NOUVELLES ANNALES DE MATHÉMATIQUES

TERQUEM

Théorème de Wilson d'après M. Gauss

Nouvelles annales de mathématiques 1re série, tome 2 (1843), p. 193-195

<http://www.numdam.org/item?id=NAM_1843_1_2__193_0>

THÉORÈME DE WILSON.

D'APRÈS M. GAUSS (*).

1. On peut toujours résoudre en nombres entiers, l'équation indéterminée $ax-1=\dot{p}$; où $\dot{p}$ désigne un multiple du nombre premier p, et a un nombre entier positif moindre que p. Les moyens de solution, qu'on doit à *Bachet* (**), sont enseignés dans tous les traités d'algèbre.

2. Il existe toujours un nombre entier x plus petit que p, qui satisfait à la question, mais il n'en existe qu'un seul; car si x est plus grand que p en rejetant les multiples de p, le reste plus petit que p, satisfait à l'équation; s'il y avait deux nombres x', x'', tous deux moindres que p et résolvant chacun l'équation, on aura donc $a(x'-x'')=\dot{p}$, équation impossible puisque les deux facteurs a et $x'-x''$ sont chacun moindres que le nombre premier p.

3. A chaque nombre donné a correspond donc un seul nombre x plus petit que p; ces deux nombres sont dits, *nombres associés*; dénomination qu'on doit à *Euler*. Ainsi le produit de deux nombres associés est de la forme $\dot{p}+1$.

4. Si $a=p-1$, le nombre associé est évidemment aussi $p-1$.

5. Soit le produit continuel $2.3.4.(p-3)(p-2)$. Ce produit peut se décomposer en $\frac{p-3}{2}$ couples, formés chacun de deux nombres associés, car le même nombre ne peut appar-

(*) *Disquisitiones arithmeticæ*, sect. III, art. 76.

(**) Problèmes plaisans et délectables qui se font par les nombres. Lyon, 1624, 2e édit., refondue dans les Recréations mathématiques d'Ozanam.

Meziriac (Claude-Gaspar Bachet, sieur de), né à Bourg en Bresse, 9 oct. 1581; mort le 25 février 1638.

tenir à deux couples (2), mais chaque couple est de la forme $\dot{p}+1$, le produit total est donc de la même forme.

Donc $2.\ 3.\ 4\ .\ .\ .\ .\ .\ p-2=\dot{p}+1$

$1.\ 2.\ 3\ .\ .\ .\ .\ .\ p-2.p-1=\dot{p}-1$

et $1.\ 1.\ 2\ .\ .\ .\ .\ .\ p-1+1=\dot{p}$

ainsi, si l'on ajoute une unité à un produit continuel formé jusqu'au nombre qui précède immédiatement un nombre premier, la somme est un multiple de ce nombre premier.

6. Si p n'est pas un nombre premier, l'équation $1.2.3..\ldots p-1+1=\dot{p}$ devient impossible, car si p n'est pas un nombre premier, il a nécessairement un diviseur plus petit que $p-1$; ce diviseur se trouve donc dans le produit continuel, et comme il divise $\dot{p}$, il devra donc diviser l'unité, ce qui est impossible; donc si l'on ajoute l'unité à un produit continuel formé jusqu'à un nombre qui précède immédiatement un nombre non premier, la somme n'est jamais un multiple du nombre non premier.

7. Les deux propositions précédentes, l'une affirmative, l'autre négative, forment le théorème que Waring (*) attribue à Wilson; il a été démontré pour la première fois par Lagrange (Voir *Nouvelles annales*, tome I, p. 178) et ensuite par Euler (*Opuscul. analyt.*, t. I, p. 329).

8. En admettant l'existence des racines primitives, on peut déduire facilement le théorème de *Wilson* de celui de *Fermat*. Soit r une racine primitive à l'égard du nombre premier p; le théorème de Fermat donne $r^{p-1}-1=\dot{p}$, donc $r^{p(p-1)}-1=\dot{p}$; d'où

$$\left(r^{\frac{p(p-1)}{2}}+1\right)\left(r^{\frac{p(p-1)}{2}}-1\right)=\dot{p};$$

(*) *Meditationes analyticæ*, 3e edit., p. 380. Edit. 1776 et 1784, in-4°. Waring (Edouard), né 1734; mort en 1798.

mais $\frac{p(p-1)}{2}$ n'est pas un multiple de $p-1$, et r étant une racine primitive, il s'ensuit que $r^{\frac{p(p-1)}{2}}-1$ n'est pas divisible par p, l'on a donc

$$r^{\frac{p(p-1)}{2}}+1=p; \quad \text{or} \quad r^{\frac{p(p-1)}{2}}=r.r^2.r^3.....r^{p-1};$$

donc par définition de la racine primitive en divisant tous les facteurs r, r^2, r^3 par p, on a pour restes les nombres de 1 à $p-1$; C. Q. F. D.

Cette démonstration est de M. le professeur Verhulst (Quételet, *Correspondance mathématique*, tome III, p. 71; 1827). Je n'avais pas ce renseignement, en écrivant la note du tome I (p. 469).

Tm.