Il en résulte que l'équation (1) n'a pas de solution en nombres naturels x,y,z,t superieurs à 1 et autres que $3,2,2,3$, où y est une puissance du nombre 2 à l'exposant naturel. En effet si $x,2^s,z,t$ serait une telle solution, $x,2,z,ts$ serait évidemment une solution de l'équation (1) en nombres naturels >1 et s'il était $x=3$, $y=2$, $z=2$, $ts=3$, on aurait ou bien $s=1$, ce qui donne la solution $3,2,2,3$, ou bien $t=1$, ce qui est impossible.

Supposons maintenant que x,y,z,t est une solution de l'équation (1) en nombres naturels >1 autre que $3,2,2,3$ et qu'on a la formule (3). On a donc

$$y^t+1=(y+1)^z, \tag{4}$$

d'où, d'après $z>1$, on trouve $t>z$, donc $t-1\geqslant z$. Le nombre y ne pouvant pas, comme nous le savons, être une puissance du nombre 2, et vu $y>1$, il existe un diviseur premier p de y. Soit s l'exposant de la plus grande puissance de p qui divise y, et soit g une racine primitive pour le module p^{st}. Comme, d'après $p|y$, on a $(y+1,p^{st})=1$, il existe un nombre naturel i tel que $g^i\equiv y+1 \pmod{p^{st}}$, d'où, d'après $p^s|y$, on a $g^i\equiv 1 \pmod{p^s}$. S'il était $g^i\equiv 1 \pmod{p^{s+1}}$, alors d'après $t>1$, d'où $g^i\equiv y+1 \pmod{p^{s+1}}$, on aurait $y\equiv 0 \pmod{p^{s+1}}$, donc $p^{s+1}|y$, contrairement à la définition du nombre s. On a donc $g^i\equiv 1 \pmod{p^s}$ et $g^i\not\equiv 1 \pmod{p^{s+1}}$. Or, g étant une racine primitive pour le module p^{st}, g est de même une racine primitive pour le module p^s, donc d'après $g^i\equiv 1 \pmod{p^s}$, on a $\varphi(p^s)|i$, et comme $g^i\not\equiv 1 \pmod{p^{s+1}}$, on n'a pas $\varphi(p^{s+1})|i$. On a donc $p^{s-1}(p-1)|i$ et on n'a pas $p^s(p-1)|i$, d'où il résulte qu'on n'a pas $p^s|i$.

D'autre part, d'après $g^i\equiv y+1 \pmod{p^{st}}$, (4) et $p^s|y$, on a $g^{iz}\equiv(y+1)^z \equiv 1 \pmod{p^{st}}$, d'où $p^{st-1}(p-1)|iz$, donc $iz=up^{st-1}$, où u est un nombre naturel. Or comme $p^{s-1}|i$ et comme on n'a pas $p^s|i$, on a $i=vp^{s-1}$, où $(v,p)=1$. On a donc $vz=p^{s(t-1)}u$ et, d'après $(v,p)=1$, on trouve $p^{s(t-1)}|z$. Or, nous avons trouvé précédemment $t-1\geqslant z$: on a donc $p^{(t-1)s}\geqslant p^{zs} \geqslant zs+1\geqslant z+1$, ce qui est incompatible avec $p^{(t-1)s}|z$.

Le théorème se trouve ainsi démontré.

Sur l'équation $x^z-y^t=a^t$, où $|x-y|=a$

par A. Rotkiewicz (Warszawa)

Le but de cette note est de démontrer le théorème suivant

Théorème. *L'équation*

$$x^z-y^t=a^t \tag{1}$$

où a est un nombre naturel, n'a pas en nombres naturels x,y,z,t plus grands que 1, d'autres solutions que $x=3$, $y=2$, $z=2$, $t=3$, si

$$|x-y|=a, \quad \text{et} \quad (x,y)=1. \tag{2}$$

Pour $a=1$ nous en obtenons le théorème de R. Hampel.

Démonstration. M. M. Birkhoff et Vandiver ont démontré le théorème T suivant (cf. [1] et [2], p. 388):

T. *Si a,b et n sont des nombres naturels, $a>b$, $(a,b)=1$, et $n>2$, le nombre a^n-b^n a au moins un diviseur premier p tel que $p|a^n-b^n$ et qu'on n'a pas $p|a^k-b^k$ pour $k=1,2,\dots,n-1$, sauf le cas où $a=2$, $b=1$, $n=6$*[1]).

Supposons maintenant que x,y,z,t sont des nombres naturels >1, differents de $3,2,2,3$ respectivement, a — un nombre naturel, et qu'on a les formules (1) et (2). D'après (2) on a $x-y=\pm a$, donc

$$x=y\pm a \tag{3}$$

et d'après (1) et (3) on trouve

$$y^t+a^t=(y\pm a)^z. \tag{4}$$

D'après (3) et $(x,y)=1$ on a $(y,a)=1$ et d'après le théorème T le nombre $y^{2t}-a^{2t}$ pour $t>1$ a un diviseur premier p tel que $p|y^{2t}-a^{2t}$ et qu'on n'a pas $p|y^k-a^k$ pour $k=1,2,\dots,2t-1$, sauf le cas où $y=2$, $a=1$, $t=3$ si $y>a$ et le cas $a=2$, $y=1$, $t=3$ si $y<a$. On n'a donc pas $p|y^t-a^t$ et, comme $(y^t-a^t)(y^t+a^t)=y^{2t}-a^{2t}$, on trouve $p|y^t+a^t$.

D'après (4) on a donc $p|y\pm a$ d'où $p|y^2-a^2$, contrairement à

$$p \text{ non}|y^k-a^k \quad \text{pour} \quad k=1,2,\dots,2t-1, \quad \text{si} \quad t>1.$$

---

[1]) Je donnerai ailleurs une démonstration élémentaire du théorème T.

Comme $y>1$, il ne nous reste qu'à examiner le cas $y=2$, $a=1$, $t=3$. Dans ce cas (1) donne $x^z-2^3=1$, d'où $x^z=9$ et vu que $z>1$, on trouve $x=3$, $z=2$.

Notre théorème se trouve ainsi démontré.

Travaux cités

[1] G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of* a^n-b^n, Annals of Math. (2) 5, p. 173-180.

[2] L. E. Dickson, *History of the Theory of Numbers*, New York 1952.

Sur les congruences aux racines données *

par M. M. Chojnacka-Pniewska (Warszawa)

Il est connu que pour chaque suite finie de nombres réels ou complexes $x_1,x_2,\ldots,x_k$ il existe un polynôme $f(x)$, dont les racines sont seulement les nombres $x_1,x_2,\ldots,x_k$. On pose la question: *lorsque m est un module donné, et $x_1,x_2,\ldots,x_k$ un système fini arbitraire de restes différents modulo m, c'est-à-dire de nombres de la suite $0,1,2,\ldots,m-1$, existe-t-il toujours un polynôme $f(x)$ aux coefficients entiers, pour lequel les racines de la congruence $f(x)\equiv 0 \pmod m$ seraient seulement les nombres $x_1,x_2,\ldots,x_k$ et les nombres congrus avec ces nombres modulo m?*

On examine différents cas de module m: m premier et m composé.

I. Si m est un nombre premier, alors la réponse à la question ci-dessus est positive et le polynôme cherché sera

$$f(x) = (x-x_1)(x-x_2)\ldots(x-x_k).$$

En effet, les racines de la congruence

$$f(x) = (x-x_1)(x-x_2)\ldots(x-x_k) \equiv 0 \pmod m$$

sont seulement les nombres congrus modulo m avec un quelconque des nombres entiers $x_1,x_2,\ldots,x_k$. Pour obtenir, notamment,

$$(x-x_1)(x-x_2)\ldots(x-x_k)\equiv 0 \pmod m,$$

il faut que $x\equiv x_i \pmod m$ pour un i de la suite $0,1,\ldots,k$.

II. Si m est un nombre composé, le problème n'est pas si simple.

1. *Soit $m=4$. Les restes de ce module forment la suite $0,1,2,3$. On vérifie que pour chaque suite $x_1,x_2,\ldots,x_k$, où $k\leqslant 4$ et $x_1,x_2,\ldots,x_k$ sont des nombres différents de la suite $0,1,2,3$ il existe un polynôme $f(x)$ du degré $\leqslant 3$ aux coefficients entiers, pour lequel les racines de la congruence $f(x)\equiv 0 \pmod 4$ sont les nombres $x_1,x_2,\ldots,x_k$, et uniquement ces nombres, ainsi que leurs nombres congrus modulo 4.*

---

* Communication presentée le 20 juin 1952 à la Societé Polonaise de Mathématiques, Section de Varsovie.