide du théorème de Hilbert-Čebotarew (1) le théorème suivant :

Si a et b sont des entiers tels que $b \neq a^k$ pour k entiers, il existe une infinité des nombres premiers p pour lesquels la congruence $a^z \equiv b \pmod{p}$ n'a pas de solution.

---

(1) D. HILBERT, *Die Theorie der Algebraischen Zahlkörper*, Ges. Abh: I p. 276, théorème 152 et N. ČEBOTAREW, *Osnowy teorii Galua*, Leningrad—Moskwa 1937, p. 150, théorème 46.