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.

Démonstration. Soit $x_1, x_2, \ldots, x_k$ une suite finie arbitraire des restes modulo 4. Alors

(a) lorsque $k=1$, le polynôme cherché est (ce qu'on peut aisément prouver) $f(x)=x-x_1$;

(b) lorsque $k=2$, pour $x_1=0$, $x_2=1$, ou $x_1=0$, $x_2=3$, ou $x_1=1$, $x_2=2$, ou enfin $x_1=2$, $x_2=3$, le polynôme exigé sera $f(x)=(x-x_1)(x-x_2)$.

Si, par contre, $x_1=0$, $x_2=2$, on peut admettre $f(x)=2x$, ainsi que, lorsque $x_1=1$, $x_2=3$, on peut admettre $f(x)=2(x-1)$;

(c) lorsque $k=3$, on obtient $f(x)=(x-x_1)(x-x_2)(x-x_3)$, notamment lorsque $x_1=0$, $x_2=1$, $x_3=3$, on peut admettre $f(x)=x(x^2-1)$; et pour $x_1=1$, $x_2=2$, $x_3=3$, on peut admettre $f(x)=(x^2-1)(x-2)$;

(d) lorsque $k=4$, le polynôme cherché est $f(x)=x(x-1)(x-2)(x-3)$.

Ainsi la réponse au problème posé, dans le cas du module composé $m=4$ est positive, comme dans le cas du module premier.

2. Soit $m=6$. On constate ici que toute congruence $f(x)\equiv 0 \pmod 6$, où $f(x)$ est un polynôme aux coefficients entiers, est équivalente à la congruence $g(x)\equiv 0 \pmod 6$, où $g(x)$ est un polynôme aux coefficients entiers du deuxième degré tout au plus. Cela s'ensuit du fait que $x^3 \equiv x \pmod 6$ pour chaque nombre entier x. En effet, $x^3\equiv x \pmod 6$ signifie que $(x-1)x(x+1)\equiv 0 \pmod 6$. Or, si x est nombre entier, $(x-1), x, (x+1)$ sont trois nombres entiers successifs. Parmi ces nombres au moins un est toujours pair, c'est-à-dire divisible par 2, et un parmi ces nombres est divisible par 3, leur produit sera donc divisible par 6. Il suffit alors pour un module 6 d'examiner des polynômes aux coefficients entiers du deuxième degré tout au plus. On y peut prouver que lorsque $f(x)$ est justement un tel polynôme et si $f(1)\equiv 0 \pmod 6$ ainsi que $f(2)\equiv 0 \pmod 6$, alors on a aussi $f(4)\equiv 0 \pmod 6$ et $f(5)\equiv 0 \pmod 6$. Il s'ensuit qu'*il n'existe pas de polynôme aux coefficients entiers pour lequel la congruence* $f(x)\equiv 0 \pmod 6$ *aurait seulement des racines* 1 *et* 2.

Démonstration. Supposons que $f(x)=ax^2+bx+c$. Si $f(1)\equiv 0 \pmod 6$ et $f(2)\equiv 0 \pmod 6$, on a $a+b+c\equiv 0 \pmod 6$ ainsi que $4a+2b+c\equiv 0 \pmod 6$. Donc, après soustraction des deux dernières congruences, il résulte $3a+b\equiv 0 \pmod 6$, donc $6a+2b\equiv 0 \pmod 6$, et $2b \equiv 0 \pmod 6$, et $-2b\equiv 0 \pmod 6$.

Vu que $a+b+c\equiv 0 \pmod 6$ et $-2b\equiv 0 \pmod 6$, il résulte, après addition, $a-b+c\equiv 0 \pmod 6$, dont il s'ensuit que $f(-1)\equiv 0 \pmod 6$. Puisque $5\equiv -1 \pmod 6$, on trouve $f(5)\equiv 0 \pmod 6$. Puisque $-2b \equiv 0 \pmod 6$, on a $-4b\equiv 0 \pmod 6$, et vu que $4a+2b+c\equiv 0 \pmod 6$, il résulte que $4a-2b+c\equiv 0 \pmod 6$, ce qui signifie que $f(-2)\equiv 0 \pmod 6$. Mais $4\equiv -2 \pmod 6$, donc aussi $f(4)\equiv 0 \pmod 6$. Il s'ensuit que les nombres 5 et 4 sont des racines de congruence $f(x)\equiv 0 \pmod 6$, c. q. f. d.

D'une manière analogue on peut démontrer que *lorsque* $f(x)=ax^2+bx+c$ *et* $6|f(0)$ *ainsi que* $6|f(1)$, *alors aussi* $6|f(3)$ *et* $6|f(4)$.

Démonstration. Il s'ensuit de $6|f(0)$ et $6|f(1)$ que $c\equiv 0 \pmod 6$ ainsi que $a+b\equiv 0 \pmod 6$, donc $3(a+b)\equiv 0 \pmod 6$ et $4(a+b)\equiv 0 \pmod 6$. Mais, vu que $6|c$, on a $f(3)=9a+3b+c\equiv 3(a+b) \pmod 6$, c'est-à-dire $f(3)\equiv 0 \pmod 6$ ainsi que $f(4)=16a+4b+c\equiv 4(a+b) \pmod 6$, c'est-à-dire $f(4)\equiv 0 \pmod 6$, c. q. f. d.

On a prouvé donc, qu'il n'existe pas un tel polynôme $f(x)$ aux coefficients entiers, pour lequel la congruence $f(x)\equiv 0 \pmod 6$ aurait seulement des racines 0 et 1.

On peut enfin démontrer que *la congruence du deuxième degré, aux racines* 2 *et* 3 *a aussi les racines* 0 *et* 5.

Démonstration. Soit $f(x)=ax^2+bx+c$. Vu que $6|f(2)$ et $6|f(3)$, on obtient $4a+2b+c\equiv 0 \pmod 6$ et $9a+3b+c\equiv 0 \pmod 6$, ça veut dire $3a+3b+c\equiv 0 \pmod 6$, d'où $-a+b\equiv 0 \pmod 6$. Vu que $6|4a+2b+c$, on a $6|8a+4b+2c$, donc $2a+4b+2c\equiv 0 \pmod 6$ et $3a+3b+c\equiv 0 \pmod 6$. Donc, après avoir soustrait $-a+b+c\equiv 0 \pmod 6$, et ayant pris en considération que $-a+b\equiv 0 \pmod 6$, on obtient $c\equiv 0 \pmod 6$, ce qui prouve que $f(0)\equiv 0 \pmod 6$.

Puisque $-a+b\equiv 0 \pmod 6$, on a $a-b\equiv 0 \pmod 6$, d'où, vu que $c\equiv 0 \pmod 6$, on trouve $a-b+c\equiv 0 \pmod 6$. Or celà signifie que $f(-1)\equiv 0 \pmod 6$, c'est-à-dire $f(5)\equiv 0 \pmod 6$, c. q. f. d.

3. Soit $m=8$. C'est un cas où on peut se servir de l'identité $x^5 \equiv x^3 \pmod 8$. En effet, on a $x^5-x^3=x^3(x^2-1)$, et x étant pair, le premier de ces facteurs est divisible par 8, tandis que pour x impair — le second est divisible par 8. Grâce à cette identité, le module étant 8, il suffit d'examiner les polynômes de quatrième degré tout au plus. Mais si $f(x)=ax^4+bx^3+cx^2+dx+e$ et $f(4)\equiv f(6)\equiv 0 \pmod 8$, on peut démontrer qu'en ce cas-là $f(0)\equiv 0 \pmod 8$ et $f(2)\equiv 0 \pmod 8$.

Démonstration. Si $f(4)\equiv f(6)\equiv 0 \pmod 8$, alors $4d+e\equiv 0 \pmod 8$ et $4c+6d+e\equiv 0 \pmod 8$, donc $4c+2d\equiv 0 \pmod 8$, et évidemment $8c+4d\equiv 0 \pmod 8$, d'où il s'ensuit que $4d\equiv 0 \pmod 8$ et $e\equiv 0 \pmod 8$. Celà prouve que $f(0)\equiv 0 \pmod 8$ et, lorsque $4c+6d+e\equiv 0 \pmod 8$ et $4d \equiv 0 \pmod 8$, on obtient $4c+2d+e\equiv 0 \pmod 8$. Puisque $f(2)\equiv 4c+2d+e \pmod 8$ on a $f(2)\equiv 0 \pmod 8$.

4. Examinons maintenant le cas $m=9$. On peut vérifier, que dans le cas de chaque x entier on obtient $x^3\equiv x^2 \pmod 9$. La réduction du degré du polynôme $f(x)$ est évidemment peu importante vu qu'on devrait examiner des polynômes de septième degré. En quelques cas c'est même superflu.

Or, on prouve aisément que *lorsque* $f(x)$ *est un polynôme aux coefficients entiers, d'un degré* n *arbitraire,*

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n ,$$

et si $f(0) \equiv 0 \pmod 9$ *et* $f(3) \equiv 0 \pmod 9$, *alors* $f(6) \equiv 0 \pmod 9$.

Démonstration. Si $f(0) \equiv 0 \pmod 9$ et $f(3) \equiv 0 \pmod 9$, alors $a_n \equiv 0 \pmod 9$ et $3a_{n-1} \equiv 0 \pmod 9$; il s'ensuit que $6a_{n-1} \equiv 0 \pmod 9$, donc $6a_{n-1} + a_n \equiv 0 \pmod 9$, et puisque $f(6) \equiv 6a_{n-1} + a_n \pmod 9$, alors $f(6) \equiv 0 \pmod 9$, c. q. f. d.

5. Nous examinerons enfin le cas $m = 10$. On prouve aisément que $x^5 \equiv x \pmod{10}$ quel que soit le nombre entier x. Il suffit donc d'examiner les polynômes de quatrième degré, comme c'etait le cas pour le module 8. Nous allons démontrer que *si* $f(x) = ax^4 + bx^3 + cx^2 + dx + e$ *et* $f(2) \equiv 0 \pmod{10}$ *et* $f(5) \equiv 0 \pmod{10}$, *alors* $f(0) \equiv 0 \pmod{10}$ *et* $f(7) \equiv 0 \pmod{10}$.

Démonstration. Si $f(2) \equiv f(5) \equiv 0 \pmod{10}$, alors

$$16a + 8b + 4c + 2d + e \equiv 0 \pmod{10}$$

et

$$625a + 125b + 25c + 5d + e \equiv 0 \pmod{10},$$

donc

$$6a + 8b + 4c + 2d + e \equiv 0 \pmod{10} \quad \text{et} \quad 5a + 5b + 5c + 5d + e \equiv 0 \pmod{10}.$$

En multipliant la première de ces congruences par 5 et la seconde par 4, on obtient $5e \equiv 0 \pmod{10}$ et $4e \equiv 0 \pmod{10}$, donc $e \equiv 0 \pmod{10}$, c'est-à-dire $f(0) \equiv 0 \pmod{10}$. Après l'addition de deux congruences on obtient $a + 3b + 9c + 7d + 2e \equiv 0 \pmod{10}$ ou, puisque $e \equiv 0 \pmod{10}$, on obtient $a + 3b + 9c + 7d + e \equiv 0 \pmod{10}$. Puisque toutefois $f(7) \equiv a + 3b + 9c + 7d + e \pmod{10}$, on a $f(7) \equiv 0 \pmod{10}$, c. q. f. d.

Remarque. Selon le théorème de Rédei, pour chaque nombre naturel $m > 1$ et pour chaque nombre entier x on a $x^m \equiv x^{m-\varphi(m)} \pmod m$, où φ est la fonction de Gauss. Il en résulte que dans les congruences modulo m, tout polynôme $f(x)$ peut être substitué par un polynôme $g(x)$ de degré $< m$, tel que $f(x) \equiv g(x) \pmod m$, pour chaque x.

Le théorème de Rédei ne donne pas toujours la réduction optimale du degré du polynôme, ce qu'on voit p. ex. lorsque $m = 6$. Selon le théorème de Rédei, on obtient $x^6 \equiv x^4 \pmod 6$ pour x entiers, tandis que nous avons $x^3 \equiv x \pmod 6$.

Sur une solution de l'équation du mouvement permanent du fluide visqueux

par J. Wolska (Warszawa)

1. Introduction. Dans l'hydrodynamique d'un fluide parfait on déduit une équation dite l'équation de Helmholtz

$$d\boldsymbol{W}/dt = (\boldsymbol{W}\nabla)\boldsymbol{v} \tag{1}$$

où $\boldsymbol{W} = \operatorname{rot}\boldsymbol{v}$, et $\boldsymbol{v}$ exprime la vitesse du fluide. L'équation (1) illustre les deux théorèmes de Helmholtz. L'équation du mouvement du fluide visqueux a la forme

$$d\boldsymbol{W}/dt = (\boldsymbol{W}\nabla)\boldsymbol{v} + \nu\Delta\boldsymbol{W} \tag{2}$$

où ν est le coefficient de viscosité cinématique. L'équation (2) est appelée l'équation de Helmholtz généralisée.

L'équation (2) devient plus simple, quand il s'agit du mouvement plan, puisque alors $v_z = 0$, et v_x, v_y ne dépendent pas de la coordonné z. Dans ce cas l'équation de continuité a la forme $\partial v_x/\partial x + \partial v_y/\partial y = 0$ ce qui permet d'introduire la fonction, dite fonction du courant, définie par les égalités $v_x = \partial\Psi/\partial y$, $v_y = -\partial\Psi/\partial x$. La composante W_z du vecteur $\boldsymbol{W}$ n'est pas nulle et s'exprime comme il suit

$$W_z = \partial v_y/\partial x - \partial v_x/\partial y = -\Delta\Psi$$

donc dans ce cas l'équation (2) devient

$$\frac{\partial\Delta\Psi}{\partial t} + \frac{\partial\Psi}{\partial y}\cdot\frac{\partial\Delta\Psi}{\partial x} - \frac{\partial\Psi}{\partial x}\cdot\frac{\partial\Delta\Psi}{\partial y} = \nu\Delta\Delta\Psi. \tag{3}$$

D'autre part, si le mouvement du fluide est permanent, la fonction Ψ ne dépend que de x et y et l'équation (3) aura la forme

$$\frac{\partial\Psi}{\partial y}\cdot\frac{\partial\Delta\Psi}{\partial x} - \frac{\partial\Psi}{\partial x}\cdot\frac{\partial\Delta\Psi}{\partial y} = \nu\Delta\Delta\Psi. \tag{4}$$

Hamel [1], Oseen [2], Rosenblatt [3] s'occupaient de l'équation (4), en donnant quelques solutions singulières.

L'équation (4) est une équation différentielle non-linéaire, du type elliptique. Ce type d'équations a été étudié récemment dans le cas liné-