NOUVELLES ANNALES DE MATHÉMATIQUES

E. PROUHET

Note sur le nombre qui indique combien il y a d'entiers inférieurs et premiers à un nombre donné

Nouvelles annales de mathématiques 1re série, tome 4 (1845), p. 75-81

<http://www.numdam.org/item?id=NAM_1845_1_4__75_0>

NOTE

Sur le nombre qui indique combien il y a d'entiers inférieurs et premiers à un nombre donné.

PAR M. E. PROUHET,
professeur au College royal d'Auch.

—

1. Le nombre qui indique combien il y a d'entiers inférieurs et premiers à un nombre donné, jouit de plusieurs propriétés importantes. Mais, comme chaque fois qu'on en parle, on est obligé de le désigner par une longue périphrase, ces propriétés deviennent d'un énoncé fastidieux et d'une démonstration prolixe. Afin d'éviter cet inconvénient, nous proposerons de désigner ce nombre par un nom particulier et de choisir pour cet objet le mot *indicateur*, qui n'a encore reçu aucun emploi en mathématiques. Dans le courant de cet article, le symbole i (N) servira à représenter l'indicateur d'un entier N (*).

I.

Nous allons d'abord nous proposer de trouver l'indicateur d'un nombre N, décomposé en ses facteur premiers. Les deux lemmes suivants faciliteront beaucoup cette recherche.

2. Lemme I. *Si a et b sont deux nombres premiers entre eux ; α un nombre inférieur et premier à a ; β un nombre inférieur et premier à b ; il n'existe qu'un seul nombre $z < ab$, qui soit à la fois $z + \alpha$ et $b + \beta$.*

Démonstration. La recherche du nombre z revient à la résolution de l'équation indéterminée

$$ax + \alpha = by + \beta,$$

laquelle est, comme on sait, toujours possible quand a et b

(*) Ce symbole est le φ de M. Gauss (Disq., § 38).

sont premiers entre eux. De plus, si on trouve un nombre remplissant les deux conditions, si on en retranche le plus grand multiple de ab qui y est contenu, le reste plus petit que ab, les remplira encore. Ainsi on voit qu'il existe un nombre $z < ab$ et à la fois $\dot{a}+\alpha$ et $\dot{b}+\beta$.

Je dis maintenant qu'il n'en existe qu'un, car s'il y en avait un autre z' on aurait :

$$z-z' = \dot{a} = \dot{b} = (\dot{ab}).$$

ce qui est impossible puisque $z - z'$ est $< ab$. Donc, etc.

3. Lemme II. *L'indicateur du produit de plusieurs nombres premiers entre eux deux à deux, est égal au produit des indicateurs de ces nombres* (*).

Démonstration. Soient d'abord deux nombres a et b premiers entre eux. Désignons par

(1) $\qquad \alpha_1, \quad \alpha_2, \quad \alpha_3 \ldots \alpha_{i(a)},$

les nombres inférieurs et premiers à a et par

(2) $\qquad \beta_1, \quad \beta_2, \quad \beta_3 \ldots \beta_{i(b)},$

les nombres inférieurs et premiers à b.

Tout nombre premier avec ab doit, si on le divise par a, donner pour reste un des termes de la suite (1), et si on le divise par b, donner pour reste un des termes de la suite (2). Mais parmi les nombres plus petits que ab, il n'y en a qu'un qui soit à la fois $\dot{a}+\alpha_1$ et $\dot{b}+\beta_1$ un seul à la fois $\dot{a}+\alpha_2$ et $\dot{b}+\beta_2$, etc.

Donc il y aura autant d'entiers inférieurs et premiers à ab que l'on pourra fournir de combinaisons avec les termes des deux suites, en prenant toujours un de la première et un de la seconde, c'est-à-dire $i(a)$, $i(b)$. Donc

$$i(ab) = i(a)\, i(b);$$

si maintenant c désigne un nombre premier avec a et b, ab etant premier avec c, on aura :

(*) Disq., § 38, III.

$$i\,(abc) = i\,(ab)\;\; i\,(c)\,,$$

donc

$$i\,(abc) = i\;(a)\;i\,(b)\;i\,(c).$$

Ainsi le théorème est vrai pour le cas de trois facteurs. On l'étendrait successivement au cas de $4, 5, \ldots . n$ facteurs. Donc il est général.

4. Problème. *Trouver l'indicateur d'un nombre donné N.*

Solution. Supposons d'abord $N = \alpha^m$, α étant un nombre premier. Parmi les α^m nombres

$$1\,,\; 2\,,\; 3\,, \ldots . \alpha^m,$$

il n'y a que les suivants

$$\alpha,\; 2\alpha,\; 3\alpha, \ldots . \alpha^{m-1}.\;\alpha,$$

au nombre de α^{m-1} qui ne soient pas premiers avec α^m. Donc on aura :

$$i\,(\alpha^m) = \alpha^m - \alpha^{m-1},$$

ou bien

$$i\,(\alpha^m) = \alpha^{m-1}\,(\alpha - 1). \qquad (3)$$

Soit maintenant

$$N = \alpha^m\,\beta^n \ldots . \lambda^r$$

$\alpha, \beta, \ldots \lambda$, étant des nombres premiers inégaux, on aura d'après le lemme II :

$$i\,(N) = i\;(\alpha^m)\;i\;(\beta^n)\,i\;(\gamma^p) \ldots .\; i\;(\lambda^r),$$

et d'après la formule (3) :

$$i\,(N) = \alpha^{m-1}\,(\alpha - 1)\beta^{n-1}\,(\beta - 1) \ldots .\; \lambda^{r-1}\,(\lambda - 1);$$

formule qu'on peut encore écrire ainsi :

$$i\,(N) = N\left(1 - \frac{1}{\alpha}\right)\left(1 - \frac{1}{\beta}\right) \ldots . \left(1 - \frac{1}{\lambda}\right). \qquad (*)$$

(*) Voir, tome I, p. 467. La première démonstration de ce théorème est due à Euler (Comm, Petrop. VIII, p. 74). Tm.

11.

5. Problème. *Étant donnés les indicateurs de plusieurs nombres, trouver l'indicateur de leur produit.*

Solution. Soient a et b deux entiers quelconques ; α, α', α'',... les facteurs premiers inégaux communs à a et b ; a_1 et b_1 deux nombres non divisibles par aucun des nombres premiers α, α', α''.... Posons :

$$a = \alpha^m \alpha'^{m'} \alpha''^{m''} \dots a_1$$
$$b = \alpha^n \alpha'^{n'} \alpha''^{n''} \dots b_1$$

on aura, d'après ce qui précède :

$$i\ (a) = \alpha^{m-1}\ (\alpha - 1)\ \alpha'^{m'-1}\ (\alpha' - 1) \dots i\ (a_1)$$
$$i\ (b) = \alpha^{n-1}\ (\alpha - 1)\ \alpha'^{n'-1}\ (\alpha' - 1) \dots i\ (b_1)$$
$$i\ (a)\ i\ (b) = \alpha^{m+n-2}\ (\alpha - 1)^2\ \alpha'^{m'+n'-2}\ (\alpha' - 1)^2 \dots i\ (a_1)\ i\ (b_1)$$
$$i\ (ab) = \alpha^{m+n-1}\ (\alpha - 1)\ \alpha'^{m'+n'-1}\ (\alpha' - 1) \dots i\ (a_1)\ i\ (b_1).$$

Donc

$$i\ (ab) = i\ (a)\ i\ (b)\ \frac{\alpha\alpha'\alpha'' \dots}{(\alpha - 1)\ (\alpha' - 1\ (\alpha'' - 1) \dots},$$

ou bien si on pose $\delta = \alpha\alpha'\alpha'' \dots$ d'où $(\alpha - 1)\ (\alpha' - 1) \dots = i\ (\delta)$. on aura plus simplement :

$$i\ (ab) = i\ (a)\ i\ (b)\ \frac{\delta}{i\ (\delta)}.$$

Soit maintenant un troisième nombre c et δ' le produit des facteurs premiers communs à ab et c. Nous aurons d'après la dernière formule :

$$i\ (abc) = i\ (ab)\ i\ (c)\ \frac{\delta'}{i\ (\delta')},$$

ou bien

$$i\ (abc) = i\ (a)\ i\ (b)\ i\ (c)\ \frac{\delta\delta'}{i\ (\delta)\ i\ (\delta')}.$$

On voit facilement que les facteurs premiers qui divisent a et c sans diviser b, ou b et c sans diviser a, ou a et b sans

diviser c, entrent une seule fois dans le produit $\delta\delta'$, et qu'il en est de même de leurs indicateurs dans le produit $i(\delta)\, i(\delta')$. Quant aux facteurs premiers communs aux trois nombres, et par conséquent à δ, ils doivent entrer à la deuxième puissance $\delta\delta'$, et leurs indicateurs aussi dans $i(\delta)\, i(\delta')$. Donc si on appelle

δ_2 le produit de 2 facteurs premiers communs à deux des nombres a, b, c;

δ_3 le produit des facteurs premiers communs aux trois nombres,

on aura :

$$i(abc) = i(a)\, i(b)\, i(c)\, \frac{\delta_2}{i(\delta_2)} \cdot \frac{\delta_3^2}{i(\delta_3)^2}.$$

En continuant à raisonner de la même manière, on voit que si a, b, $c\ldots$ l sont n nombres entiers quelconques, $\delta_2, \delta_3, \ldots \delta_n$ les produits des facteurs premiers inégaux communs respectivement à 2, 3, ... n des nombres proposés, on aura :

$$i(abc..l) = i(a)\, i(b)\, i(c) \ldots i(b)\, \frac{\delta_2}{i(\delta_2)} \cdot \frac{\delta_3^2}{i(\delta_3)^2}\, \frac{\delta_4^3}{i(\delta_4)^3} \ldots \frac{\delta_n^{n-1}}{i(\delta_n)^{n-1}},$$

formule qui résout le problème proposé.

6. *Corollaire.* Soit $N = A^m$ et a le produit des facteurs premiers inégaux de A. Si on considère A^m comme le produit de facteurs égaux à A, on aura $\delta_m = am$ et la formule générale donnera :

$$i(A^m) = i(A)^m \cdot \frac{a^{m-1}}{i(a)^{m-1}},$$

ou, à cause de $i(A) = \frac{A}{a}\, i(a)$,

$$(A^m) = \frac{A^m\, i(a)}{a}.$$

Quand $a = A$, c est-à-dire lorsque les facteurs premiers de

de A n'y entrent qu'à la première puissance, on a plus simplement

$$i(\mathrm{A}^m) = \mathrm{A}^{m-1} i(\mathrm{A}).$$

III.

7. Théorème. *La somme des indicateurs de tous les diviseurs d'un nombre est égale à ce nombre* (*).

Démonstration. Soit

$$\mathrm{N} = \alpha^m \beta^n \gamma^p \ldots \lambda^r$$

un entier décomposé en ses facteurs premiers. Tout diviseur de N sera de la forme

$$d = \alpha^x \beta^y \gamma^z \ldots \lambda^v,$$

d'où

$$i(d) = \alpha^{x-1}(\alpha-1)\,\beta^{y-1}(\beta-1)\,\gamma^{z-2}(\gamma-1)\ldots\lambda^{v-1}(\lambda-1).$$

Pour avoir les indicateurs de tous les diviseurs de N, il faudra faire varier dans cette expression x de 0 à m, y de 0 à n, etc. En ayant soin de supprimer le facteur $(\alpha-1)$ quand $x=0$; le facteur $(\beta-1)$ quand $y=0$, etc. Or un peu d'attention suffit pour faire voir que tous ces indicateurs seront les différents termes du produit

$$[(1+(\alpha-1)+\alpha(\alpha-1)+\alpha^2(\alpha-1)+\ldots+\alpha^{m-1}(\alpha-1)]\times$$
$$[(1+(\beta-1)+\beta(\beta-1)+\beta^2(\beta-1)+\ldots+\beta^{n-1}(\beta-1)\ldots]$$
$$[\ldots(1+(\lambda-1)+\lambda(\lambda-1)+\lambda^2(\lambda-1)+\ldots+\lambda^{r-1}(\lambda-1)].$$

Mais le premier facteur de ce produit $=\alpha^m$, le second $=\beta^n$,.... le dernier égale λ^r. Donc

$$\Sigma i(d) = \alpha^m \beta^n \ldots \lambda^r = \mathrm{N},$$

C. Q. F. D.

IV.

8. Voici encore quelques théorèmes dans lesquels l'indicateur joue un rôle important.

(*) Disq., § 39. Tm

Deux nombres a *et* p *étant premiers entre eux, on a toujours* $a^{i(p)} - 1 = \dot{p}$. On en déduit comme corollaire ce célèbre théorème de Fermat : *si* p *est premier* $a^{n-1} - 1 = \dot{p}$.

Si p *est un nombre premier et* n *un diviseur de* p^{m-1} (p—1) *ou de* $i(p^m)^2$, *on trouvera toujours* i (n) *nombres inférieurs à* p^m, *dont les puissances divisées par* p^m *donnent* n *résidus différents.*

Nous nous proposons de revenir sur ce dernier théorème dans un prochain article, qui aura pour objet l'étude des périodes de résidus, obtenus en divisant les puissances d'un nombre a par un nombre p premier avec a.