Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 9 (1907)
Heft: 1: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LE LEMME FONDAMENTAL DE LA THÉORIE DES NOMBRES
Autor: Aubry, A.
DOI: https://doi.org/10.5169/seals-10154

dans la résolution d'une équation du deuxième degré citée plus haut, qu'en divisant 19350 par 407 on obtient $x_2 = 40$, et 2) par le compte rendu de Maximilien Marie sur l'ouvrage de Viète, consacré au sujet considéré, qu'il envisage comme « un essai infructeux de résolution des équations de tous les degrés à coefficients numériques [1]. »

(Traduction de M. V. Frédéricksz, Genève.)

V. Bobynin (Moscou).

LE LEMME FONDAMENTAL DE LA THÉORIE DES NOMBRES

Avant-Propos. — Historiquement, la théorie des nombres tire son origine des spéculations des Anciens sur les identités géométriques ou algébriques, les proportions, les progressions, les combinaisons, les nombres polygones, figurés, parfaits, les carrés magiques, les problèmes indéterminés et surtout les triangles rectangles en nombres entiers; mais la voie la plus naturelle qui y conduit est sans contredit, l'idée de congruence, énoncée explicitement, pour la première fois par Gauss. Plus immédiatement, on peut établir cette théorie en partant, par exemple, de l'analyse indéterminée, du théorème de Fermat, de la théorie des résidus, de la loi de réciprocité, de la formule de Moivre, ou encore d'un théorème démontré par Euler, page 75 du tome VIII des *Novi Comm. Petr* [2].

Ce dernier moyen paraît le plus propre à pénétrer rapidement dans le sujet, car il en fait comprendre d'un seul coup

[1] Maximilien Marie. *Histoire des Sciences mathématiques et physiques*, III, p. 61.

[2] « Si per numerum quemcunque n termini progressionis arithmeticæ cujuscunque, cujus differentia sit numerus ad n primus, dividantur, inter residua occurrent omnes numeri divisore n minores ».

l'esprit et la méthode ; d'ailleurs il y est employé à chaque instant,

Pour ces deux raisons, il semble que ce serait chose utile qu'une monographie de ce théorème et de ses nombreuses conséquences, presque toutes origines directes des diverses divisions de la théorie des nombres. Tel est le programme du présent article, le second de ceux que nous avons annoncés, page 25[1].

1. — La relation que présentent deux entiers a, A, ne différant que d'un multiple de b, s'écrit $a \equiv \mathrm{A} \pmod{b}$ et s'énonce a *congru* à A, *suivant le module* b.

Si on a :

$$a \equiv \mathrm{A}\,,\ a' \equiv \mathrm{A}'\,,\ a'' \equiv \mathrm{A}'''\,,\ \ldots \qquad (\mathrm{mod.}\ b)$$

on aura aussi :

$$aa' \ldots \equiv \mathrm{AA}' \ldots\,,\quad ka \equiv k\mathrm{A}\,,\quad ka + la' + \ldots \equiv k\mathrm{A} + l\mathrm{A}' + \ldots\,,$$
$$a^n \equiv \mathrm{A}^n \qquad (\mathrm{mod.}\ b)$$

De plus, si le nombre k divise a et A et qu'en outre il soit premier avec b,

$$\frac{a}{k} \equiv \frac{\mathrm{A}}{k}\,. \qquad (\mathrm{mod.}\ b)$$

2. — *Les entiers* a *et* b *étant premiers entre eux, si on divise par* b *les* (b — 1) *premiers multiples de* a, *les restes seront, dans un certain ordre les* (b — 1) *premiers entiers*. (Euler, 1759). Aucun reste n'est nul, et il ne peut y en avoir deux qui soient égaux, car, autrement on aurait, par exemple,

$$\alpha a \equiv r \quad \text{et} \quad \beta a \equiv r \quad \text{d'où} \quad (\alpha - \beta)\, a \equiv 0 \qquad (\mathrm{mod.}\ b)$$

ce qui est impossible, puisque a est premier avec b et que, $\alpha - \beta$ étant $< b$, l'expression $(\alpha - \beta)\, a$ ne peut représenter un multiple de b.

Cor. I. Si a et b sont premiers entre eux, on peut toujours trouver, au-dessous de b, un nombre x qui satisfasse à la congruence $ax \equiv c \pmod{b}$, ou, si l'on veut, à la relation $ax - by = c$.

---

[1] Dans le premier article, prière de rectifier ainsi le commencement du n° 3, page 26 :

3. — Posons $\rho^2 \equiv r$, il viendra $\rho^{\mu-1} \equiv r^m \equiv 1$: on a donc, etc.

Si a et b ne sont pas premiers entre eux et que θ soit leur p. g. c. d., $\frac{a}{\theta}$ et $\frac{b}{\theta}$ seront premiers entre eux et on pourra écrire $ax - by = c\theta$.

On remarquera que si x satisfait à la congruence $ax \equiv c$ (mod. b), tous les nombres congrus à x, c'est-à-dire compris dans la formule $kb + x$, y satisferont également, et il n'y aura que ceux-là.

Cor. II. Si $(kb + a)(lb + x) = mb + c$, x a toujours une valeur unique $< b$. Ainsi tout nombre qui, multiplié par $8 + 5$[1], donne un produit $8 + 7$, est de la forme $8 + 3$, puisque $3.5 = 8 + 7$.

Si a et αa sont tous deux $\equiv 1$ (mod. b), il en est de même de α.

Cor. III. Supposons b impair : les restes de la division par b des nombres a, $2a$, $3a$, ... $\frac{b-1}{2}\,a$ sont tous différents et de plus la somme de deux restes quelconques ne peut être égale à b. (Gauss).

Cor. IV. Soit a l'un des nombres $1, \alpha, \alpha', \alpha'', \ldots b - 1$, lesquels sont inférieurs à b et premiers avec lui : la division des nombres a, $a\alpha$, $a\alpha'$, ... $a(b - 1)$ par b, donnera comme restes les mêmes nombres $1, \alpha, \alpha', \ldots$ (Gauss).

Cor. V. Nombres associés. Appelons *associés relativement* à b, deux nombres dont le produit est $\equiv 1$ (mod. b) : un nombre quelconque, premier avec b, a son associé (Euler 1772).

En particulier, si b est un nombre premier p, tout entier inférieur à p a son *associé*. En outre les nombres 1 et $p - 1$ sont les seuls à être leurs propres associés, car, de $x^2 \equiv 1$[2], on tire $(x + 1)(x - 1) \equiv 0$.

On verra de même : 1° que 2 et $\frac{p+1}{2}$ sont associés, de même que $\frac{p-1}{2}$ et $p - 2$; 2° que les compléments à p de deux associés sont eux-mêmes associés.

Cor. VI. Si n divise $a^2 \pm kb^2$, a et b étant premiers entre eux, il divise aussi un certain nombre de la forme $x \pm k$.

[1] Nous entendons par là un multiple de 8 augmenté de 5.

[2] Quand le module est le nombre premier indéterminé p, on se dispense d'écrire la mention (mod. p).

(Euler 1748). Démonstration de Lagrange (1769). On peut écrire $a \equiv bx \pmod{n}$, d'où

$$0 \equiv a^2 \pm kb^2 \equiv b^2x^2 \pm kb^2 = b^2(x^2 \pm k) . \qquad \pmod{n}$$

En particulier, si le nombre premier p divise $a^2 \pm kb^2$, il divise aussi $x^2 \pm k$ [1].

Cor. VII. Les nombres a et b étant premiers entre eux, tout diviseur de $a^2 + kb^2$ est de la forme $Lb^2 + Mbx + Nx^2$ et on a en outre $4LN - M^2 = 4k$ (Lagrange 1775)[2].

Soit n un diviseur de $a^2 + kb^2$; on peut écrire $a = bv + nx$, ce qui donne

$$a^2 + kb^2 = (v^2 + k)\, b^2 + 2vnbx + n^2x^2 ,$$

ce qui montre que n divise $v^2 + k$, puisque n et b sont premiers entre eux.

Remarques. Formes réduites. On donnera ainsi qu'il suit une forme plus précise au diviseur. Si, en valeur absolue, $M > L$ ou $> N$, la formule $Lb^2 + Mbx + Nx^2$ peut se changer en $L'b'^2 + M'b'x' + N'x'^2$, avec les relations

$$4L'N' - M'^2 = 4k \quad \text{et} \quad M' < N , \; L' \geqq L , \; N' \geqq N .$$

Faisons en effet $b = b' - mx'$, $x = x'$; la transformée s'obtiendra en posant :

$$L' = L , \; M' = M - 2Lm , \; N' = Lm^2 - Mm + N ,$$

d'où

$$(\alpha) \qquad 4L'N' - M'^2 = 4LN - M^2 .$$

Or on peut prendre m tel que, en valeur absolue, on ait $M' < L' = L < M$ et de là, à cause de (α), $L'N' > LN$ ou $N' > N$.

Si $M' > N'$ on opérera de même et on obtiendra une autre transformée du diviseur, laquelle donnera $4L''N'' - M''^2 = 4k$, $N'' = N'$, $M'' < M'$. $L'' > L'$; et ainsi de suite.

---

[1] On dit souvent que p *divise* $Ax^2 + Bx + C$, pour signaler qu'il existe un entier x, qui rend la valeur de l'expression $Ax^2 + Bx + C$ divisible par p.

[2] Le théorème de Lagrange est plus général : il traite l'expression $Aa^2 + Bab + Cb^2$, au lieu de $a^2 + kb^2$; mais il suffit de considérer cette dernière, car la précédente s'y ramène immédiatement, puisqu'on peut l'écrire ainsi

$$\frac{(2Aa + Bb)^2 + (4AC - B^2)b^2}{4A} .$$

Puisque les nombres M, M′, M″, ... décroissent de plus en plus, que L, L′, ... et N, N′, ... ne croissent pas, on arrivera à une expression de la forme suivante

$$Py^2 + \Phi yz + Rz^2 ,$$

pour le diviseur de $a^2 + kb^2$. Dans cette expression, appelée par Gauss, la *forme réduite*[1], y et z sont premiers entre eux, $\Phi \leq P$, $\Phi \leq R$ et de plus

$$(\beta) \qquad 4PR - \Phi^2 = 4k .$$

Si $k > 0$, 4PR est positif et comme $P \geq \Phi$, $R \geq \Phi$, on aura :

$$4PR \geq 4\Phi^2 , \quad \text{d'où} \quad \Phi \leq 2\sqrt{\frac{k}{3}} .$$

Si $k < 0$, on aura :

$$\Phi^2 - 4PR > 0 , \quad \text{d'où} \quad \Phi \leq 2\sqrt{\frac{-k}{5}} .$$

Φ est pair d'après (β) ; on prendra Φ d'après les limites indiquées et pour P et R, les facteurs de $\frac{\Phi^2 + k}{4}$, en rejetant ceux qui seraient $< \Phi$.

Le nombre des diviseurs est visiblement fini.

Diviseurs quadratiques. — 1° soit $k = 1$; on aura $\Phi \leq 2\sqrt{\frac{1}{3}}$; donc $\Phi = 0$ et d'après (β), $PR = 1$, d'où $P = 1$, $R = 1$. Ainsi *les diviseurs de* $a^2 + b^2$ *sont de la forme* $y^2 + z^2$ (Fermat).

2° Soit $k = 2$; il viendra $\Phi \leq 2\sqrt{\frac{2}{3}}$, d'où $\Phi = 0$, $PR = 2$, $PR = 1$, $R = 2$. Ainsi *les diviseurs de* $a^2 + 2b^2$ *sont de la même forme* (Euler).

3° Soit $k = 3$; il viendra $\Phi \leq 2$; Φ peut prendre les valeurs 0 ou 2. La première donne $PR = 3$, d'où $P = 1$, $R = 3$. La seconde, $PR = 4$, d'où $P = R = 2$. Ainsi *les diviseurs impairs de* $a^2 + 3b^2$ *sont de la même forme* (Euler).

---

[1] Gauss y arrive par certaines transformations qui en rendent l'étude théorique plus accessible, mais il suffit pour notre objet de montrer l'existence de la forme réduite.

4° Soit enfin $k = -2$; on aura $\Phi \leq 2\sqrt{\frac{2}{5}}$; donc $\Phi = 0$, PR = 2, P = 1, R = 2 ; ou bien P = 2, R = 1.

Les diviseurs sont ainsi de l'une des formes $y^2 - 2z^2$ ou $2y^2 - z^2$, lesquelles n'en font qu'une, car on a

$$y^2 - 2z^2 = 2(y - z)^2 - (y - 2z)^2 .$$

Ainsi *les diviseurs de* $a^2 - 2b^2$ *sont de la même forme* (Euler).

Legendre a donné la table des diviseurs quadratiques jusqu'à $k = \pm 103$. Pour s'exercer, on pourra vérifier que les facteurs de $a^2 + 13b^2$ sont de l'une des formes

$$y^2 + 13z^2 , \quad 2y^2 + 2yz + 7z^2 .$$

Diviseurs linéaires. Reportons nous aux quatre applications qui précédent et considérons seulement les diviseurs impairs.

1° y et z étant premiers entre eux et $y^2 + z^2$ un diviseur impair, on a, par exemple, y pair et z impair. Il suit de là que *les diviseurs impairs de* $a^2 + b^2$ *sont de la forme* $4 + 1$ (Fermat).

2° $y^2 + 2z^2$ ne peut représenter un impair que si y est impair. Selon que z sera pair ou impair, on aura $y^2 + 2z^2 = 8 + 1$ ou $8 + 3$: telles sont les formes des diviseurs de $a^2 + 2b^2$ (Fermat).

3° L'un des nombres y, z est pair, l'autre impair : autrement $y^2 + 3z^2$ serait pair. D'ailleurs y ne peut être un multiple de 3 car $y^2 + 3z^2$ le serait aussi. Supposons y pair, il sera de la forme 6 ± 2, z sera impair et on aura $y^2 + 3z^2 = 6 + 1$. Soit y impair, ce qui demande qu'il soit de la forme 6 ± 1, z sera pair et on aura $y^2 + 3z^2 = 6 + 1$. Cette dernière forme est donc celle des diviseurs premiers impairs de $a^2 + 3b^2$ (Fermat).

4° On verra de même que tout diviseur impair de $a^2 - 2b^2$ est de l'une des formes $8 + 1$, $8 - 1$ (Fermat).

Diviseurs numériques. Les formules des diviseurs servent principalement dans la recherche des diviseurs des grands nombres. On en saisira l'usage par l'exemple simple suivant.

On a $10273 = 101^2 + 2.6^2 = 89^2 + 3.28^2$. Les diviseurs de ce nombre appartiennent ainsi aux formes $8 + 1$, $8 + 3$, $6 + 1$. La seule forme à essayer est donc $24 + 1$; or les seuls nombres premiers de cette forme inférieurs à $\sqrt{10273}$ sont 73 et 97 : la division par ces deux nombres ne réussissant pas, le nombre 10273 est donc premier.

Formes quadratiques. C'est ici le lieu de donner une idée de la théorie des *formes quadratiques*, c'est-à-dire des expressions de la forme $ax^2 + 2bxy + cy^2$, qu'on représente par la notation (a, b, c). Cette théorie tire son origine des beaux théorèmes dûs à Fermat et démontrés par Euler, qui en a compris l'importance et dégagé les principes. Lagrange l'a définitivement fondée par sa considération des formes réduites ; Legendre l'a ensuite perfectionnée à divers égards ; mais c'est surtout Gauss qui, la reprenant systématiquement, en a fait le chapitre le plus vaste et le plus fécond de la théorie des nombres.

Le but de Gauss était primitivement la représentation des nombres par des formes, mais l'intérêt propre de ces expressions les lui a fait étudier en elles-mêmes et il a été suivi dans cette voie par les plus éminents arithméticiens.

Nous nous contenterons d'indiquer ici quelques notions très élémentaires de cette théorie, dans le but de familiariser avec la terminologie de Gauss, laquelle a souvent effrayé les débutants par le grand nombre des idées et des expressions nouvelles qu'elle a introduites dans la science des nombres.

1° Dans la forme $(a, b, c) = ax^2 + 2bxy + cy^2$, substituons les valeurs

$$x = \alpha x' + \beta y' \quad , \quad y = \gamma x' + \delta y' \; ;$$

il viendra une autre expression de la forme

$$(a', b', c') = a'x'^2 + 2b'x'y' + c'y'^2 \; .$$

On dit que la première forme *renferme* la seconde, et la substitution se figure par la notation $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$. De même dans la seconde forme, effectuons une substitution $\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$, il viendra une troisième forme *renfermée* dans la deuxième. Or la pre-

mière forme peut donner la troisième à l'aide d'une certaine substitution $\begin{pmatrix}\alpha''\beta''\\ \gamma''\delta''\end{pmatrix}$ déterminée par les formules

$$(1)\qquad \alpha'' = \alpha\alpha' + \beta\gamma' \ , \quad \beta'' = \alpha\beta' + \beta\delta' \ , \quad \gamma'' = \gamma\alpha' + \delta\gamma' \ ,$$
$$\delta'' = \gamma\beta' + \delta\delta' \ .$$

et liée aux deux autres par la relation

$$(2)\qquad (\alpha\delta - \beta\gamma)\,(\alpha'\delta' - \beta'\gamma') = \alpha''\delta'' - \beta''\gamma''.$$

2°. Si dans la deuxième forme, les nombres x' et y' sont entiers, les nombres x et y de la première le seront également si l'on a $\alpha\delta - \beta\gamma = \pm 1$; et, dans ce cas, les deux formes sont dites *équivalentes*[1], *proprement* dans le cas du signe + et *improprement* dans le cas du signe —. L'équivalence de ces deux formes se note ainsi $(a, b, c) \backsim (a'b'c')$.

La quantité $ac - b^2$ s'appelle d'après Gauss, le *déterminant* de la forme (a, b, c). Les déterminants de deux formes équivalentes sont égaux ; la réciproque n'est pas vraie en général.

3°. Les lettres x, y, x', y'... représentant des entiers qui peuvent être quelconques, on peut supprimer les accents dans une forme considérée isolément, et ainsi on peut dire que, si deux formes sont équivalentes, tout nombre représentable par l'une l'est également par l'autre.

4°. Si on a $\alpha\delta - \beta\gamma = 1$, la substitution $\begin{pmatrix}\alpha\ \beta\\ \gamma\ \delta\end{pmatrix}$ est très remarquable ; elle est dite *modulaire* et les formes qui s'en déduisent sont dites *de même classe*. Si $\alpha\delta - \beta\gamma = -1$, effectuer la substitution $\begin{pmatrix}\alpha\ \beta\\ \gamma\ \delta\end{pmatrix}$ puis la substitution $\begin{pmatrix}1\ \ 0\\ 0\ -1\end{pmatrix}$ revient à effectuer la substitution unique $\begin{pmatrix}\alpha\ -\beta\\ \gamma\ -\delta\end{pmatrix}$, qui est modulaire.

---

[1] Telles sont les formes (a, b, c) , (c, b, a) , $(c, -b, a)$, $(a, -b. c)$, qui sont respectivement les formes *identique, associée, complémentaire et opposée* à la forme (a, b, c). Elles s'en déduisent par le moyen des substitutions $\begin{pmatrix}1\ 0\\ 0\ 1\end{pmatrix}$, $\begin{pmatrix}0\ 1\\ 1\ 0\end{pmatrix}$, $\begin{pmatrix}0\ -1\\ 1\ \ 0\end{pmatrix}$ et $\begin{pmatrix}1\ \ 0\\ 0\ -1\end{pmatrix}$.

Dedekind a appelé par analogie *nombres équivalents* ceux qui sont compris dans la formule $\frac{\alpha x + \beta}{\gamma x + \delta}$, quand $\alpha\delta - \beta\gamma = \pm 1$. Ils jouent un rôle important dans la résolution des congruences du second degré.

5°. Deux formes réduites, qui ont un même déterminant positif, ne peuvent être de même classe que si elles sont identiques. De là le moyen de reconnaître si deux formes de même déterminant positif sont de même classe.

Si les nombres a, b, c n'ont aucun diviseur commun, et qu'on pose $ac - b^2 = D$, les valeurs déterminées par la relation $t^2 + Du^2 = 1$ donneront toutes les substitutions $\begin{pmatrix} t - bu & -cu \\ au & t + bu \end{pmatrix}$ qui changent la forme (a, b, c) en elle-même. On tire de là le moyen de trouver les substitutions modulaires qui lient deux formes à déterminants positifs et de la même classe.

Les théorèmes analogues dans le cas d'un déterminant négatif sont beaucoup moins simples.

6°. Les problèmes généraux résolus par Gauss et ses continuateurs visent surtout la détermination et le dénombrement des classes des formes de même déterminant, ainsi que différents modes de les grouper.

Cor. VIII. Si $n = a\mu^2 + 2b\mu\nu + c\nu^2$, μ et ν étant premiers entre eux, on peut déterminer un nombre dont le carré divisé par n, donne pour reste $b^2 - ac$[1] (Gauss.) Posons en effet $\mu x - \nu y = 1$, il viendra

$$(3) \quad [x(b\mu + c\nu) + y(a\mu + b\nu)]^2 = n(ay^2 + 2bxy + cx^2) + b^2 - ac .$$

Cor. IX. Une expression de la forme $Ax^n + \ldots + M \equiv 0$ s'appelle une *congruence* du n^e degré et les valeurs de x qui y satisfont et sont inférieures à p en sont les *racines*; les autres nombres plus petits que p en sont les *non-racines*.

n désignant un nombre inférieur à p, la congruence $F(x) = Ax^n + Bx^{n-1} + \ldots + Lx + M \equiv 0$ ne saurait avoir plus de n racines (Lagrange, 1768.) Soit en effet a une racine de $F(x) \equiv 0$; on a :

$$F(a) \equiv 0 , \quad \text{d'où} \quad A(x^n - a^n) + B(x^{n-1} - a^{n-1}) + \ldots + L(x - a) \equiv 0.$$

Le premier membre est divisible par $x - a$, quantité non multiple de p. De là, une transformée, de la forme $Ax^{n-1} + \ldots + L \equiv 0$. Si le nombre b, plus petit que p est une autre

[1] Le nombre $b^2 - ac$ est dit *résidu* de n.

racine, on aura de même $A(x^{n-1} - b^{n-1}) + \ldots \equiv 0$, d'où, en divisant par $x - b$, $Ax^{n-2} + \ldots \equiv 0$, laquelle ne peut avoir qu'une solution.

Certaines congruences ont toutes leurs racines ; certaines, au contraire, n'en ont aucune, comme la suivante, $x^2 - 2x + 4 \equiv 0 \pmod 5$.

On suppose que les coefficients de $F(x)$ ne sont pas tous des multiples de p : autrement on aurait $F(x) \equiv 0$, quel que soit x. Une telle congruence est dite *identique*. Réciproquement, si on a $F(x) \equiv 0$ quel que soit x, les coefficients sont tous des multiples de p.

Remarques. 1° Euler avait esquissé, en 1754, une démonstration de ce théorème, qu'on peut présenter ainsi : Si les $(n + 1)$ premiers entiers étaient racines de $F(x) \equiv 0$, les valeurs correspondantes de $F(x)$ et leurs différences premières, secondes, ... seraient $\equiv 0$. Or la différence n^e est égale à $An!$ quantité incongrue à p. La supposition est donc fausse, et la congruence a des non-racines $\leq n + 1$.

2° Si le premier membre $F(x)$ peut se décomposer en deux facteurs entiers $f(x)$, $\varphi(x)$ de degrés k et $n - k$ et que la congruence $F(x) \equiv 0$ ait n racines, les congruences $f(x) \equiv 0$, $\varphi(x) \equiv 0$ en ont respectivement k et $n - k$ (Lagrange.) En effet chacune ne peut en avoir davantage et elles ne peuvent en avoir moins, car toutes les racines doivent se retrouver dans la congruence $f(x)\,\varphi(x) \equiv 0$.

Euler avait auparavant démontré cette proposition, dans un cas particulier.

Cor. X. Criterium d'Euler. 1° Soit $a^2 \equiv r$, on aura également $(p - a)^2 \equiv r$: la congruence $x^2 \equiv r$ n'a que les deux racines a et $-a$ [1], car on peut l'écrire $(x + r)(x - r) \equiv 0$.

Les $p - 3$ entiers inférieurs à p et différents de a et de $-a$ se partagent en $\frac{p-3}{2}$ groupes de deux nombres dont le produit est $\equiv r$. Comme $a(p - a) \equiv -a^2 \equiv -r$, on a, en multipliant, ces $\frac{p-1}{2}$ groupes et posant $p = 2m + 1$,

$$(4) \qquad (p - 1)! \equiv -r^m .$$

[1] Pour abréger, on écrit souvent $-a$ au lieu de $p - a$.

2° Puisque dans certains cas, la congruence $x^2 \equiv z$ a deux racines, il y a, au-dessous de p, des valeurs ρ, de z, qui ne permettent pas de satisfaire à cette congruence[1]. On peut donc former, avec les $p-1$ premiers entiers, $\frac{p-1}{2}$ groupes de deux nombres dont le produit est $\equiv \rho$, et par suite on peut écrire :

$$(p-1)! \equiv \rho^m . \tag{5}$$

3° La valeur $z = 1$ permet visiblement de satisfaire à la congruence $x^2 \equiv z$: on n'a qu'à faire $x = z = 1$. Donc, puisque le nombre r^m est congru à une constante, on peut écrire

$$r^m \equiv 1^m = 1 , \quad \text{et de là} \quad \rho^m \equiv -r^m \equiv -1 .$$

Ainsi, selon que la valeur de z permet ou ne permet pas de satisfaire à la congruence $x^2 \equiv z$, on a :

$$z^m \equiv \pm 1 .$$

Cette démonstration est due à Lejeune-Dirichlet.

Cor. XI. Représentons par $s_{k,n}$ la somme des n^{es} puissances des k premiers entiers, on a, pour $n < p-1$,

$$s_{p-1,n} \equiv 0 . \tag{6}$$ (Gauss et Libri.)

Démonstration de Poinsot (1845). Ecrivons $ax \equiv b$, d'où $(ax)^n \equiv b^n$; il s'ensuit que, pour $a = 1, 2, 3, \ldots p-1$, les restes de $(ax)^n$ seront, dans un certain ordre, les mêmes que ceux de a^n. On a donc, en comparant les deux séries de résultats et additionnant,

$$(x^n - 1)\, s_{p-1,n} \equiv 0 .$$

Prenons pour x une des non-racines de $x^n - 1 \equiv 0$, il viendra la relation annoncée.

Autre démonstration. L'expression $(x+1)^n - x^n$ est la somme des n termes

$$(x+1)^{n-1},\ (x+1)^{n-2}\, x ,\ (x+1)^{n-3}\, x^2 ,\ \ldots\ x^{n-1} ,$$

[1] Les valeurs de z sont appelées *résidus* ou *non-résidus* de p, selon qu'elles permettent ou non la réalisation de la congruence $x^2 \equiv z$.

et par suite, elle comprend visiblement n fois le terme x^{n-1}, plus des termes en x^{n-2}, x^{n-3}, ... On a donc :

$$(x+1)^n - x^n = nx^{n-1} + Ax^{n-2} + Bx^{n-3} + \dots Lx + 1 ,$$

A, B, ... désignant des coefficients indépendants de x. Changeant successivement x en 1, 2, 3, ... $a-1$ et additionnant, il viendra :

$$a^n = ns_{a-1,\,n-1} + As_{a-1,\,n-2} + \dots + Ls_{a-1,1} + a ;$$

de sorte que si $s_{a-1,\,n-2}$, $s_{a-1,\,n-3}$, ... sont des multiples de a et que n ne le soit pas, $s_{a-1,\,n-1}$ le sera également.

Or $s_{a-1,1}$ est un multiple de a ; il en est donc de même de $s_{a-1,2}$, puis de $s_{a-1,3}$, etc.

Cor. XII. Lemme de Gauss. Divisons par p les $\frac{p-1}{2} = m$ premiers multiples de a ; les restes seront, dans un certain ordre et avec des signes divers, les nombres ± 1, ± 2, ± 3, ... $\pm m$. Posons en conséquence :

$$a \equiv r_1 , \quad 2a \equiv r_2 , \quad \dots \quad ma \equiv r_m ,$$

on aura, en multipliant, n désignant le nombre des restes négatifs,

$$m\,!\; a^m \equiv r_1 r_2 \dots r_m = (-1)^n\, m\,!$$

d'où

$$a^m \equiv (-1)^n . \tag{7}$$

Application. Soit $a = 2$. Les restes ne sont autres que les produits eux-mêmes 2, 4, 6, ... $2m = p-1$. Les produits plus petits que $\frac{1}{2}p$ donnent des restes positifs. Or le nombre des produits 2, 4, 6, ... $p-1$, inférieurs à $\frac{1}{2}p$ est pair, si $p = 8+1$ ou $8+3$; et il est impair si $p = 8+5$ ou $8+7$. Mais le nombre total m des produits est pair pour $8+1$ ou $8+5$, et impair pour $p = 8+3$ ou $8+7$. Le nombre n des restes plus grand que $\frac{1}{2}p$, est donc pair ou impair selon que $p = 8 \pm 1$ ou $p = 8 \pm 3$.

En résumé, on a :

$$2^m \equiv (-1)^{\frac{p^2-1}{8}} . \tag{8}$$

Cor. XIII. Théorème d'Euler. Les nombres a et b étant premiers entre eux, on a :

$$a^{\varphi(b)} \equiv 1 \pmod{b} \tag{9}$$

$\varphi(b)$ désigne, d'après Gauss, le nombre des entiers inférieurs à b et premiers avec lui, $1, \alpha, \alpha', \alpha'', \ldots b-1$.

Démonstration de Gauss. Appelons Π le produit $1\alpha\alpha'\alpha''\ldots(b-1)$, il viendra, en se rappelant le *Cor. IV.*

$$\Pi a^{\varphi(b)} \equiv \Pi . \quad \text{ou} \quad \Pi [a^{\varphi(b)} - 1] \equiv 0 \pmod{b}$$

d'où la relation (9).

Remarques. 1°. Si b est un nombre premier p, comme $\varphi(p) = p - 1$, la formule (9) devient

$$a^{p-1} \equiv 1 \tag{10}$$

et constitue le *théorème de Fermat.*

2° *Démonstration de Poinsot.* Joignons de a en a les b sommets d'un polygone ; b étant premier avec a, on retombera sur le point de départ. Autrement celui auquel on aboutit pourrait être considéré comme le point de départ d'un certain polygone fermé. Si on suppose que, dans cette construction, on ne passe que par n sommets, le nombre total des sommets rencontrés en répétant cette construction pour chacun des b sommets, serait ainsi na, nombre divisible par b puisqu'on parcourt une ou plusieurs fois le polygone, n est donc multiple de b et ne peut être que b.

Ayant joint les b sommets de a en a, à partir d'un sommet déterminé, on aura un second polygone de b côtés qu'on traitera de même, ce qui en donnera un troisième ; et ainsi de suite, jusqu'à ce qu'on retrouve le premier polygone. On aura ainsi n polygones différant entre eux et qui seront tout ou partie des polygones étoilés possibles, lesquels sont au nombre de $\varphi(b)$, d'après ce qui a été dit plus haut. Dans ce second cas, n sera un diviseur de $\varphi(b)$; en effet prenons un des $\varphi(b)$ polygones qui ne se trouvent pas dans la série des

n polygones différents qu'on vient de définir ; on pourra de même en tirer n [1] polygones différant entre eux et différents des premiers ; car les constructions dérivant de la même loi, si un polygone de la première série était identique à un de la seconde, par exemple, les deux séries seraient forcément identiques. Ainsi les polygones non compris dans le premier groupe se partagent également en groupes de n.

Mais le procédé revient à prendre les sommets de a en a, de a^2 en a^2, de a^3 en a^3, ... de a^n en a^n ; or dans ce dernier cas, les sommets sont pris de 1 en 1 : on a donc

$$a^n \equiv 1 \pmod{b}$$

d'où (9) en élevant à la puissance entière $\frac{\varphi(b)}{n}$.

Cor. XIV. Théorème de Wilson. On a :

$$(11) \qquad (p-1)! \equiv -1$$

Démonstration de Gauss. Associons deux à deux les nombres 2, 3, ... $p-2$; il viendra en multipliant ces $\frac{1}{2}(p-3)$ groupes,

$$(12) \qquad 2.3 \ldots (p-2) \equiv 1 ,$$

d'où (11) en multipliant par $p-1$.

Remarques. 1°. Ce beau théorème paraît avoir été entrevu par Leibniz ; Waring (*Med. alg.* 1770) en fait honneur à Jean Wilson. La première démonstration en a été donnée par Lagrange en 1771 : il considère l'égalité

$$(\alpha) \qquad (x+1)(x+2)\ldots(x+p-1) = x^{p-1} + \mathrm{A}x^{p-2} + \mathrm{B}x^{p-3} + \ldots + \mathrm{K}x + \mathrm{L}$$

et compare les deux résultats obtenus, 1° en changeant dans (α) x en $x+1$, 2° en multipliant (α) par $x+p$. Il tire de là les relations

$$(13) \quad \begin{cases} \mathrm{A} \equiv 0 , \quad \mathrm{B} \equiv 0 , \ldots \mathrm{K} \equiv 0 , \quad \mathrm{L}+1 \equiv 0 . \\ (p-1)\,\mathrm{L} = \mathrm{C}_{p,p} + \mathrm{C}_{p-1,p-1}\,\mathrm{A} + \mathrm{C}_{p-2,p-2}\,\mathrm{B} + \ldots = \\ \qquad 1 + \mathrm{A} + \mathrm{B} + \ldots + \mathrm{K} . \end{cases}$$

$$(14) \qquad (x+1)(x+2)\ldots(x+p-1) - x^{p-1} + 1 \equiv 0 .$$

[1] Le nombre n des polygones différents obtenus est indépendant en effet de la position des b points : il doit être le même, quel que soit le polygone dont on part.

Si x est nul ou congru à p, la relation (14) donne le théorème de Wilson. Dans les autres cas, il conduit au théorème de Fermat.

2°. Le théorème de Wilson fournit un moyen de reconnaître si un nombre donné est premier; en effet si p était multiple de a, par exemple, a diviserait $(p-1)!$ et par suite ne pourrait diviser $(p-1)!+1$. Malheureusement ce moyen est impraticable à cause des immenses calculs que nécessiterait cette recherche, même dans le cas de nombres peu considérables.

3°. *Généralisation de Gauss.* Le produit des $\varphi(b)$ nombres plus petits que b et premiers avec lui, est de l'une des deux formes $\pm 1 \pmod{b}$. Poinsot a donné, de ce théorème les trois démonstrations que voici :

Si a est l'un des nombres α, α', α'', ... $b-1$, l'un des nombres $a\alpha$, $a\alpha'$, ... est de la forme $1 \pmod{b}$. Soit $a\alpha \equiv 1 \pmod{b}$ et supposons d'abord $a = \alpha$, il viendra $a(b-a) \equiv -1 \pmod{b}$; le produit des couples de la forme $a(b-a)$ sera donc $\pm 1 \pmod{b}$, selon que leur nombre sera pair ou impair. Ce nombre n'est d'ailleurs autre chose que celui des racines de la congruence $x^2 \equiv 1 \pmod{b}$.

Soit maintenant a différent de α. Les produits analogues à $a\alpha$ seront tous de la forme $1 \pmod{b}$ et aucun des nombres considérés tout à l'heure ne se retrouvera parmi ces derniers, puisqu'à chaque nombre a donnant $a^2 \equiv 1 \pmod{b}$, ne correspond qu'un nombre $a' = b - a$, donnant $aa' \equiv -1 \pmod{b}$, et qu'à chaque nombre a, différent de son associé α, ne correspond qu'un seul nombre α tel que $a\alpha \equiv 1 \pmod{b}$.

Multipliant tous ces couples, on obtient le théorème.

Gauss distingue les cas où il faut le signe + ou le signe —, mais nous nous en tiendrons là.

Autre démonstration. Posons $\alpha\alpha'\alpha''\ldots(b-1) = \Pi$; les nombres

$$\Pi, \frac{\Pi}{\alpha}, \frac{\Pi}{\alpha'}, \ldots \frac{\Pi}{b-1}$$

sont tous différents et premiers avec b. Les restes de leur

division par b seront les nombres α, α', ... ; de là, en multipliant, la congruence

$$\Pi^{\varphi(b)-1} \equiv \Pi , \qquad \text{d'où} \qquad \Pi^{\varphi(b)} \equiv \Pi^2 \qquad (\text{mod. } b)$$

Autre démonstration. Joignons, de α en α, les sommets d'un polygone P, de b côtés, et, de x en x, ceux du deuxième polygone P′ ainsi obtenu, x étant choisi tel que le troisième polygone coïncide avec le premier P. On a ainsi pris les sommets de αx en αx, ce qui produit le même résultat que si on les avait pris de 1 en 1. Ainsi si α est premier avec b, il y aura toujours un nombre x tel que $\alpha x \equiv 1$ (mod. b) [1].

Si $x = \alpha$, et qu'on prenne les sommets de P′ de $b - \alpha$ en $b - x$, on retombera sur le polygone P renversé ; donc $\alpha(b - \alpha)$ revient à -1 ou bien $\alpha(b - \alpha) \equiv -1$ (mod. b).

Ainsi, dans tous les cas, les nombres $1, \alpha, \alpha', \ldots b - 1$ peuvent s'associer de manière que leur produit soit de la forme ± 1 (mod. b) : on peut donc écrire

$$\Pi \equiv \pm 1 \qquad (\text{mod. } b).$$

selon que le nombre des produits de la forme -1 (mod. b), est pair ou impair [2].

Exercices.

1. La somme des quotients provenant de la division par b des nombres $a, 2a, 3a, \ldots (b-1)a$, est égale à $\frac{1}{2}(a-1)(b-1)$. (Gauss).

---

[1] De là, une solution graphique de la congruence $\alpha x - by = 1$. (Poinsot).

[2] Si b est un nombre premier p, la démonstration se simplifie ainsi, d'après Cayley.

D'après ce qui a été dit, *Cor. XIII*, 2°, premier alinéa, b points disposés régulièrement sur une circonférence sont les sommets de $\frac{\varphi(b)+1}{2}$ polygones réguliers de b côtés ; d'où, si q est premier et égal à p, $\frac{1}{2}(p-1)$ polygones.

Or le nombre total des polygones, tant réguliers qu'irréguliers, est évidemment la moitié du nombre des permutations de $p-1$ objets, puisque ces polygones se reproduisent deux à deux. D'un autre côté, si nous faisons tourner autour de son centre, et successivement des angles $\frac{2\pi}{p}, \frac{4\pi}{p}, \frac{6\pi}{p}, \ldots \frac{2(p-1)\pi}{p}$, un polygone irrégulier quelconque, nous obtiendrons $p-1$ autres polygones irréguliers : le nombre des polygones irréguliers possibles est donc un multiple de p. De là, la relation

$$\frac{1}{2}(p-1)! - \frac{1}{2}(p-1) \equiv 0 .$$

2. Si $x = \alpha$, $y = \beta$ est une solution de $ax - by = 1$; $x = c\alpha$, $y = c\beta$ en est une de $ax - by = c$.

3. Trouver x tel que $x \equiv \alpha$ (mod. a) et $x \equiv \beta$ (mod. b).

On cherche $b\mathrm{A} \equiv 1$ (mod. a) et $a\mathrm{B} \equiv 1$ (mod. b), ce qui donne

$$x \equiv \mathrm{A}b\alpha + \mathrm{B}a\beta \qquad (\text{mod. } ab)$$

4. Soit g celui des $b - 1$ premiers entiers positifs qui rend $c - ag$ multiple de b, l'équation $ax + by = c$ a un nombre de solution représenté par la *formule de Paoli,*

$$\mathrm{E}\left(\frac{c - ag}{ab}\right) + 1 .$$

5. La solution de $ax - by = c$ est donnée par la *formule de Libri,*

$$x = \frac{c - 1}{2} + \frac{1}{2} \sum_{k=1}^{k=b} \frac{\sin \dfrac{(2c - a)\, k\pi}{b}}{\sin \dfrac{ak\pi}{b}} .$$

6. Soit μ le plus grand commun diviseur des nombres donnés α, β, γ, ... On peut toujours déterminer les nombres A, B, C, ... de manière qu'on ait

$$\frac{\mathrm{A}}{\alpha} + \frac{\mathrm{B}}{\beta} + \ldots = \mu \qquad \text{(Gauss).}$$

7. Résoudre les équations

$$x'y'' - x''y' = a\ ,\quad x''y - xy'' = a'\ ,\quad xy' - x'y = a''. \qquad \text{(Gauss)}$$

8. Soit à résoudre les équations

$$x = ay + \alpha = bz + \beta = cw + \gamma = \ldots$$

a, b, c, ... étant premiers deux à deux. On pose $\mathrm{P} = abc \ldots$ et on calcule a', b', c', ... de manière qu'on ait

$$\frac{\mathrm{P}}{a}\, a' \equiv 1 \text{ (mod. } a)\ ,\qquad \frac{\mathrm{P}}{b}\, b' \equiv 1 \text{ (mod. } b)\ , \ldots$$

d'où

$$x = \mathrm{P}\left(\frac{a'\alpha}{a} + \frac{b'\beta}{b} + \ldots\right)$$

Le problème est ramené au calcul des associés de $\frac{P}{a}$, ... (Voir exercices n^{os} 10, 11 et 22).

9. *Regula cœci.* Partager A en n parties telles que a fois la première, b fois la deuxième, ... fassent ensemble une somme B.

Supposons que a est le plus petit des nombres $a, b, c, \ldots$ On a :

$$(b - a)\,y + (c - a)\,z + \ldots = B - aA\,,$$

équation de la forme $\alpha y + \beta z + \ldots = C$, qu'on résout en remarquant qu'il y a au moins deux coefficients, α et β par exemple, qui sont premiers entre eux, ce qui permet de poser

$$\alpha\alpha' + \beta\beta' = 1\,, \quad \text{d'où} \quad x = \alpha'(C - \gamma\alpha - \ldots) + \beta\lambda\,,$$
$$y = \beta'(C - \gamma\alpha - \ldots) + \alpha\mu\,, \ldots$$

$\lambda, \mu, \ldots$ désignant des quantités indéterminées.

10. Divisons a par b, b par le reste, ce reste par le second reste, et ainsi de suite, de sorte qu'on ait

$$a = \alpha b + c\,, \quad b = \beta c + d\,, \quad c = \gamma d + e\,, \ldots$$

$\alpha, \beta, \ldots$ sont entiers et $b, c, \ldots$ diminuent jusqu'à ce qu'on parvienne à $m = \mu n + 1$.

Formons les expressions

$$[\alpha] = \alpha = A$$
$$[\alpha, \beta] = \beta A + 1 = B\,,$$
$$[\alpha, \beta, \gamma] = \gamma B + 1 = C\,,$$
$$\ldots\ldots\ldots\ldots$$

on aura

$$[\alpha, \beta, \ldots \mu]\,[\beta, \ldots \lambda] - [\alpha, \ldots \lambda]\,[\beta, \ldots \mu] = \pm 1\,.$$

De là le moyen de résoudre $ax - by = \pm 1$[1].

11. Soient $r_1, r_2, r_3, \ldots$ et $q_1, q_2, q_3, \ldots$ les restes et les quotients obtenus successivement en divisant p par a, $r_1, r_2, r_3, \ldots$ Les restes sont tous différents de zéro et décroissent jusqu'à $r_n = 1$. On a :

$$aq_1 q_2 \cdots q_{n-1} \equiv -(-1)^n$$

[1] Les théories que contiennent les exercices 2, 3, 8. 9 et 10 étaient connues des Indiens, comme on le voit chez Brahmegupta et Bhaskara. Mais c'est seulement Bachet qui a commencé à les exposer avec méthode et en détail.

De là, la solution de $ax \equiv \pm 1$. (Binet).

12. a et b étant premiers entre eux, le produit

$$\frac{x^a - 1}{x - 1} \quad \frac{x^b - 1}{x - 1}$$

est divisible par $\frac{x^{ab} - 1}{x - 1}$ (Gauss).

13. Si on peut écrire $a^2 \equiv r$ et $b^2 \equiv -r$, on a : $x^2 \equiv -1$ (Euler). En effet posons $ax \equiv b$, il viendra $a^2x^2 \equiv b^2 \equiv -a^2$. (Gauss).

14. Soient $a^2 \equiv r$, $b^2 \equiv rs$, on peut écrire $x^2 = s$ (Euler). En effet posons $ax \equiv b$, il viendra $rs \equiv b^2 \equiv a^2x^2 \equiv rx^2$. (Gauss).

15. Soit $a^g \equiv a^h \equiv r$, g et h étant premiers entre eux, on peut écrire $r^z \equiv a$. En effet posons $gx - hy = 1$, il viendra

$$r^x \equiv a^{gx} = a^{hy+1} \equiv ar^y \ . \qquad \text{(Legendre).}$$

16. Aucun nombre non décomposable en deux carrés entier ne l'est pas non plus en deux carrés fractionnaires (Fermat).

17. L'égalité $ax^2 - y^2 = 1$ ne peut avoir lieu si a n'est pas la somme de deux carrés. (Brahmegupta).

18. Les diviseurs du nombre $a^2 - 3b^2$ sont de l'une des formes quadratiques $\pm x^2 \mp 3y^2$, ou de l'une des formes linéaires 12 ± 1. (Lagrange).

19. Les nombres $a^4 + 1$ et $a^4 - a^2 + 1$ sont respectivement des deux formes linéaires $8 + 1$ et $12 + 1$. En effet on peut les écrire

$$(a^2 - 1)^2 + 1 \quad \text{et} \quad (a^2 - 1)^2 + a^2 = (a^2 + 1)^2 - 3a^2. \quad \text{(Serret).}$$

20. Si l'un des coefficients A, B, est multiple de p, la congruence $Ax^n + Bx^{n-1} + \ldots + M \equiv 0$ ne saurait avoir n racines.

Il en est de même si $M \equiv 0$.

Si elle a n racines, a, b, ... on peut l'écrire $A(x - a)(x - b) \ldots \equiv 0$ et l'on a :

$$A(a + b + \ldots) + B \equiv 0 \ , \quad ab \ldots \equiv \pm M \ .$$

21. Du *Cor. XI,* déduire la relation

$$s_{p-1,\,p-1} \equiv (p-1)\,!$$

ainsi que le *Cor. IX.*

22. Posons $a^{\varphi(b)} = kb + 1$, on aura

$$a\,(ca^{\varphi(b)-1}) - b\,(ck) = c$$

d'où une solution de $ax - by = c$ (Poinsot). Ainsi l'associé de a relativement à b est

$$x = a^{\varphi(b)-1}$$

23. Trouver x tel que $x \equiv \alpha$ (mod. a) et $\equiv \beta$ (mod. b). On a :

$$x = b^{\varphi(a)}\,\alpha + a^{\varphi(b)}\,\beta \qquad \text{(mod. } ab\text{)}.$$

Ainsi les nombres à la fois des deux formes $3 + 1$ et $4 - 1$ sont de la forme $12 + 7$; ceux des formes $3 - 1$ et $4 + 1$, de la forme $12 + 5$; ceux des formes 3 ± 1 et 4 ± 1, de la forme 12 ± 1.

24. Changeons successivement x et y en $1, \alpha, \alpha', \ldots b - 1$ dans la relation $a \equiv xy$ (mod. b) et multiplions, il viendra

$$a^{\varphi(b)} \equiv -\Pi^2 \quad \text{(mod. } b\text{)} \qquad \text{d'où} \qquad \Pi^2 \equiv 1 \quad \text{(mod. } b^2\text{)}$$

25. Démontrer les relations

$$\frac{(p-1)\,(p-2)\,\ldots\,m}{\left(\frac{p+1}{2}\right)\,!} \equiv (-1)^m\,. \qquad \text{(Lebesgue).}$$

$$(a-1)\,!\,(p-a)\,! \equiv (-1)^a\,. \qquad \text{(Lagrange).}$$

A. Aubry (Beaugency, Loiret).