PROBLÈMES ET THÉORÈMES D'ARITHMÉTIQUE

Par M. E. **Catalan** (*).

1. — **Problème I.** — *De* 1 *à* n (inclusivement), *combien y a-t-il de nombres non divisibles par des nombres premiers donnés*, β, γ, ... π?

Soit N le nombre cherché. On sait (**) que

$$N = n - \sum\left(\frac{n}{\beta}\right) + \sum\left(\frac{n}{\beta\gamma}\right) - \sum\left(\frac{n}{\beta\gamma\delta}\right) + \ldots \quad (1)$$

Dans cette formule, le symbole $\left(\frac{n}{a}\right)$ représente *le plus grand nombre entier contenu dans* $\frac{n}{a}$ (***).

2. — **Théorème I.** — *Soit* n *un nombre entier, compris entre* 2^k *et* $2^{k+1} - 1$ (inclusivement) ; *soient* β, γ, δ, ... *les nombres premiers supérieurs à* 2. *On a*

$$n - \sum\left(\frac{n}{\beta}\right) + \sum\left(\frac{n}{\beta\gamma}\right) - \sum\left(\frac{n}{\beta\gamma\delta}\right) + \ldots = k + 1 \quad (2) \text{(****)}$$

Dans la suite $1, 2, 3, \ldots n$,

les seuls nombres premiers avec

$$\beta = 3, \gamma = 5, \delta = 7, \ldots$$

sont $1, 2, 2^2, 2^3, \ldots 2^k$.

Ainsi, $N = k + 1$.

3. — Remarque. — De $n = 4$ à $n = 14$, le premier membre se réduit à $n - \sum\left(\frac{n}{\beta}\right)$;

(*) *Extrait des Mémoires de la Société royale des sciences de Liège.*

(**) *Mélanges mathématiques*, p. 133. — *Journal de Mathématiques élémentaires et spéciales*, 1881, p. 296, etc.

(***) Il a la même signification que celui de Legendre : $E\left(\frac{n}{a}\right)$.

(****) L'égalité (2), à peu près évidente, est une simple variante de celle-ci :

$$n - \sum\left(\frac{n}{\alpha}\right) + \sum\left(\frac{n}{\alpha\beta}\right) - \sum\left(\frac{n}{\alpha\beta\gamma}\right) + \ldots = 1,$$

qu'on trouve à la page 134 des *Mélanges*.

De $n = 15$ à $n = 104$ (*), ce premier membre se réduit à

$$n - \sum\left(\frac{n}{\beta}\right) + \sum\left(\frac{n}{\beta\gamma}\right);$$

et ainsi de suite.

4.—Problème II.— *Connaissant les nombres premiers qui ne surpassent pas* n, *trouver combien il y a de nombres premiers compris entre* n + 1 *et* 2n.

Soit π le plus grand nombre premier, non supérieur à n. De 1 à $2n$, les nombres non divisibles par

$$\beta = 3, \quad \gamma = 5, \quad \delta = 7, \ \ldots \ \pi,$$

sont, d'une part, $1, 2, 2^2, \ \ldots \ 2^{k+1}$;

et, en second lieu, les nombres premiers compris entre $n + 1$ et $2n$. Soit x la *quotité* (**) de ceux-ci. Nous avons, en vertu de l'égalité (2),

$$k + 2 + x = 2n \sum\left(\frac{2n}{\beta}\right) + \sum\left(\frac{2n}{\beta\gamma}\right) - \sum\left(\frac{2n}{\beta\gamma\delta}\right) + \ldots \quad (3)$$

5. — Application. — *Entre* 25 *et* 50, *combien y a-t-il de nombres premiers?*

Dans cet exemple,

$$n = 25, \ 2n = 50, \ k = 4.$$

En outre, les diviseurs *simples* sont :

$$3, 5, 7, 11, 13, 17, 19, 23;$$

et les diviseurs *composés:*

$$15, 21, 33, 39, 35.$$

Par conséquent,

$$6 + x = 50 - [16 + 10 + 7 + 4 + 3 + 2 + 2 + 2] + [3 + 2 + 1 + 1 + 1];$$

d'où $x = 6$.

En effet, entre 25 et 50, il y a *six* nombres premiers ; savoir:

$$29, 31, 37, 41, 43, 47.$$

6.—Remarque. —La combinaison des égalités (2), (3) donne celle-ci :

(*) $15 = 3.5, \ 104 = 3.5.7 - 1.$

(**) J'emploie ce mot pour éviter : *nombre des nombres.*

$$k-x=\sum\left[\left(\frac{2n}{\beta}\right)-2\left(\frac{n}{\beta}\right)\right]-\sum\left[\left(\frac{2n}{\beta\gamma}\right)-2\left(\frac{n}{\beta\gamma}\right)\right]+\sum\left[\left(\frac{2n}{\beta\gamma\delta}\right)-2\left(\frac{n}{\beta\gamma\delta}\right)\right]-\ldots \quad (4)$$

Pour simplifier le second membre, on peut s'appuyer sur la proposition suivante.

7.—Lemme—*Selon que* $\left(\frac{2n}{a}\right)$ *est* pair *ou* impair,

$$\left(\frac{2n}{a}\right)-2\left(\frac{n}{a}\right)$$

égale zéro ou un.

1° De $$2n=a.2\mu+r$$

on déduit $$n=a\mu+\frac{r}{2}.$$

Donc, à cause de $r<a$, μ *est le quotient entier de* n *par* a (*). Autrement dit :

$$\left(\frac{2n}{a}\right)=2\mu=2\left(\frac{2n}{a}\right),\quad \left(\frac{n}{a}\right)-2\left(\frac{n}{a}\right)=0.$$

2° Soit $$2n=a(2\mu+1)+r;$$

et, par conséquent $$n=a\mu+\frac{a+r}{2}.$$

De $r<a$, on conclut $\frac{a+r}{2}<a$: μ *est le quotient entier de* n *par* a. Nous avons donc, simultanément,

$$\left(\frac{2n}{a}\right)=2\mu+1,\left(\frac{n}{a}\right)=\mu,\quad \left(\frac{2n}{a}\right)-2\left(\frac{n}{a}\right)=1.$$

8. — Revenons à la formule (4). En vertu du lemme; *chacun des binômes* soumis au signe Σ *égale* 0 *ou* 1, *selon que son premier terme est pair ou impair.*

D'après cela, si l'on appelle :

l_1, *le nombre de ceux des quotients* $\left(\frac{2n}{\beta}\right)$, *qui sont impairs*;

l_2, *le nombre de ceux des quotients* $\left(\frac{2n}{\beta\gamma}\right)$, *qui sont impairs*;

. . . . . .

l'égalité (4) peut être énoncée ainsi:

(*) Ce petit théorème se trouve dans tous les Traités d'arithmétique.

Théorème II. — *En conservant les hypothèses et les dénominations précédentes, on a*

$$x = k - l_1 + l_2 - l_3 + \dots \qquad (A)$$

9. — Application. — *Entre* 25 *et* 50, *combien y-a-t-il de nombres premiers?*

Je divise 50

par 3, 5, 7, 11, 13, 17, 19, 23;

\+ \+

puis par 15, 21, 33, 39, 35,

\+ \+ \+ \+

en négligeant les quotients pairs.

Je trouve $l_1 = 2$, $l_2 = 4$; donc

$$x = 4 - 2 + 4 = 6;$$

comme ci-dessus.

10. — Autre application. — *De* 61 *à* 120, *combien y-a-t-il de nombres premiers?*

$$n = 60, \quad k = 5.$$

Dividende : 120

Premiers diviseurs :

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37,

\+ \+ \+ \+ \+ \+

41, 43, 47, 53, 59 $l_1 = 6.$

Deuxièmes diviseurs :

15, 21, 33, 39, 51, 57, 69, 87, 93, 111, 35,

\+ \+ \+ \+ \+ \+ \+ \+ \+

55, 65, 85, 95, 115, 77, 91, 119

\+ \+ \+ \+ \+ \+ \+ \+ $l_2 = 15.$

Troisièmes diviseurs : 105

\+ $l_3 = 1.$

$$x = 5 - 6 + 16 - 1 = 13.$$

Les *treize* nombres premiers compris entre 61 et 120 (inclusivement) sont

61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113.

11. — Remarque. — Si l'on admet qu'*entre* $n + 1$ *et* $2n$,

il y a, au moins, un nombre premier (*), l'égalité (A) donne

$$k - l_1 + l_2 - l_3 + \cdots \geqq 1. \qquad \text{(B)}$$

Inversement, si l'on pouvait, *a priori*, établir la relation (B), le *postulatum* serait démontré (**).

12. — Théorème III. — n *étant toujours un nombre entier, compris entre* 2^k *et* $2^{k+1} - 1$, *soient* β, γ, δ, ... *les nombres premiers, supérieurs à* 2. *Soient, en outre:*

λ_1 *le nombre de ceux des quotients* $\left(\frac{2n}{\beta}\right)$, *qui sont impairs;*

λ_2 *le nombre de ceux des quotients* $\left(\frac{2n}{\beta\gamma}\right)$, *qui sont impairs;*

. . . . . .

On a $\lambda_1 - \lambda_2 + \lambda_3 - \cdots = k.$ (C)

Ce théorème, conséquence des égalités

$$n - \sum\left(\frac{n}{\beta}\right) + \sum\left(\frac{n}{\beta\gamma}\right) - \cdots = k + 1 \qquad (2)$$

$$2n - \sum\left(\frac{2n}{\beta}\right) + \sum\left(\frac{2n}{\beta\gamma}\right) - \cdots = k + 3, \quad (2')(***)$$

résulte aussi du théorème II.

Soient, en effet, ρ, σ, θ, ... ω les x nombres premiers, compris entre $n + 1$ et $2n$.

Chacun des quotients $\left(\frac{2n}{\rho}\right)$, $\left(\frac{2n}{\sigma}\right)$, $\left(\frac{2n}{\theta}\right)$, ... égale 1; et chacun des quotients $\left(\frac{2n}{\beta\rho}\right)$, $\left(\frac{2n}{\rho\sigma}\right)$, ... *est nul* (****). Donc

$$\lambda_1 = l_1 + x, \quad \lambda_2 = l_2, \quad \lambda_3 = l_3, \ldots$$

Par suite, l'égalité (A) devient

$$x = k - (\lambda_1 - x) + \lambda_2 - \lambda_3 + \ldots,$$

ou

$$\lambda_1 - \lambda_2 + \lambda_3 - \ldots = k. \qquad \text{(C)}$$

13. — Application. — $n = 25$, $k = 4$.

Dividende : 50.

(*) Cette proposition ne diffère pas, au fond, du *postulatum* de M. Bertrand, démontré par M. Tchebychev (*Journal de Liouville*, t. XVII, p. 381).

(**) *Nouvelle Correspondance mathématique*, t. VI, p. 263.

(***) Voyez les paragraphes 6 et 8

(****) A cause de $\beta > 2, \rho > n$.

Premiers diviseurs :

3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

\+ + + + + + + $\lambda_1 = 8.$

Deuxièmes diviseurs :

15, 21, 33, 39, 35.

\+ + + + $\lambda_2 = 4$

$8 - 4 = 4.$

14. — Remarque. — La fonction qui constitue le premier membre de l'égalité (C) dépend, *uniquement*, de n : appelons-la F (n). *Cette fonction conserve la même valeur quand* n *varie entre* 2^k *et* $2^{k+1} - 1$ (inclusivement). En outre, *chaque fois que* n *dépasse une nouvelle puissance de* 2, F (n) *augmente d'une unité.* Cet exemple de discontinuité, analogue à celui que présente la fonction E(x), nous paraît remarquable.

15. — *Sur une équation indéterminée.* L'identité

$$(\alpha+\beta)^2(\alpha-2\beta)^2(\beta-2\alpha)^2+27\alpha^2\beta^2(\alpha-\beta)^2=4(\alpha^2-\alpha\beta+\beta^2)^3, \quad (D)$$

facile à vérifier, donne une infinité de solutions, en nombres entiers, de

$$x^2 + 3y^2 = z^3. \quad (5)$$

En effet, on peut prendre

$$x=\frac{1}{2}(\alpha+\beta)(\alpha-2\beta)(\beta-2\alpha), \quad y=\frac{3}{2}\alpha\beta(\alpha-\beta),$$

$$z = \alpha^2 - \alpha\beta + \beta^2. \quad (6)$$

Ces valeurs seront entières, si α, β sont de *même parité.*

16. — Remarque. — Ces formules ne donnent pas toutes les solutions. Par exemple, on n'en saurait déduire

$$x = y = z = 4.$$

17. — *Autres identités.*

$$(a^2 + b^2)^4 = (a^4 - 6a^2b^2 + b^4)^2 + [4(a^2 - b^2)ab]^2$$

$$= (a^4 + b^4)^3 + (2a^3b)^2 + (2a^2b^2)^2 + (2ab^3)^2. \quad (E)$$

Ainsi, $(a^2 + b^2)^4$ *est : un carré ; une somme de deux carrés ; une somme de quatre carrés.* Généralement, ce nombre n'est pas la somme de trois carrés.

M. Realis, à qui j'avais communiqué les identités (D), (E), m'a répondu par l'intéressante note suivante :

I. La résolution de l'équation

$$x^2 + 3y^2 = z^3$$

en nombre entiers se rattache directement à la théorie générale développée par Lagrange dans le § IX des *Additions à l'Analyse indéterminée d'Euler*.

Le nombre z, diviseur du premier membre, ne peut être que de la forme $\alpha^2 + 3\beta^2$; on a donc l'identité

$$\alpha^2(\alpha^3 - 9\beta^2)^2 + 3\beta^2(3\alpha^2 - 3\beta^2)^2 = (\alpha^2 + 3\beta^2)^2.$$

Quant à l'égalité $4^2 + 3.4^2 = 4^3$, où 4^2 est facteur commun à tous les termes, elle ne conduit pas à une solution: car en écrivant, comme on doit le faire, $1^2 + 3.1^2 = 4.1^3$, on n'a pas un cube dans le second membre.

Quant, enfin, à l'identité

$$(\alpha + \beta)^2(\alpha - 2\beta)^2(\beta - 2\alpha)^3 + 27\alpha^2\beta^2(\alpha - \beta)^2 = 4(\alpha^2 - \alpha\beta + \beta^2)^3,$$

rapportée par M. Catalan, elle n'est manifestement qu'une transformée de celle qui précède.

II. L'expression $(a^2 + b^2)^4$ est assurément: un carré, — une somme de deux carrés, — une somme de quatre carrés. On ne peut pas affirmer qu'elle est généralement une somme de trois carrés effectifs, puisque $(1^2 + 1^2)^4 = 16$, par exemple, ne l'est pas. Cependant, pour des nombres a, b premiers entre eux (ou simplement inégaux), on peut mettre en évidence, par des formules, que l'expression considérée est toujours une somme de trois carrés.

1° Si a et b sont premiers avec 3, posons l'identité

$$a^2 + (a + 3h)^2 = (a + h)^2 + (a + 2h)^2 + (2h)^2, \quad (*)$$

dans laquelle on prendra a premier avec h; il s'en déduit, par l'emploi répété de la formule connue

$$(\alpha^2 + \beta^2 + \gamma^2)^2 = (\alpha^2 + \beta^2 - \gamma^2)^2 + (2\alpha\gamma)^2 + (2\beta\gamma)^2,$$

le théorème général exprimé par la relation

$$[a^2 + (a + 3h)^2]^m = A^2 + B^2 + C^2,$$

où A, B, C sont des entiers dont aucun n'est nul, et m est une puissance de 2.

Il s'ensuit, comme corollaire, que: a et b étant deux entiers, dont un seul divisible par 3, et m désignant une puissance de 2, l'expression $[2(a^2 + b^2)]^m$ est la somme de trois carrés.

(*) Lettre de M. Catalan à D. B. Boncompagni, en date de « Liège, 15 décembre 1880 ».

2° Si l'un des nombres a, b, premiers entre eux, est un multiple de 3, par exemple, $a = 3a'$, on pose l'identité $(9a'^2 + b^2)^2 = (7a'^2 - b^2)^2 + 16a'^2(a' + b)^2 + 16a'^2(a' - b)^2$, et l'on en déduit, comme ci-dessus, la relation

$$(9a'^2 + b^2)^m = A^2 + B^2 + C^2,$$

en nombres entiers, m étant une puissance de 2.

Observation. — Tout ce qui précède est entièrement indépendant de la *Théorie des nombres* proprement dite; on n'y fait usage que de formules directes, exprimant les propositions, et indiquant en même temps les calculs à effectuer. Mais si l'on sort des éléments, et que l'on s'appuie sur les théorèmes de l'arithmétique supérieure, toutes les propositions énoncées, et bien d'autres, se présentent comme des conséquences immédiates de ce principe, que : *tout bicarré impair, autre que l'unité, est la somme de trois carrés.* D'après ce principe (qui ne se démontre pas à l'aide de simples identités algébriques), *un nombre de la forme* $(a^2 + b^2)^4$ *est toujours décomposable en trois carrés, s'il ne se réduit pas à une puissance de* 2.

SOLUTION DES PROBLÈMES

DONNÉS AU CONCOURS DE L'ÉCOLE SAINT-CYR (1882)

Étant donnés un cercle de rayon r, *et un point* A *dans son plan, à une distance* d *du centre, on suppose menée par le point* A *une sécante telle que la somme des carrés des segments compris entre ce point et les points d'intersection avec la circonférence soit égale à un carré donné* m^2. *Démontrer que, si* α *désigne l'angle que la sécante fait avec le diamètre passant par le point* A, *on aura la formule*

$$\cos 2\alpha = \frac{m^2 - 2r^2}{2d^2} : \qquad (1)$$

Discussion. — *Limites de* m, *quand on fait varier* α, *le point* A *étant à l'intérieur du cercle.*

Les valeurs des segments AB et AC sont les racines de l'équation $r^2 = d^2 + x^2 - 2dx \cos \alpha$