

G. FONTENÉ

Sur les nombres de la forme $X^2 + XY + Y^2$

Nouvelles annales de mathématiques 4^e série, tome 10
(1910), p. 217-221

http://www.numdam.org/item?id=NAM_1910_4_10__217_1

© Nouvelles annales de mathématiques, 1910, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

[13a]

SUR LES NOMBRES DE LA FORME $X^2 + XY + Y^2$;

PAR M. G. FONTENÉ.

1. Soit p un nombre premier, au moins égal à 3, et soit λ un des nombres de la suite complète

$$1, 2, 3, \dots, p-1;$$

points diamétralement opposés. C et C_1 sont deux des circonférences circonscrites à ce contre-parallélogramme.

On voit qu'il existe quatre circonférences circonscrites au contre-parallélogramme (on ne s'occupe pas des grands cercles contenant quatre sommets). Si l'on convient de ne jamais associer deux circonférences diamétralement opposées, on voit que les quatre circonférences circonscrites associées deux à deux conduisent toujours aux mêmes quatre centres de similitude qui sont les pôles des quatre circonférences inscrites dans le contre-parallélogramme. Les circonférences circonscrites se coupent entre elles sous des angles égaux à ceux du contre-parallélogramme.

nous voulons étudier la congruence

$$(A) \quad x^2 - \lambda x + \lambda^2 \equiv 0 \pmod{p}.$$

Cette congruence admet au plus deux solutions; car, si elle admet la solution $x = a$, ce qui donne

$$a^2 - \lambda a + \lambda^2 \equiv 0,$$

on peut écrire

$$(x - a)[(x + a) - \lambda] \equiv 0.$$

Elle peut n'admettre qu'une solution (*voir plus loin*). Elle peut être impossible.

Une solution de cette congruence ne peut d'ailleurs être 0 ou λ , les deux premiers termes formant le produit $x(x - \lambda)$, de sorte qu'une solution appartient nécessairement à la *suite réduite*

$$(S) \quad 1, 2, 3, \dots, p-1 \quad (\text{sans } \lambda).$$

2. Si a est un des nombres de cette suite réduite, on peut trouver dans la suite complète un nombre b et un seul, tel que l'on ait

$$(1) \quad ab - \lambda a + \lambda^2 \equiv 0 \pmod{p},$$

car on peut écrire

$$ab \equiv \lambda(a - \lambda) \pmod{p},$$

et le second membre n'est pas congru à zéro suivant le module p ; le nombre b n'est d'ailleurs pas λ , de sorte qu'il fait partie de la suite réduite (S).

On aura, de même, en supprimant l'indication du module,

$$(2) \quad bc - \lambda b + \lambda^2 \equiv 0,$$

le nombre c faisant partie de la suite (S), et je dis qu'on

a alors

$$(3) \quad ca - \lambda c + \lambda^2 \equiv 0.$$

Éliminons en effet b entre les congruences (1) et (2); la seconde peut s'écrire

$$bc - \lambda(b - \lambda) \equiv 0;$$

en multipliant par a , et en remplaçant ab par $\lambda(a - \lambda)$, et $a(b - \lambda)$ par $-\lambda^2$, d'après la première, on a

$$\lambda c(a - \lambda) + \lambda^3 \equiv 0,$$

ou

$$ca - \lambda c + \lambda^2 \equiv 0.$$

3. Si deux des nombres a , b , c , sont égaux, ces trois nombres sont égaux. Ce fait, qui est intuitif sur les relations (1) (2) (3), se vérifie naturellement sur les relations (1) et (2), sans avoir recours à (3), soit qu'on suppose a ou c égal à b , soit qu'on suppose $a = c$. Le nombre a est alors une racine de la congruence (A).

Si la congruence (A) est impossible, les nombres de la suite (S) se répartissent donc en groupes de trois termes, et l'on a

$$p - 2 = 3k, \quad p = 3k' - 1;$$

Si cette congruence est possible avec deux solutions, les nombres de la suite (S), sauf deux, se répartissent en groupes de trois termes, et l'on a

$$p - 2 = 3k + 2, \quad p = 3k' + 1;$$

Si la congruence est possible avec une seule solution, on a

$$p - 2 = 3k + 1, \quad p = 3.$$

Les réciproques sont, par suite, exactes : *La congruence*

$$x^2 - \lambda x + \lambda^2 \equiv 0 \pmod{p}, \quad \lambda \neq 0,$$

est impossible si p est de la forme $3k' - 1$, possible avec deux solutions si p est de la forme $3k' + 1$, possible avec une solution si $p = 3$.

[On peut voir directement que le seul cas où la congruence ait une solution unique est le cas $p = 3$. Lorsque la congruence est possible, si elle admet la racine a , elle admet la racine $\lambda - a$ ou $p + \lambda - a$, qui ne se confond avec la première que si l'on a

$$2a - \lambda \equiv 0,$$

par suite, en remplaçant λ par $2a$ dans la congruence,

$$a^2 - 2a^2 + 4a^2 \equiv 0, \quad 3a^2 \equiv 0, \quad p = 3.$$

Pour $p = 3$, s'il existe un nombre a vérifiant la congruence

$$2a - \lambda \equiv 0 \pmod{3},$$

on vient de voir que ce nombre est solution de la congruence (A), et solution unique; ce nombre existe, et c'est $3 - \lambda$; on peut avoir $\lambda = 1$, $a = 2$, ou $\lambda = 2$, $a = 1$.]

4. Les considérations précédentes ont été présentées par M. Bricard pour $\lambda = 1$, en vue d'établir d'une manière élémentaire le caractère quadratique du nombre -3 par rapport à un module premier (*N. A.*, 3^e série, t. XVI, p. 546). On ramènerait le cas général à ce cas particulier en observant qu'on peut avoir

$$a = \lambda\alpha + \text{mult. } p,$$

$$b = \lambda\beta + \text{mult. } p,$$

ce qui transforme l'égalité (1) en celle-ci :

$$\alpha\beta - \alpha + 1 \equiv 0 \pmod{p}.$$

Mais on vient de voir que le cas général se traite exactement comme le cas particulier.

5. Il résulte de ce qui précède que *tout nombre de la forme*

$$X^2 + XY + Y^2,$$

X et Y étant premiers entre eux, a ses facteurs premiers de la forme $3k' + 1$ (ou encore $6k'' + 1$), à l'exception du facteur 3 qui existe dans l'hypothèse $X - Y = \text{mult. } 3$, dans cette hypothèse seulement, et qui existe alors avec l'exposant 1. En effet, un tel nombre ne peut d'abord admettre le diviseur premier 2. S'il admet le diviseur premier p , au moins égal à 3, soit

$$X = \text{mult. } p + x, \quad Y = \text{mult. } p - \lambda,$$

x et λ étant différents de zéro; on a alors

$$x^2 - \lambda x + \lambda^2 \equiv 0 \pmod{p},$$

avec $\lambda \neq 0$, ce qui exige $p = 3k' + 1$, ou $p = 3$. Pour $p = 3$, on doit avoir

$$x = 3 - \lambda \quad \text{ou} \quad X = Y + 3k;$$

le nombre considéré est alors

$$3(Y^2 + 3kY + 3k^2),$$

et il contient une seule fois le facteur 3.

Le résultat obtenu se généralise (question 2137); mais je ne vois pas comment on pourrait généraliser les considérations qui y ont conduit ici.