EXERCICES D'ANALYSE

ET DE

PHYSIQUE MATHÉMATIQUE

MÉMOIRE

SUR LA

RÉSOLUTION DES ÉQUATIONS INDÉTERMINÉES

DU PREMIER DEGRÉ EN NOMBRES ENTIERS.

Supposons qu'il s'agisse de résoudre, en nombres entiers, une équation indéterminée du premier degré à plusieurs inconnues. Si ces inconnues se réduisent à deux

$$x, \quad y,$$

l'équation indéterminée sera de la forme

$$ax + by = k, \tag{1}$$

a, b, k désignant trois quantités entières, et ne pourra être résolue que dans le cas où le plus grand commun diviseur de a et de b divisera k. Mais alors on pourra diviser les deux membres de l'équation (1) par ce plus grand commun diviseur; et comme on pourra, en outre, si a est négatif, changer les signes de tous les termes, il est clair que l'équation (1) pourra être réduite à la forme

$$mx \pm ny = \pm l, \tag{2}$$

l, m, n désignant trois nombres entiers, et m, n étant premiers entre eux.

Observons maintenant que l'équation (2) coïncide avec l'équivalence

$$mx \equiv \pm l \pmod{n}$$

ou

$$x \equiv \pm \frac{l}{m} \pmod{n}, \tag{3}$$

et qu'en vertu de la formule

$$\frac{l}{m} \equiv l\frac{1}{m} \pmod{n},$$

la résolution de l'équivalence (3) peut être réduite à celle de la suivante

$$x \equiv \frac{1}{m} \pmod{n}. \tag{4}$$

D'autre part, si n est un nombre premier, on aura, d'après un théorème connu de Fermat,

$$m^{n-1} \equiv 1 \pmod{n}; \tag{5}$$

par conséquent

$$\frac{1}{m} \equiv m^{n-2} \pmod{n}.$$

Donc alors m^{n-2} sera une des valeurs de x propres à vérifier l'équivalence (4), de sorte qu'on résoudra cette équivalence en posant

$$x \equiv m^{n-2} \pmod{n}. \tag{6}$$

Telle est la conclusion très simple à laquelle M. Libri et M. Binet sont parvenus pour le cas où le module n est un nombre premier. Pour étendre cette même solution à tous les cas possibles, il suffirait de substituer au théorème de Fermat le théorème d'Euler suivant lequel, n étant un module quelconque et m un entier premier à n, on aura généralement

$$m^{\chi} \equiv 1 \pmod{n}, \tag{7}$$

si l'exposant N renferme autant d'unités qu'il y a de nombres entiers inférieurs à n et premiers à n (¹). En effet, l'équation (7) étant admise, on en conclura

$$\frac{1}{m} \equiv m^{N-1} \pmod{n},$$

et, par conséquent,

$$m^{N-1}$$

sera l'une des valeurs de x propres à vérifier l'équivalence (4), de sorte qu'on résoudra cette équivalence en prenant

$$x \equiv m^{N-1} \pmod{n}. \tag{8}$$

L'équivalence (4), étant résolue comme on vient de le dire, entraînera la résolution de l'équivalence (3) qui coïncide avec l'équation (2), et, par suite, la résolution de l'équation (1), dans le cas où le plus grand commun diviseur de a et de b divisera k. On résoudra, en particulier, l'équivalence (3) en prenant

$$x \equiv \pm m^{N-1} l \pmod{n}. \tag{9}$$

(¹) M. Poinsot nous a dit avoir remis autrefois à M. Legendre une Note manuscrite dans laquelle il avait ainsi étendu à des modules quelconques la solution présentée par M. Binet, et relative au cas où n est un nombre premier. Dans cette même Note, M. Poinsot donnait du théorème d'Euler la démonstration suivante, analogue à celle qui, dans le Mémoire de M. Binet, se trouve appliquée au théorème de Fermat :

Soient

$$1, a, b, c, \ldots$$

la suite des entiers inférieurs à n, mais premiers à n; N le nombre de ces entiers et m l'un quelconque d'entre eux. La suite

$$m, am, bm, cm, \ldots$$

se composera encore de termes, premiers à n, mais qui, divisés par n, donneront des restes différents. Donc chaque terme de la seconde suite sera équivalent, suivant le module n, à un seul terme de la première, et l'on aura

$$1.a.b.c\ldots \equiv m.am.bm.cm\ldots \equiv 1.a.b.c\ldots m^N \pmod{n}$$

ou, ce qui revient au même,

$$1.a.b.c\ldots(m^N - 1) \equiv 0 \pmod{n},$$

puis on en conclura

$$m^N - 1 \equiv 0 \quad \text{ou} \quad m^N \equiv 1 \pmod{n}$$

En résumé, on pourra énoncer la proposition suivante :

THÉORÈME I. — *a, b, k désignant trois quantités entières, on pourra résoudre en nombres entiers l'équation indéterminée*

$$ax + by = k, \tag{1}$$

si le plus grand commun diviseur de a et de b divise k.

Supposons d'ailleurs qu'en divisant a, b, k par ce plus grand commun diviseur, et changeant s'il est nécessaire les signes de tous les termes de l'équation ainsi obtenue, on la réduise à la suivante

$$mx \pm ny = \pm l, \tag{2}$$

ou, ce qui revient au même, à l'équivalence

$$x \equiv \pm \frac{l}{m} \pmod{n}, \tag{3}$$

l, m, n désignant trois nombres entiers, et m, n étant premiers entre eux. Pour vérifier l'équivalence (3), il suffira de poser

$$x \equiv \pm m^{N-1} l \pmod{n},$$

N désignant le nombre des entiers inférieurs à n, mais premiers à n.

Corollaire I. — L'équation indéterminée

$$ax + by = k$$

est toujours résoluble en nombres entiers, non seulement lorsque les coefficients a, b des deux inconnues sont premiers entre eux, mais aussi lorsque la valeur numérique du terme tout connu k est égale au plus grand commun diviseur de a, b, ou divisible par ce plus grand commun diviseur. Par suite, le plus grand commun diviseur de deux quantités entières a, b peut toujours être présenté sous la forme

$$ax + by,$$

x, y désignant encore des quantités entières.

Corollaire II. — l, m, n désignant trois nombres entiers, et m, n étant premiers entre eux, on peut toujours satisfaire, par des valeurs entières de x, y, à l'équation

$$mx - ny = \pm l.$$

D'ailleurs les diverses valeurs de x propres à vérifier cette équation, ou, ce qui revient au même, l'équivalence

$$x \equiv \mp \frac{l}{m} \pmod{n},$$

sont toutes équivalentes entre elles suivant ce module n; en sorte que, l'une d'elles étant désignée par ξ, on aura généralement

$$x = \xi + nz,$$

z désignant une quantité positive ou négative.

On déduit aisément du premier théorème celui que nous allons énoncer.

THÉORÈME II. — *Soient*

$$n = n_{,} n_{,,}$$

un module décomposable en deux facteurs $n_{,}, n_{,,}$, *premiers entre eux; r l'un quelconque des entiers inférieurs à n, mais premiers à n; et*

$$r_{,}, \quad r_{,,}$$

les restes qu'on obtient, quand on divise r par le premier ou le second des deux facteurs

$$n_{,}, \quad n_{,,}.$$

Non seulement à chaque valeur de r correspondra un seul système de valeurs de $r_{,}, r_{,,}$, *mais réciproquement à chaque système de valeurs de* $r_{,}, r_{,,}$ *correspondra une seule valeur de r.*

Démonstration. — D'abord $r_{,}$, étant le reste de la division de r par $n_{,}$, sera complètement déterminé quand on connaîtra r, et l'on pourra en dire autant de $r_{,,}$. De plus, à deux valeurs données de

$$r_{,}, \quad r_{,,}$$

correspondra une valeur de r qui devra être de chacune des formes

$$r_{\prime} + n_{\prime} x, \quad r_{\prime\prime} + n_{\prime\prime} y,$$

x, y désignant deux quantités entières. Or les deux équations

$$r = r_{\prime} + n_{\prime} x, \qquad r = r_{\prime\prime} + n_{\prime\prime} y$$

entraîneront la formule

$$r_{\prime} + n_{\prime} x = r_{\prime\prime} + n_{\prime\prime} y,$$

ou

$$n_{\prime} x - n_{\prime\prime} y = r_{\prime\prime} - r_{\prime};$$

et les valeurs de x, propres à vérifier cette formule, seront de la forme

$$\xi + n_{\prime\prime} z,$$

ξ désignant l'une quelconque de ces mêmes valeurs et z une quantité entière positive ou négative. Cela posé, si l'on fait, pour abréger,

$$r_{\prime} + n_{\prime} \xi = \mathfrak{R},$$

l'équation

$$r = r_{\prime} + n_{\prime} x$$

donnera

$$r = \mathfrak{R} + n_{\prime} n_{\prime\prime} z,$$

ou, ce qui revient au même,

$$r = \mathfrak{R} + n z.$$

Or, puisque les diverses valeurs de r que déterminerait cette dernière équation, si la quantité entière z restait arbitraire, sont équivalentes entre elles suivant le module n, il est clair qu'une seule sera positive et inférieure à n. Donc à des valeurs données de $r_{\prime}$, $r_{\prime\prime}$ correspondra une seule valeur de r, positive et inférieure à n. Si l'on étend le théorème II au cas où le module n est décomposable en plus de deux facteurs, on obtiendra la proposition suivante :

THÉORÈME III. — *Soient :*

$$n = n_{\prime} n_{\prime\prime} n_{\prime\prime\prime} \ldots$$

un module décomposable en plusieurs facteurs

$$n_{\prime}, \quad n_{\prime\prime}, \quad n_{\prime\prime\prime}, \quad \ldots,$$

qui soient tous premiers entre eux ; r l'un quelconque des entiers inférieurs à n ; et

$$r_{\prime}, \quad r_{\prime\prime}, \quad r_{\prime\prime\prime}, \quad \ldots$$

les restes qu'on obtient quand on divise r par l'un des facteurs

$$n_{\prime}, \quad n_{\prime\prime}, \quad n_{\prime\prime\prime}, \quad \ldots.$$

Non seulement à chaque valeur de r correspondra un seul système de valeurs de $r_{\prime}$, $r_{\prime\prime}$, $r_{\prime\prime\prime}$, ...; *mais réciproquement, à chaque système de valeurs de* $r_{\prime}$, $r_{\prime\prime}$, $r_{\prime\prime\prime}$, ... *correspondra une seule valeur de r.*

Démonstration. — En raisonnant comme dans le cas où les facteurs $n_{\prime}$, $n_{\prime\prime}$, ... se réduisent à deux, on prouvera d'abord qu'à chaque valeur de r répond un seul système de valeurs de $r_{\prime}$, $r_{\prime\prime}$, $r_{\prime\prime\prime}$, ... Soit d'ailleurs

$$n'$$

le produit des facteurs de n différents de $n_{\prime}$, en sorte qu'on ait

$$n' = \frac{n}{n_{\prime}} = n_{\prime\prime} n_{\prime\prime\prime} \ldots,$$

et nommons r' le reste de la division de r par n'. En vertu du théorème I, si les facteurs $n_{\prime}$, $n_{\prime\prime}$, $n_{\prime\prime\prime}$ se réduisent à trois, on verra correspondre une seule valeur de r' à chaque système de valeurs de $r_{\prime\prime}$, $r_{\prime\prime\prime}$, et une seule valeur de r à chaque système de valeurs de $r_{\prime}$, r', par conséquent à chaque système de valeurs de $r_{\prime}$, $r_{\prime\prime}$, $r_{\prime\prime\prime}$. Ainsi l'on passe facilement du cas où le nombre des facteurs de n est 2, au cas où ce nombre devient égal à 3. On passera de la même manière du cas où il existe trois facteurs de n premiers entre eux, au cas où il en existe quatre, et ainsi de suite. Donc le théorème III est généralement exact, quel que soit le nombre des facteurs premiers de n.

Corollaire. — Le module

$$n = n_{\prime} n_{\prime\prime} n_{\prime\prime\prime} \ldots,$$

étant décomposable en facteurs

$$n_{,}, \quad n_{,,}, \quad n_{,,,}, \quad \ldots,$$

qui soient premiers entre eux, nommons toujours

r, l'un quelconque des entiers inférieurs à n, mais premiers à n;
$r_{,}$, l'un quelconque des entiers inférieurs à $n_{,}$, mais premiers à $n_{,}$;
$r_{,,}$, l'un quelconque des entiers inférieurs à $n_{,,}$, mais premiers à $n_{,,}$;
etc.;

et soient en outre :

N, le nombre des valeurs de r;
$\mathrm{N}_{,}$, le nombre des valeurs de $r_{,}$;
$\mathrm{N}_{,,}$, le nombre des valeurs de $r_{,,}$;
etc.

Les systèmes de valeurs qu'on pourra former en combinant une valeur de $r_{,}$ avec une valeur de $r_{,,}$, avec une valeur de $r_{,,,}$, ... seront évidemment en nombre égal au produit

$$\mathrm{N}_{,}\mathrm{N}_{,,}\mathrm{N}_{,,,}\ldots.$$

Donc, puisqu'à chacun des systèmes correspond une seule valeur de r, et réciproquement, on aura

$$\mathrm{N} = \mathrm{N}_{,}\mathrm{N}_{,,}\mathrm{N}_{,,,}\ldots.$$

Il sera facile maintenant de résoudre la question que nous allons énoncer.

PROBLÈME I. — *Déterminer le nombre* N *des entiers inférieurs à un module donné* n *et premiers à ce module.*

Solution. — Pour résoudre aisément ce problème, il sera bon de considérer successivement les divers cas qui peuvent se présenter, suivant que le module n est un nombre premier, ou une puissance d'un nombre premier, ou un nombre composé quelconque.

Or : 1° si le module n est un nombre premier, alors les entiers

$$1, \quad 2, \quad 3, \quad \ldots, \quad n-1, \quad n,$$

non supérieurs au module n, étant tous, à l'exception de n, premiers à ce module, on aura évidemment

$$\mathrm{N} = n - 1. \tag{10}$$

Alors aussi, la solution que fournira le théorème I pour une équation indéterminée ne différera pas de la solution donnée par M. Libri et par M. Binet.

2° Si le module

$$n = \nu^a$$

se réduit à une certaine puissance d'un nombre premier ν, alors parmi les entiers

$$1, \quad 2, \quad 3, \quad \ldots, \quad n-1, \quad n,$$

dont le nombre est n, les uns, divisibles par ν, seront le produit de ν par les entiers

$$1, \quad 2, \quad 3, \quad \ldots, \quad \frac{n}{\nu},$$

dont le nombre est $\frac{n}{\nu}$; les autres, premiers à ν, ou, ce qui revient au même, à n, seront évidemment en nombre égal à la différence

$$n - \frac{n}{\nu} = n\left(1 - \frac{1}{\nu}\right).$$

On aura donc

$$\mathrm{N} = n\left(1 - \frac{1}{\nu}\right) = \nu^{a-1}(\nu - 1). \tag{11}$$

3° Si le module n est un nombre entier quelconque, on pourra toujours le décomposer en facteurs dont chacun se réduise à un nombre premier ou à une puissance d'un nombre premier. Nommons

$$n_{\prime}, \quad n_{\prime\prime}, \quad n_{\prime\prime\prime}, \quad \ldots$$

ces mêmes facteurs, en sorte qu'on ait

$$n = n_{\prime} n_{\prime\prime} n_{\prime\prime\prime} \ldots$$

et

$$n_{\prime} = \nu_{\prime}^{a}, \qquad n_{\prime\prime} = \nu_{\prime\prime}^{b}, \qquad n_{\prime\prime\prime} = \nu_{\prime\prime\prime}^{c}, \qquad \dots,$$

$\nu_{\prime}, \nu_{\prime\prime}, \nu_{\prime\prime\prime}, \dots$ désignant des nombres premiers distincts les uns des autres. Représentons d'ailleurs

par $N_{\prime}$ le nombre des entiers inférieurs et premiers à $n_{\prime}$;
par $N_{\prime\prime}$ le nombre des entiers inférieurs et premiers à $n_{\prime\prime}$;
par $N_{\prime\prime\prime}$ le nombre des entiers inférieurs et premiers à $n_{\prime\prime\prime}$;
etc.

Le corollaire du théorème III donnera

$$\mathrm{N} = \mathrm{N}_{\prime}\mathrm{N}_{\prime\prime}\mathrm{N}_{\prime\prime\prime}\dots, \tag{12}$$

puis on en conclura, eu égard à la formule (11),

$$\mathrm{N} = n\left(1-\frac{1}{\nu_{\prime}}\right)\left(1-\frac{1}{\nu_{\prime\prime}}\right)\left(1-\frac{1}{\nu_{\prime\prime\prime}}\right)\cdots \tag{13}$$

ou, ce qui revient au même,

$$\mathrm{N} = \nu_{\prime}^{a-1}\,\nu_{\prime\prime}^{b-1}\,\nu_{\prime\prime\prime}^{c-1}\dots(\nu_{\prime}-1)(\nu_{\prime\prime}-1)(\nu_{\prime\prime\prime}-1)\dots. \tag{14}$$

Corollaire. — Lorsque le module n se réduit au nombre 2, ou plus généralement à une puissance 2^{a} de ce même nombre, la valeur de N, en vertu de la formule (10) ou (11), se réduit à l'unité ou plus généralement à 2^{a-1}, en sorte qu'on a

$$\mathrm{N} = 2^{a-1} = \frac{1}{2}n.$$

Revenons maintenant au théorème I. On peut évidemment, dans ce théorème et dans les formules (8), (9), remplacer le nombre N des entiers inférieurs au module n, mais premiers à n, par l'une quelconque des valeurs de i pour lesquelles se vérifie l'équivalence

$$m^{i} \equiv 1 \pmod{n}. \tag{15}$$

Or parmi ces valeurs il en existe une, inférieure à toutes les autres, et