Travaux cités

[1] S. Gołąb, *Généralisation des équations de Bonnet-Kowalewski dans l'espace à un nombre arbitraire de dimensions*. Ann. Soc. Polon. Math. 22 (1949), p. 97-156.

[2] G. Kowalewski, *Allgemeine natürliche Geometrie und Liesche Transformationsgruppen*, Berlin und Leipzig 1931.

[3] L. Bianchi, *Lezioni di geometria differenziale*, T. I, Pisa 1923.

[4] S. Gołąb et T. Wróbel, *Courbure et torsion géodésique pour les courbes situées sur les hypersurfaces à $n-1$ dimensions plongés dans l'espace à n dimensions*. Ann. Soc. Polon. Math. 26 (1951), p. 28-54.

INSTYTUT MATEMATYCZNY POLSKIEJ AKADEMII NAUK
INSTITUT MATHÉMATIQUE DE L'ACADÉMIE POLONAISE DES SCIENCES

Remarques sur les racines d'une congruence

par W. Sierpiński (Warszawa)

Dans une note encore non publiée M. M. Chojnacka a démontré que pour des modules composés m (par exemple pour les modules 6, 8 et 10) il existe trois entiers a, b, c non congruents deux à deux modulo m, tels que si $f(x)$ est un polynôme en x aux coefficients entiers et si $f(a) \equiv f(b) \equiv 0 \pmod m$, on ait aussi $f(c) \equiv 0 \pmod m$. (M. M. Chojnacka a prouvé que cette proposition est fausse pour $m=4$ et pour les modules premiers.) Je généraliserai ici la proposition de M. M. Chojnacka en démontrant le théorème suivant:

Théorème. *Si m est un module composé $\neq 4$, il existe deux entiers a et b tels que $a \not\equiv 0 \pmod m$, $b \not\equiv 0 \pmod m$ et que, si $f(x)$ est un polynôme aux coefficients entiers tel que $f(a) \equiv f(b) \equiv 0 \pmod m$, on ait aussi $f(0) \equiv 0 \pmod m$.*

Démonstration. Distinguons trois cas:

1° m est le carré d'un nombre premier, $m=p^2$. Comme $m \neq 4$, p est un nombre premier impair. Soit $a=p$, $b=-p$; on a donc $a \not\equiv 0 \pmod m$ et $b \not\equiv 0 \pmod m$. Soit $f(x)$ un polynôme aux coefficients entiers

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n, \tag{1}$$

et supposons $f(a) \equiv f(b) \equiv 0 \pmod m$. Vu que $p^l \equiv 0 \pmod m$ pour $l = 2, 3, \ldots, n$, on trouve, d'après la formule (1), $a_{n-1} p + a_n \equiv 0 \pmod m$ et $-a_{n-1} p + a_n \equiv 0 \pmod m$, d'où, en additionant: $2a_n \equiv 0 \pmod m$, c'est-à-dire $m \mid 2a_n$; m étant un nombre impair, il en résulte que $m \mid a_n$, donc $f(0) = a_n \equiv 0 \pmod m$. On a ainsi $f(0) \equiv 0 \pmod m$.

2° $m = p^\alpha$, où p est un nombre premier et $\alpha \geqslant 3$. On a donc $2\alpha - 3 = \alpha + (\alpha - 3) \geqslant \alpha$, et $m \mid p^{2\alpha-3}$. Posons $a = p^{\alpha-2}$ et $b = p^{\alpha-1}$. On aura $a \not\equiv 0 \pmod m$ et $b \not\equiv 0 \pmod m$. Soit (1) un polynôme aux coefficients entiers et supposons que $f(a) \equiv f(b) \equiv 0 \pmod m$. Comme $\alpha \geqslant 3$ et $p^{2\alpha-3} \equiv 0 \pmod m$, on trouve sans peine $p f(a) \equiv a_{n-1} p^{\alpha-1} + p a_n \pmod m$ et $f(b) \equiv a_{n-1} p^{\alpha-1} + a_n \pmod m$ d'où, en soustrayant: $(p-1) a_n \equiv 0 \pmod m$. On a évidemment $(p, p-1) = 1$ et, comme $m = p^\alpha$, on a $(m, p-1) = 1$. Il résulte donc de $m \mid (p-1) a_n$ que $m \mid a_n$, et $f(0) = a_n \equiv 0 \pmod m$.

3° m n'est pas puissance d'un nombre premier. Comme m est un nombre composé, on peut donc développer m en facteurs premiers $m=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, où $k\geqslant 2, p_1<p_2<\dots<p_k$, et où $a_1,a_2,\dots,a_k$ sont des nombres naturels. Posons $a=m/p_1$ et $b=m/p_2$. On aura $a\not\equiv 0 \pmod m$ et $b\not\equiv 0 \pmod m$. Soit (1) un polynôme aux coefficients entiers et supposons que $f(a)\equiv f(b)\equiv 0 \pmod m$. On a donc $p_2f(b)-p_1f(a)\equiv 0 \pmod m$. On trouve sans peine $p_1a^l\equiv p_2b^l\equiv 0 \pmod m$ pour l naturels, d'où il résulte que $p_1f(a)\equiv p_1a_n \pmod m$ et $p_2f(b)\equiv p_2a_n \pmod m$. On a donc $(p_2-p_1)a_n \equiv 0 \pmod m$, c'est-à-dire $m|(p_2-p_1)a_n$. Or, p_1 et p_2 étant deux facteurs premiers les plus petits du nombre m, les nombres m et p_2-p_1 sont premiers entre eux, et on trouve $m|a_n$, donc $f(0)=a_n\equiv 0 \pmod m$.

Le théorème se trouve ainsi démontré.

En voici maintenant un corollaire immédiat:

COROLLAIRE. *Si m est un module composé $\neq 4$, il existe un polynôme de degré 2, $f(x)=x^2+a_1x+a_2$, aux coefficients entiers, tel que la congruence $f(x)\equiv 0 \pmod m$ ait plus que deux racines.*

En effet, pour obtenir le polynôme $f(x)$ qui satisfasse au corollaire, il suffit de poser $f(x)=(x-a)(x-b)$, où a et b sont des entiers satisfaisant au théorème. D'après ce dernier, la congruence $f(x)\equiv 0 \pmod m$ aura au moins trois racines distinctes: a, b et 0.

Ici encore le nombre composé 4 est exceptionnel. En effet, on démontre sans peine que si (1) est un polynôme aux coefficients entiers tels que a_0 et 4 sont des nombres premiers entre eux, la congruence $f(x)\equiv 0 \pmod 4$ ne peut avoir plus que n racines[1]).

Il en résulte que 4 est le seul nombre composé auquel peut être étendu le théorème de Lagrange, d'après lequel, m étant un nombre premier, n un nombre naturel et (1) un polynôme aux coefficients entiers où $(a_0,m)=1$, la congruence $f(x)\equiv 0 \pmod m$ a au plus n racines.

---

[1]) Voir mon livre, *Teoria liczb* (en polonais), 3me édition, Warszawa-Wrocław 1950, p. 180-181.

Sur quelques propriétés des courbes planes

par S. GOŁĄB (Kraków)

Introduction

On connaît bien, depuis les temps d'Archimède, la propriété des arcs paraboliques disant que si $\overset{\frown}{AB}$ est un arc arbitraire d'une parabole quelconque (de deuxième ordre) et $\overline{AB}$ est la corde joignant les points extrêmes A, B de l'arc, alors si l'on désigne par p la surface du segment parabolique limité par l'arc $\overset{\frown}{AB}$ et la corde $\overline{AB}$ et par P la surface du rectangle de base $\overline{AB}$, circonscrit à ce segment parabolique, on a

$$\frac{p}{P}=\frac{2}{3}. \tag{1}$$

Il est facile de montrer que si un arc convexe est tel que pour chaque couple de ses points A, B le rapport de la surface de la lentille, limitée par la corde $\overline{AB}$ et l'arc $\overset{\frown}{AB}$, à la surface du rectangle de base $\overline{AB}$, circonscrit à cette lentille, est une grandeur constante, cette constante doit être égale à 2/3 et l'arc doit faire partie d'une parabole.

On peut poser le problème suivant: soit $\overset{\frown}{AB}$ l'arc d'une courbe arbitraire plane convexe Γ et $\overline{AB}$ — la corde joignant les points extrêmes A,B. Désignons par L la lentille limitée par l'arc $\overset{\frown}{AB}$ et la corde $\overline{AB}$. Désignons encore par R le rectangle de base $\overline{AB}$ circonscrit à la lentille L (le côté parallèle à $\overline{AB}$ est tangent à l'arc $\overset{\frown}{AB}$). Désignons enfin par p et P respectivement les mésures superficielles des domaines L et R

$$p=m(L), \qquad P=m(R). \tag{2}$$

Demandons quand le rapport p/P est voisin du nombre 2/3 en supposant que le diamètre de la lentille soit assez grand en comparaison avec sa largeur, c'est-à-dire que la hauteur du rectangle soit petite en comparaison avec sa base. Il est évident que le rapport p/P sera un nombre satisfaisant à l'inégalité

$$\frac{1}{2}\leqslant\frac{p}{P}\leqslant 1. \tag{3}$$