

**Généralisation de la théorie des nombres  
associés et théorèmes y relatifs. D'après  
M. Lejeune-Dirichlet**

*Nouvelles annales de mathématiques 1<sup>re</sup> série*, tome 4  
(1845), p. 379-382

[http://www.numdam.org/item?id=NAM\\_1845\\_1\\_4\\_\\_379\\_1](http://www.numdam.org/item?id=NAM_1845_1_4__379_1)

© Nouvelles annales de mathématiques, 1845, 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/>

---

## GÉNÉRALISATION

*de la théorie des nombres associés et théorèmes y relatifs.*

( D'après M. Lejeune-Dirichlet ( Crelle , t. III , p. 390. 1828. )

—

I. *Observation préliminaire.* Dans tout ce qui suit, il ne

s'agit que de nombres entiers ; la lettre  $p$  est exclusivement consacrée à désigner un nombre premier ;  $a = b$  désigne que  $a$  est égal à  $b$  ;  $a = \dot{b}$  désigne que  $a$  est un multiple de  $b$  ;  $a < \dot{b}$  désigne que  $a$  n'est pas un multiple de  $b$ . Ces symboles ne sont pas ceux de l'auteur.

II. *Définition d'Euler.* Si l'on a  $mn - 1 = \dot{p}$  ;  $m$  et  $n$  étant moindres que  $p$ ,  $m$  et  $n$  sont dits nombres associés (voir N<sup>l</sup>es Ann., t. III, p. 193, et Prouhet, t. IV, p. 273).

III. *Définition générale de M. Lejeune - Dirichlet.* Si  $mn - a = \dot{p}$  ;  $a < \dot{p}$  ; et  $m$  et  $n < p$  ;  $m$  et  $n$  sont des nombres associés ; lorsque  $a = 1$  ; cette définition rentre dans celle d'Euler.

IV. Soit  $[p - 1]$  le produit continu de 1 jusqu'à  $p - 1$  inclus. Chaque facteur  $m$  de ce produit a son associé  $n$  dans le même produit, relativement à  $p$ , et n'en a qu'un ; à moins que  $m$  ne soit égal à  $n$ , cas que nous réservons ; le produit se partage donc en  $\frac{p-1}{2}$  groupes de nombres associés ; donc on a ce théorème :

$$[p - 1] - a^{\frac{p-1}{2}} = p.$$

Les moyens de démonstration sont les mêmes qu'on a employés pour établir le théorème de Wilson (t. III, p. 194).

V. Venons au cas où  $m = n$  ; donc  $m^2 - a = \dot{p}$  ; on aura évidemment aussi  $(p - m)^2 - a = \dot{p}$  ;  $m$  et  $p - m$  sont les deux seuls nombres qui soient associés à eux-mêmes, *associés doubles* (Voir p. 273). S'il y avait un troisième  $x$ , on aurait donc :  $x^2 - m^2 = (x - m)(x + m) = \dot{p}$ . congruence impossible. Il reste donc  $\frac{p-3}{2}$  groupes de nombres associés inégaux ; ainsi l'on a :

$$[p-1] - a^{\frac{p-3}{2}} m(p-m) = p, \text{ ou bien } [p-1] + a^{\frac{p-3}{2}} m^2 = p ;$$

mais  $m^2 = \dot{p} + a$  ;

donc  $[p-1] + a^{\frac{p-1}{2}} = \dot{p}$ .

VI. *Définition du RÉSIDU QUADRATIQUE.* On dit que le nombre  $a$  est résidu quadratique du nombre premier  $p$ , lorsqu'on peut satisfaire à cette congruence  $x^2 - a = \dot{p}$  ; il est évident que l'unité est résidu quadratique d'un nombre premier quelconque. Il suffit de faire  $x = 1$  ; en général, si  $a$  est un carré, il est résidu quadratique par rapport à un nombre premier quelconque ; on fait  $x$  égal à la racine carrée de  $a$ .

VII. Les deux théorèmes (IV et V) peuvent se réunir en un seul ; savoir :  $[p-1] \pm a^{\frac{p-1}{2}} = \dot{p}$  ; le signe supérieur a lieu lorsque  $a$  est résidu quadratique relativement à  $p$  ; et le signe inférieur lorsque  $a$  n'est pas résidu quadratique.

VIII. *Théorème de Wilson.* Lorsque  $a = 1$  ; on a donc  $[p-1] + 1 = \dot{p}$ .

IX. *Théorème d'Euler.*  $[p-1] = \dot{p} - 1$  ; donc  $-1 \pm a^{\frac{p-1}{2}} = \dot{p}$  ; ou changeant les signes,  $a^{\frac{p-1}{2}} \pm 1 = \dot{p}$  ; le signe supérieur lorsque  $a$  n'est pas résidu quadratique, et le signe inférieur lorsque  $a$  est résidu quadratique.

X. *Théorème de Fermat.*  $a^{\frac{p-1}{2}} = p \mp 1$  ; élevant au carré on a donc  $a^{p-1} - 1 = \dot{p}$ .

*Observation.* M. Lejeune-Dirichlet donne une seconde démonstration du théorème de Fermat, que M. Catalan a trouvée de son côté, par les considérations sur les fractions périodiques ( t. I, p. 463, et t. IV, p. 273 ). Tm.

*Avis concernant les tables de Callet.*

Le logarithme naturel de 1099 est fautif : au lieu de 7,0021(1)5954403, il faut lire : 7,002155954403. On trouve

**cette rectification dans le Journal de Crelle, t. IV, p. 291.  
Elle est signalée par M. le professeur Gudermann de Clèves.**

---

---