NOUVELLES ANNALES DE MATHÉMATIQUES

R. BRICARD

Sur un théorème connu d'arithmétique

Nouvelles annales de mathématiques 4^e série, tome 13 (1913), p. 558-562

<http://www.numdam.org/item?id=NAM_1913_4_13__558_1>

[I13bα]

SUR UN THÉORÈME CONNU D'ARITHMÉTIQUE;

PAR M. R. BRICARD.

1. Ce théorème est le suivant : *Tout nombre premier de la forme* $4q+1$ *est somme de deux carrés.* La démonstration très élémentaire que voici utilise, d'une manière peut-être nouvelle, les considérations géométriques que plusieurs auteurs et surtout Minkowski ont introduites avec succès dans la Théorie des nombres, sous une forme d'ailleurs bien plus générale (*voir* par exemple les *Leçons* de M. A. Châtelet, p. 108).

2. Soit p le nombre premier considéré. On déduit facilement du théorème de Wilson, comme on sait, la congruence

$$m^2+1\equiv 0 \pmod{p}, \tag{1}$$

en posant

$$m = \left(\frac{p-1}{2}\right)!.$$

Multiplions successivement par $1^2, 2^2, \ldots, (p-1)^2$ les deux membres de la congruence (1) et désignons par x_i le reste minimum de $mi \pmod p$, de sorte qu'on a

$$x_i \equiv mi \pmod p \qquad (0 < x_i < p).$$

On formera ainsi les $p-1$ congruences

$$(2) \qquad x_i^2 + i^2 \equiv 0 \pmod p \qquad (i = 1, 2, \ldots, p-1).$$

Prenons maintenant deux axes rectangulaires et marquons les $p-1$ points M_i, de coordonnées x_i, i. Chacun d'eux a son abscisse et son ordonnée au moins égales à 1 et au plus égales à $p-1$. Tous ces points sont donc contenus (au sens large) à l'intérieur d'un carré C de côté égal à $p-2$.

Le carré de la distance $M_i M_j$ *de deux quelconques de ces points est divisible par* p. En effet, si l'on désigne par d_{ij} ce carré, on a

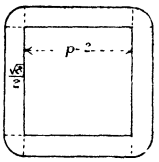
$$(3) \qquad \begin{aligned} d_{ij} &= (x_i - x_j)^2 + (i-j)^2 \equiv (mi - mj)^2 + (i-j)^2 \\ &= (i-j)^2(m^2+1) \equiv 0 \pmod p, \end{aligned}$$

d'après la congruence (1).

Soit maintenant δ la plus petite des quantités d_{ij}. Nous allons montrer que δ est plus petit que $2p$, du moins si p dépasse un certain nombre. En effet, décrivons les $p-1$ cercles Γ_i ayant pour centres les points M_i et pour rayon commun $\frac{\sqrt{\delta}}{2}$. Tous ces cercles sont au plus tangents et n'ont pas de parties communes. Menons d'autre part (*fig.* 1), extérieurement au carré C, des parallèles à ses côtés, à une distance égale à $\frac{\sqrt{\delta}}{2}$, et raccordons-les par quatre quarts de cercle, ayant leurs

centres aux sommets du carré. Tous les cercles Γ_i sont contenus à l'intérieur de la région limitée par le con-

Fig. 1.



tour ainsi constitué. La somme de leurs aires est donc inférieure à l'aire de cette région, ce qui fournit immédiatement l'inégalité

$$(p-1)\pi\frac{\delta}{4} < (p-2)^2 + 4(p-2)\frac{\sqrt{\delta}}{2} + \pi\frac{\delta}{4}.$$

On peut faire passer le dernier terme du second membre dans le premier et diviser ensuite par $p-2$. Il vient ainsi :

$$\pi\frac{\delta}{4} < p - 2 + 2\sqrt{\delta},$$

et, *a fortiori*,

$$\frac{3\delta}{4} < p + 2\sqrt{\delta},$$

ou

$$\delta - \frac{8}{3}\sqrt{\delta} - \frac{4}{3}p < 0.$$

L'équation du second degré en $\sqrt{\delta}$, obtenue en annulant le premier membre, a ses racines de signes contraires. Il faut donc que $\sqrt{\delta}$ soit inférieur à la racine positive, ce qui donne

$$\sqrt{\delta} < \frac{4}{3} + \sqrt{\frac{16}{9} + \frac{4}{3}p}.$$

Le second membre sera inférieur à $\sqrt{2p}$, si l'on a

$$\frac{16}{9} + \frac{4}{3}p < \left(\sqrt{2p} - \frac{4}{3}\right)^2 = 2p - \frac{8}{3}\sqrt{2p} + \frac{16}{9},$$

ce qui se réduit à

$$\frac{2}{3}p > \frac{8}{3}\sqrt{2p},$$

ou

$$p > 32.$$

En résumé, il existe un nombre δ, somme de deux carrés et multiple de p, d'après la congruence (3), et inférieur à $2p$, si p est plus grand que 32. Ce multiple est donc p lui-même.

Nous avons ainsi démontré la proposition rappelée au début de cette Note, pour les nombres p supérieurs à 32. Pour les nombres inférieurs (5, 13, 17, 29) la vérification est immédiate.

La même démonstration, convenablement modifiée, permet d'établir les théorèmes analogues et bien connus aussi relatifs aux représentations de certains nombres premiers par les formes $x^2 + 2y^2$, $x^2 + 3y^2$, et même par la forme indéfinie $x^2 - 2y^2$. Voici l'esquisse de la démonstration pour ce dernier cas :

Soit p un nombre premier dont 2 est résidu quadratique (nombre de la forme $8q+1$ ou de la forme $8q+7$). On considérera des points M_i de coordonnées x_i, $\sqrt{2}\,i$ ($i = 1, \ldots, p-1$), tels que

$$x_i^2 - 2i^2 \equiv 0 \pmod{p},$$

et tous contenus à l'intérieur d'un rectangle de côtés $p-2$, $\sqrt{2}(p-2)$; pour deux quelconques d'entre eux, on a

$$\delta_{ij} = (x_i - x_j)^2 + 2(i-j)^2 \equiv 0 \pmod{p}.$$

Par le même raisonnement géométrique que précédemment, on reconnaît que, si p est plus grand qu'un certain nombre, on a pour un choix convenable des nombres i et j,

$$(x_i - x_j)^2 + 2(i-j)^2 < 2p.$$

On en déduit

$$|\delta_{ij}| < 2p$$

et par suite

$$|\delta_{ij}| = p.$$

Par conséquent p est représentable par l'une des formes $x^2 - 2y^2$, $-x^2 + 2y^2$. On sait d'ailleurs que ces formes sont équivalentes, en vertu de l'identité

$$x^2 - 2y^2 = 2(x+y)^2 - (x+2y)^2.$$