NOUVELLES ANNALES DE MATHÉMATIQUES

E. PROUHET

Note sur les nombres associés ; généralisation du théorème de Wilson

Nouvelles annales de mathématiques 1re série, tome 4 (1845), p. 273-278

<http://www.numdam.org/item?id=NAM_1845_1_4__273_0>

NOTE

Sur les nombres associés; généralisation du théorème de Wilson.

PAR M. E. PROUHET,

Professeur au collége royal d'Auch.

1. Deux entiers a et a' inférieurs et premiers à P sont dits *associés* par rapport à ce dernier nombre, lorsque le produit est de la forme $\dot{P}+1$. En général a' est différent de a; mais lorsque $a=1$, ou $P-1$, l'associé de a est le nombre a lui-même, et on a l'égalité

$$a^2=\dot{P}+1.$$

Les nombres qui jouissent de cette propriété pourraient être nommés *associés doubles*, par rapport à P. Notre principal but, dans cette note, est de rechercher combien il y a d'associés doubles pour chaque valeur attribuée à P, ou, en d'autres termes, combien il y a d'entiers moindres que P propres à satisfaire à la relation

$$x^2-1=\dot{P}. \tag{1}$$

I.

2. Nous supposerons d'abord P impair, et égal au produit de deux nombres A et B premiers entre eux. On satisfera à la relation (1) en posant

$$x-1=\dot{A},\quad x+1=\dot{B}.$$

C'est-à-dire en prenant pour x un nombre à la fois $\dot{A}+1$

et $\dot{B}-1$; nous savons qu'il existe toujours un nombre moindre que AB et remplissant ces deux conditions (*).

On pourra encore prendre x à la fois $\dot{A}-1$ et $\dot{B}-1$; ce qui donnera un second associé double, différent du premier ; puisque les deux nombres $x-1$ et $x+1$, dont la différence est 2, ne peuvent pas avoir de facteur commun impair.

Ainsi chaque manière de décomposer P en deux facteurs premiers entre eux donne lieu à deux associés doubles.

On n'a pas à craindre qu'un autre mode de décomposition donne les mêmes associés Car, soit encore $P=A'B'$. Si l'on avait en même temps :

$$x-1=\dot{A},\quad x+1=\dot{B}:$$
$$x-1=\dot{A}',\quad x+1=\dot{B}',$$

A' devrait être premier avec B, et B' avec A, d'après la remarque faite plus haut. Donc, puisque $AB=A'B'$, A' devrait diviser B, et de même B' devrait diviser A ; ce qui ne peut avoir lieu ; à moins que $A'=B$, $B'=A$, ou que les deux modes de décomposition soient identiques, ce qui est contraire à l'hypothèse. Donc.

Il y a deux fois *autant d'associés doubles par rapport à un nombre* impair P, *qu'il y a de manières de décomposer* P *en deux facteurs premiers entre eux.*

II.

3. En second lieu, supposons $P=2^mA.B$, A et B étant deux nombres impairs premiers entre eux, et m étant *au moins égal* à 2.

Si l'un des deux facteurs $x-1$, $x+1$ est pair, il en sera de même de l'autre. On satisfera donc à la relation (1) en posant

$$x-1=\dot{(2^{m-1}A)},\quad x+1=\dot{B},$$

(*) Voir tome IV, p. 75, lemme 1

ou en prenant x à la fois $(\dot{2^{m-1}A})+1$ et $\dot{B}-1$: or il existe *deux* nombres moindres que $2(^{m-1}A.E)$, et remplissant ces deux conditions.

On peut encore prendre pour x un nombre à la fois $(\dot{2^{m-1}A})-1$ et $\dot{B}+1$, ce qui donne deux associés doubles. On démontrerait comme plus haut, qu'ils sont différents des premiers.

Ainsi chaque manière de décomposer P en deux facteurs premiers entre eux, donne lieu à quatre associés doubles.

4. Voyons maintenant si les associés doubles provenant des deux décompositions $P=2^mA.B$ et $P=2^mA'.B'$ ne peuvent pas être les mêmes. Pour qu'une pareille circonstance se présente, il faut que le nombre x soit dans l'un des quatre cas suivants :

I. $x-1=(\dot{2^{m-1}A})=(\dot{2^{m-1}A'}), x+1=\dot{B} \quad =\dot{B}'$

II. $x-1=\dot{B} \quad =\dot{B}' \quad , x+1=(\dot{2^{m-1}A}) = (\dot{2^{m-1}A'})$

III. $x-1=(\dot{2^{m-1}A})=\dot{B}' \quad , x+1=\dot{B} \quad =(\dot{2^{m-1}A'})$

IV. $x-1=\dot{B} \quad =(\dot{2^{m-1}A'}), x+1=(\dot{2^{m-1}A}) = \dot{B}'$

Mais comme $x-1$ et $x+1$ n'ont pas de facteur commun autre que 2, les deux premiers cas ne peuvent se présenter ; et les deux derniers cas n'ont lieu que si on a simultanément : $m=2$, $A=B'$, $B=A'$.

Ainsi ce n'est que dans le cas de $m=2$ que deux modes de décompositions ($P=4A.B$, $P=4B.A$), donnent les mêmes associés. Donc

Suivant que $\frac{P}{4}$ est impair, *ou* pair, *il y a* deux fois *ou* quatre fois *autant d'associés doubles, par rapport à* P, *qu'il y a de manières de décomposer* P *en deux facteurs premiers entre eux.*

5. Nous avons laissé de côté le cas où $m=1$, c'est-à-dire où P est double d'un nombre impair, parce que les raisonnements précédents ne sont plus applicables. En effet, on ne peut alors satisfaire à la relation (1) qu'en posant

$$x-1=\dot{(2A)}, \quad x+1=\dot{B}$$

ou bien

$$x-1=\dot{B} \quad , \quad x+1=\dot{\overline{2A}}$$

ce qui donne seulement deux associés doubles. En outre, les associés doubles provenant des deux décompositions $P=2A.B$ et $P=2B.A$ sont évidemment les mêmes. Donc,

Il y a autant d'associés doubles, par rapport à un nombre P *double* d'un nombre impair, *qu'il y a de manières de décomposer* P *en deux facteurs premiers entre eux.*

III.

6. Désignons par ν le nombre des associés doubles par rapport à P ; par K le nombre des facteurs premiers inégaux de P. On sait que 2^{k-1} indique de combien de manières on peut décomposer P en deux facteurs premiers entre eux (*). On aura donc d'après les nos 2, 4, 5,

$\nu=2^k$ *si* P *est impair.*
$\nu=2^{k-1}$ *si* P *est double d'un nombre impair.*
$\nu=2^k$ *si* P *est quatre fois un nombre impair.*
$\nu=2^{k+1}$ *si* P *est quatre fois un nombre pair.*

7. Ces formules font voir que si P est une puissance ou le double d'une puissance d'un nombre premier impair, il n'y a que deux associés doubles, qui sont : 1, P—1.

Si $P=2^m$, m étant supérieur à 2, il y a quatre associés doubles, qui sont :

$$1, \quad 2^{m-1}, \quad 1, \quad 2^{m-1}+1, \quad 2^m-1.$$

(*) Legendre, Théorie des nombres, t. I, p. 13.

IV.

8. Désignons par P_1 le produit de tous les nombres inférieurs et premiers à P, et cherchons le reste de la division de P_1 par P.

Les nombres inférieurs et premiers à P, à l'exception des associés doubles, se groupent par couples dont le produit est de la forme $\dot{P}+1$, le produit de tous ces couples sera donc de même forme. Ainsi le reste de P_1 dépendra du produit de tous les associés doubles.

Pour trouver ce dernier reste, je remarque d'abord que si a est associé double, il en est de même de $P-a$, car on a

$$(P-a)^2 = \dot{P} + a^2 = \dot{P} + 1,$$

et ensuite, que

$$a(P-a) = \dot{P} - a^2 = \dot{P} - 1.$$

Les associés doubles se groupent donc par couples dont le produit est de la forme $\dot{P}-1$. Par conséquent le produit des associés doubles sera $\dot{P}+1$ ou $\dot{P}-1$, suivant que le nombre de ces couples sera *pair* ou *impair*; c'est-à-dire suivant que ν sera ou ne sera pas divisible par 4.

Donc, si on se rappelle les valeurs de ν trouvées plus haut, on en déduira le théorème suivant :

Le produit de tous les nombres inférieurs et premiers à P, *est de la forme* $\dot{P}+1$, *excepté lorsque* P *est une puissance d'un nombre premier, ou le double d'une puissance d'un nombre premier.* Dans ce dernier cas, le produit en question est de la forme $\dot{P}-1$.

On voit que cet énoncé comprend le théorème de *Wilson*, déjà démontré dans ce recueil, par des considérations analogues. (Voir t. II, p. 193).

Note. Nous possédons depuis longtemps une démonstration du théorème de *Wilson*, généralisée et fondée sur la doctrine

des résidus quadratiques de Gauss (*Disquisitiones*, sect. IV), nous la donnerons avec l'exposition de cette doctrine dont les théorèmes de M. Prouhet sont aussi des conséquences. Il en est de même de la démonstration que M. Poinsot vient de publier récemment dans le journal de M. Liouville (janvier et février 1845), dont celle de M. Prouhet ne diffère pas essentiellement. Tm.