NOUVELLES ANNALES DE MATHÉMATIQUES

E. CAHEN

Sur une question proposée par M. Fontené

Nouvelles annales de mathématiques 4^e série, tome 11 (1911), p. 70-72

<http://www.numdam.org/item?id=NAM_1911_4_11__70_0>

[17a]

SUR UNE QUESTION PROPOSÉE PAR M. FONTENÉ;

PAR M. E. CAHEN.

De la propriété énoncée par M. Fontené (4e série, t. IX, p. 384) et résolue par M. Bricard (4e série, t. X, p. 475), on peut déduire deux conséquences intéressantes. Je suppose $b = 1$ de sorte que le théorème prend la forme suivante : *p étant un nombre premier et a un entier non* $\equiv 1 \pmod p$, *le nombre*

$$a^{p-1} + a^{p-2} + \ldots + a + 1$$

a tous ses diviseurs premiers et, par suite, tous ses diviseurs $\equiv 1 \pmod p$.

I. *Le polynome* $x^{p-1} + x^{p-2} + \ldots + x + 1$ *est irréductible.*

Car soit

$$x^{p-1} + x^{p-2} + \ldots + x + 1 = f(x)\, g(x),$$

f et g étant deux polynomes entiers à coefficients entiers. Donnons à x toutes les valeurs incongrues $(\mathrm{mod}\, p)$ possibles, sauf la valeur 1, soient 0, 2, 3, ..., $p - 1$. Pour chacune de ces $p - 1$ valeurs $f(x)$, qui est un diviseur de $x^{p-1} + x^{p-2} + \ldots + x + 1$, prend une valeur $\equiv 1 \pmod p$. Donc la congruence

$$f(x) \equiv 1 \pmod p$$

a $p - 1$ racines incongrues. Donc ou bien elle est identique, ou bien son degré ne peut être intérieur à $p - 1$. Or, si elle est identique, comme son premier

coefficient est manifestement égal à 1, c'est que $f(x)$ se réduit à 1. Si elle est de degré $p-1$, c'est $g(x)$ qui se réduit à 1. Donc..., etc.

II. *Il y a une infinité de nombres premiers* $\equiv 1 \pmod p$.

Ce n'est qu'un cas particulier du théorème de Dirichlet, mais la démonstration suivante est intéressante par sa simplicité.

D'abord il existe au moins un tel nombre, car il suffit de donner à x une valeur non congrue à $1 \pmod p$, par exemple 2, et de calculer un facteur premier du nombre obtenu $2^p - 1$, pour en avoir un.

Soient alors $\alpha, \beta, \ldots, \lambda$ des nombres premiers $\equiv 1 \pmod p$, je vais en calculer un autre. Il suffit pour cela de former le nombre

$$(\alpha\beta\ldots\lambda)^{p-1} - (\alpha\beta\ldots\lambda)^{p-2} + \ldots - \alpha\beta\ldots\lambda + 1.$$

C'est la valeur que prend $x^{p-1} + x^{p-2} + \ldots + x + 1$, lorsque $x = -\alpha\beta\ldots\lambda$. Or cette valeur de x est $\equiv -1 \pmod p$. Donc tout facteur premier de ce nombre est

$$\equiv 1 \pmod p$$

et d'ailleurs ce ne peut être ni α, ni β, ..., ni λ. Donc..., etc.

Le théorème en question se généralise en remplaçant p par un nombre non premier n et

$$x^{p-1} + x^{p-2} + \ldots + x + 1$$

par le polynome qui donne les racines primitives de x^{n-1}. Cette démonstration du théorème de Dirichlet ou des démonstrations du même genre sont connues depuis longtemps. *Voir*, par exemple, *Encyclopédie des Sciences mathématiques* (édition française, t. I_3,

p. 285) et E. LANDAU, *Handbuch der Lehre der Verteilung der Primzahlen*, t. I, p. 436 et suiv.