ŒUVRES

COMPLÈTES

D'AUGUSTIN CAUCHY

PARIS. — IMPRIMERIE GAUTHIER-VILLARS ET Cie,
52034 Quai des Grands-Augustins, 55.

ŒUVRES

COMPLÈTES

D'AUGUSTIN CAUCHY

PUBLIÉES SOUS LA DIRECTION SCIENTIFIQUE

DE L'ACADÉMIE DES SCIENCES

ET SOUS LES AUSPICES

DE M. LE MINISTRE DE L'INSTRUCTION PUBLIQUE.

IIe SÉRIE. — TOME XII.

PARIS,
GAUTHIER-VILLARS ET Cie, ÉDITEURS,
LIBRAIRES DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,
Quai des Grands-Augustins, 55.
—
MCMXVI.

SECONDE SÉRIE.

III.

MÉMOIRES

PUBLIÉS EN CORPS D'OUVRAGE.

EXERCICES D'ANALYSE

ET DE

PHYSIQUE MATHÉMATIQUE

(NOUVEAUX EXERCICES)

TOME II. — PARIS, 1841.

DEUXIÈME ÉDITION

RÉIMPRIMÉE

D'APRÈS LA PREMIÈRE ÉDITION.

EXERCICES D'ANALYSE

ET DE

PHYSIQUE MATHÉMATIQUE,

PAR LE BARON AUGUSTIN CAUCHY,

Membre de l'Académie des Sciences de Paris, de la Société Italienne, de la Société royale de Londres, des Académies de Berlin, de Saint-Pétersbourg, de Prague, de Stockholm, de Gœttingue, de l'Académie Américaine, etc

TOME DEUXIÈME.

PARIS,

BACHELIER, IMPRIMEUR-LIBRAIRE

DE L'ÉCOLE POLYTECHNIQUE, DU BUREAU DES LONGITUDES, ETC.,

QUAI DES AUGUSTINS, N° 55.

1841

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

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

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

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

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*

$$n = n_1 n_2$$

un module décomposable en deux facteurs n_1, n_2, premiers entre eux; r l'un quelconque des entiers inférieurs à n, mais premiers à n; et

$$r_1, \quad r_2$$

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

$$n_1, \quad n_2.$$

Non seulement à chaque valeur de r correspondra un seul système de valeurs de r_1, r_2, mais réciproquement à chaque système de valeurs de r_1, r_2 correspondra une seule valeur de r.

Démonstration. — D'abord r_1, étant le reste de la division de r par n_1, sera complètement déterminé quand on connaîtra r, et l'on pourra en dire autant de r_2. De plus, à deux valeurs données de

$$r_1, \quad r_2$$

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

$$r_1 + n_1 x, \quad r_2 + n_2 y,$$

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

$$r = r_1 + n_1 x, \qquad r = r_2 + n_2 y$$

entraîneront la formule

$$r_1 + n_1 x = r_2 + n_2 y,$$

ou

$$n_1 x - n_2 y = r_2 - r_1;$$

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

$$\xi + n_2 z,$$

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,

$$r_1 + n_1 \xi = \mathcal{R},$$

l'équation

$$r = r_1 + n_1 x$$

donnera

$$r = \mathcal{R} + n_1 n_2 z,$$

ou, ce qui revient au même,

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

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_1, r_2 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 :*

$$n = n_1 n_2 n_3 \ldots$$

un module décomposable en plusieurs facteurs

$$n_1, \quad n_2, \quad n_3, \quad \ldots,$$

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

$$r_1, \quad r_2, \quad r_3, \quad \ldots$$

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

$$n_1, \quad n_2, \quad n_3, \quad \ldots.$$

Non seulement à chaque valeur de r correspondra un seul système de valeurs de r_1, r_2, r_3, ... ; mais réciproquement, à chaque système de valeurs de r_1, r_2, r_3, ... correspondra une seule valeur de r.

Démonstration. — En raisonnant comme dans le cas où les facteurs n_1, n_2, ... se réduisent à deux, on prouvera d'abord qu'à chaque valeur de r répond un seul système de valeurs de r_1, r_2, r_3, ... Soit d'ailleurs

$$n'$$

le produit des facteurs de n différents de n_1, en sorte qu'on ait

$$n' = \frac{n}{n_1} = n_2 n_3 \ldots,$$

et nommons r' le reste de la division de r par n'. En vertu du théorème I, si les facteurs n_1, n_2, n_3 se réduisent à trois, on verra correspondre une seule valeur de r' à chaque système de valeurs de r_2, r_3, et une seule valeur de r à chaque système de valeurs de r_1, r', par conséquent à chaque système de valeurs de r_1, r_2, r_3. 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

$$n = n_1 n_2 n_3 \ldots,$$

étant décomposable en facteurs

$$n_1, \quad n_2, \quad n_3, \quad \ldots,$$

qui soient premiers entre eux, nommons toujours

r, l'un quelconque des entiers inférieurs à n, mais premiers à n;
r_1, l'un quelconque des entiers inférieurs à n_1, mais premiers à n_1;
r_2, l'un quelconque des entiers inférieurs à n_2, mais premiers à n_2;
etc.;

et soient en outre :

N, le nombre des valeurs de r;
N_1, le nombre des valeurs de r_1;
N_2, le nombre des valeurs de r_2;
etc.

Les systèmes de valeurs qu'on pourra former en combinant une valeur de r_1 avec une valeur de r_2, avec une valeur de r_3, ... seront évidemment en nombre égal au produit

$$N_1 N_2 N_3 \ldots.$$

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

$$N = N_1 N_2 N_3 \ldots.$$

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

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

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

$$n = \nu^{\alpha}$$

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

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

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

$$n_1, \quad n_2, \quad n_3, \quad \ldots$$

ces mêmes facteurs, en sorte qu'on ait

$$n = n_1 n_2 n_3 \ldots$$

et

$$n_{\prime} = \nu_{\prime}^{\lambda}, \qquad n_{\prime\prime} = \nu_{\prime\prime}^{\mu}, \qquad n_{\prime\prime\prime} = \nu_{\prime\prime\prime}^{\varepsilon}, \qquad \ldots,$$

$\nu_{\prime}, \nu_{\prime\prime}, \nu_{\prime\prime\prime}, \ldots$ 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

$$N = N_{\prime} N_{\prime\prime} N_{\prime\prime\prime} \ldots, \tag{12}$$

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

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

ou, ce qui revient au même,

$$N = \nu_{\prime}^{\lambda-1}\nu_{\prime\prime}^{\mu-1}\nu_{\prime\prime\prime}^{\varepsilon-1}\ldots(\nu_{\prime}-1)(\nu_{\prime\prime}-1)(\nu_{\prime\prime\prime}-1)\ldots. \tag{14}$$

Corollaire. — Lorsque le module n se réduit au nombre 2, ou plus généralement à une puissance 2^{α} 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 $2^{\alpha-1}$, en sorte qu'on a

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

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

qui pour ce motif doit être employée de préférence. D'ailleurs cette valeur particulière de i jouit de propriétés remarquables qui peuvent servir à la faire reconnaître et calculer. Entrons à ce sujet dans quelques détails.

Les nombres entiers m, n étant supposés premiers entre eux, l'unité sera certainement, dans la progression géométrique

$$1, \quad m, \quad m^2, \quad m^3, \quad \ldots,$$

le premier terme qui se trouve équivalent, selon le module n, à l'un des termes suivants. En effet, une équivalence de la forme

$$m^{l} \equiv m^{l+i} \pmod{n},$$

dans laquelle l et i seraient entiers et positifs, entraînera nécessairement une autre équivalence de la forme

$$1 \equiv m^{i} \pmod{n},$$

dans laquelle le terme m^{l} de la progression se trouverait remplacé par l'unité. Ajoutons que, si m^{i} représente la moins élevée des puissances entières et positives de m, équivalentes à l'unité suivant le module n, les restes qu'on obtiendra en divisant par n les termes de la progression

$$1, \quad m, \quad m^2, \quad m^3, \quad \ldots$$

formeront une suite périodique, dans laquelle les i premiers termes seront différents les uns des autres. Représentons par

$$1, \quad m', \quad m'', \quad \ldots, \quad m^{(i-1)}$$

ces premiers termes. Comme, dans la progression dont il s'agit, deux termes seront équivalents entre eux suivant le module n quand ils répondront à des exposants de la *base m* équivalents entre eux suivant le module i, on aura évidemment

$$\left\{\begin{array}{l} m^0 \equiv m^i \equiv m^{2i} \equiv \ldots \equiv 1, \\ m^1 \equiv m^{i+1} \equiv m^{2i+1} \equiv \ldots \equiv m', \\ m^2 \equiv m^{i+2} \equiv m^{2i+2} \equiv \ldots \equiv m'', \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ m^{i-1} \equiv m^{2i-1} \equiv m^{3i-1} \equiv \ldots \equiv m^{(i-1)}. \end{array}\right. \pmod{n}. \tag{16}$$

L'exposant de la puissance à laquelle il faut élever la base m pour obtenir un nombre équivalent suivant le module n à un reste donné, est ce qu'on nomme l'*indice* de ce nombre ou de ce reste. Cela posé, il est clair que, dans les formules (16), les indices correspondants au reste 1 seront représentés par les exposants

$$0, \quad i, \quad 2i, \quad \ldots,$$

les indices correspondants au reste m' par les exposants

$$1, \quad i+1, \quad 2i+1, \quad \ldots,$$

les indices correspondants au reste m^2 par les exposants

$$2, \quad i+2, \quad 2i+2, \quad \ldots,$$

etc., enfin les indices correspondants au reste m^{i-1} par les exposants

$$i-1, \quad 2i-1, \quad 3i-1, \quad \ldots.$$

Donc, puisque les restes

$$1, \quad m', \quad m^2, \quad \ldots, \quad m^{i-1}$$

seront tous inégaux entre eux, les seuls indices positifs de l'unité seront les divers multiples de i; et le plus petit de ces indices ou le nombre i montrera combien la suite périodique des restes, indéfiniment prolongée, renferme de restes différents. L'étendue de la période formée avec ces restes

$$1, \quad m', \quad m^2, \quad \ldots, \quad m^{i-1}$$

se trouvera donc indiquée par le plus petit des indices de l'unité, auquel nous donnerons, pour cette raison, le nom d'*indicateur*. Cela posé, on pourra évidemment énoncer la proposition suivante :

THÉORÈME IV. — *m, n désignant deux nombres entiers, et m étant premier à n, les seules puissances entières et positives de m qui seront équivalentes à l'unité suivant le module n, seront celles qui offriront pour exposants l'indicateur i correspondant à la base m et ses divers multiples.*

On déduit immédiatement du théorème IV celui que nous allons énoncer.

THÉORÈME V. — *Si le module n est décomposable en divers facteurs n_1, n_2, ..., en sorte qu'on ait*

$$n = n_1 n_2 \ldots,$$

et si, la base m étant un nombre premier à n, on nomme

$$i_1, \quad i_2, \quad \ldots$$

les indicateurs correspondant aux modules

$$n_1, \quad n_2, \quad \ldots,$$

l'indicateur i, correspondant au module n, sera le plus petit nombre entier qui soit divisible par chacun des indicateurs i_1, i_2, ...

Démonstration. — En effet, l'indicateur i correspondant au module n sera la plus petite des valeurs de i pour lesquelles se vérifiera la formule

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

D'ailleurs, n étant égal au produit des facteurs $n_1, n_2, \ldots$, cette formule entraînera les suivantes :

$$m^i \equiv 1 \pmod{n_1}, \quad m^i \equiv 1 \pmod{n_2}, \quad \ldots.$$

Donc, en vertu du théorème précédent, i devra être à la fois un des multiples de i_1, un des multiples de i_2, ... Donc la valeur cherchée de i sera la plus petite de celles qui seront à la fois divisibles par i_1, par i_2, ...

L'indicateur i, correspondant à un module donné n, varie généralement avec la base m, mais cette variation s'effectue suivant certaines lois, et l'on peut énoncer à ce sujet les propositions suivantes :

THÉORÈME VI. — *Si la base m est décomposable en deux facteurs*

$$m_1, \quad m_2,$$

auxquels correspondent des indicateurs

$$i_1, \quad i_2,$$

premiers entre eux, dans le cas où le nombre n est pris pour module; on aura non seulement

$$m = m_1 m_2^2$$

mais encore, en désignant par i l'indicateur correspondant à la base m et au module n,

$$i = i_1 i_2.$$

Démonstration. — L'indicateur i relatif à la base m vérifiera la formule

$$m^i \equiv 1 \pmod{n},$$

de laquelle on tirera

$$m^{2i} \equiv 1, \qquad m^{3i} \equiv 1, \qquad \ldots,$$

et généralement, si l'on désigne par j un multiple quelconque de i,

$$m^j \equiv 1 \pmod{n}, \tag{17}$$

ou, ce qui revient au même,

$$m^j_1 m^j_2 \equiv 1 \pmod{n}. \tag{18}$$

D'autre part, les indicateurs i_1, i_2, relatifs aux bases m_1, m_2, vérifieront les équivalences

$$m_1^{i_1} \equiv 1, \qquad m_2^{i_2} \equiv 1 \pmod{n}, \tag{19}$$

et il suffira que i_1 divise j pour que la première des formules (19) entraine l'équivalence

$$m_1^j \equiv 1 \pmod{n},$$

par conséquent, eu égard à la formule (18), l'équivalence

$$m_2^j \equiv 1 \pmod{n},$$

qui suppose (*voir* le théorème IV) j divisible par i_2. Ainsi, de ce que le nombre i vérifie l'équivalence

$$m^i \equiv 1 \pmod{n},$$

il résulte que tout multiple de i, divisible par i_1, sera en même temps divisible par i_2; en sorte que i_2 divisera nécessairement le produit ii_1, et par suite le nombre i, si i_1, i_2 sont premiers entre eux. Mais alors i divisible par i_1 devra l'être pareillement, et pour la même raison, par i_2. Donc, si i_1, i_2 sont premiers entre eux, tout nombre i, propre à vérifier l'équivalence

$$m^i \equiv 1 \pmod{n},$$

sera divisible par le produit $i_1 i_2$, et l'indicateur correspondant à la base m, ou la plus petite des valeurs de i pour lesquelles on aura

$$m^i \equiv 1 \pmod{n},$$

devra se réduire à ce produit.

Théorème VII. — *Soient*

$$i_1, \quad i_2$$

les indicateurs correspondant à deux bases diverses

$$m_1, \quad m_2,$$

mais à un même module n. Le plus grand commun diviseur ω des indicateurs i_1, i_2, pourra être décomposé, souvent même de plusieurs manières, en deux facteurs u, v tellement choisis, que les rapports

$$\frac{i_1}{u}, \quad \frac{i_2}{v}$$

soient des nombres premiers entre eux; et, si l'on pose alors

$$m = m_1^u m_2^v,$$

l'indicateur i, relatif à la base m, sera le plus petit nombre entier que puissent diviser simultanément les indicateurs i_1, i_2.

Démonstration. — Concevons que le plus grand commun diviseur ω de i_1, i_2 soit décomposé en facteurs

$$\alpha, \quad \epsilon, \quad \gamma, \quad \ldots,$$

dont chacun représente un nombre premier, ou une puissance d'un nombre premier. Deux produits

$$u, \quad v,$$

formés avec ces même facteurs, de manière qu'on ait

$$uv = \omega,$$

fourniront pour les rapports

$$\frac{i_\prime}{u}, \quad \frac{i_{\prime\prime}}{v}$$

des nombres premiers entre eux, si l'on fait concourir chaque facteur, par exemple le facteur α, à la formation du produit u, quand α est premier à $\frac{i_\prime}{\alpha}$; du produit v, quand α est premier à $\frac{i_{\prime\prime}}{\alpha}$; enfin du produit u ou du produit v indifféremment, quand α est premier à chacun des deux nombres

$$\frac{i_\prime}{\alpha}, \quad \frac{i_{\prime\prime}}{\alpha}.$$

Les deux produits u, v étant formés comme on vient de le dire, pour déduire le théorème VII du théorème VI, il suffit d'observer que,

$$i_\prime, \quad i_{\prime\prime}$$

étant les indicateurs relatifs aux bases

$$m_\prime, \quad m_{\prime\prime},$$

les nombres entiers

$$\frac{i_\prime}{u}, \quad \frac{i_{\prime\prime}}{v}$$

seront les indicateurs relatifs aux bases

$$m_\prime^u, \quad m_{\prime\prime}^v,$$

et que, ces indicateurs étant premiers entre eux, la base m déterminée par la formule

$$m = m_\prime^u m_{\prime\prime}^v$$

devra correspondre à l'indicateur

$$i = \frac{i_\prime}{u}\frac{i_{\prime\prime}}{v} = \frac{i_\prime i_{\prime\prime}}{\omega}.$$

Or cette dernière valeur i sera précisément le plus petit nombre entier que puissent diviser simultanément les indicateurs $i_\prime$, $i_{\prime\prime}$.

Corollaire I. — Pour montrer une application du théorème VII, considérons en particulier le cas où l'on aurait

$$n = 78,$$
$$m_\prime = 5, \qquad m_{\prime\prime} = 29.$$

Comme

$$5^4 \quad \text{et} \quad 29^6$$

seront les puissances les moins élevées des nombres 5 et 29 qui, divisées par le module 78, donneront pour reste l'unité, on aura nécessairement

$$i_\prime = 4, \qquad i_{\prime\prime} = 6, \qquad \omega = 2,$$

et par suite

$$u = 1, \qquad v = 2,$$

attendu que des deux rapports

$$\frac{i_\prime}{2} = 2, \qquad \frac{i_{\prime\prime}}{2} = 3,$$

le second seul sera premier au facteur 2 de ω. Cela posé, pour obtenir une base m correspondant à l'indicateur

$$i = \frac{i_\prime i_{\prime\prime}}{\omega} = 12,$$

il suffira de prendre

$$m = m_\prime^u m_{\prime\prime}^v = 5.29^2;$$

et, puisque

$$5.29^2 \equiv 71 \equiv -7 \pmod{78},$$

il suffira de prendre

$$m = 71.$$

Effectivement, 71^{12} est la première puissance de 71 qui, divisée par 78, donne pour reste l'unité.

Corollaire II. — Étant données deux bases

$$m_1, \quad m_2,$$

qui correspondent à deux indicateurs différents

$$i_1, \quad i_2,$$

on peut toujours trouver une troisième base

$$m$$

qui corresponde à l'indicateur i représenté par le plus petit des nombres que divisent à la fois les deux indicateurs donnés.

Corollaire III. — Soient

$$m_1, \quad m_2, \quad m_3$$

trois bases différentes, et

$$i_1, \quad i_2, \quad i_3$$

les indicateurs qui correspondent à ces trois bases, mais à un seul et même module n. Si l'on nomme i' le plus petit nombre que diviseront simultanément i_2 et i_3, le plus petit nombre i que pourront diviser simultanément i_1 et i' sera en même temps le plus petit des nombres divisibles par chacun des trois facteurs

$$i_1, \quad i_2, \quad i_3.$$

D'ailleurs, à l'aide du théorème VII, on pourra trouver non seulement une base m' correspondant à l'indicateur i', mais encore une base m correspondant à l'indicateur i. Donc, étant données trois bases différentes avec un seul module, on peut toujours trouver une nouvelle base qui corresponde à l'indicateur représenté par le plus petit des nombres que divisent les trois indicateurs correspondants aux trois bases données. En appliquant un raisonnement semblable au cas où l'on donnerait quatre ou cinq bases au lieu de trois, on obtiendra généralement la proposition suivante :

Théorème VIII. — *Étant données plusieurs bases différentes*

$$m_1, \quad m_2, \quad m_3, \quad \ldots,$$

avec un seul module n, on peut toujours trouver une nouvelle base qui corresponde à l'indicateur représenté par le plus petit des nombres que divisent à la fois les indicateurs correspondants aux bases données.

Corollaire. — Si le système des bases données

$$m_1, \quad m_2, \quad m_3, \quad \ldots$$

comprend tous les entiers inférieurs au module donné n et premiers à ce module, les indicateurs

$$i_1, \quad i_2, \quad i_3, \quad \ldots,$$

relatifs à ces mêmes bases, seront tous ceux qui peuvent correspondre au module n. Cela posé, on doit conclure du théorème VIII que tous les indicateurs correspondants à un module donné divisent un même nombre qui coïncide avec l'un de ces indicateurs. Il est d'ailleurs évident que ce dernier doit être le plus grand de tous les indicateurs, ou celui qu'on peut appeler l'*indicateur maximum*. Nommons I cet indicateur maximum. En vertu de la remarque précédente et du théorème IV, l'équivalence

$$m^{\mathrm{I}} \equiv 1 \pmod{n} \tag{20}$$

se trouvera vérifiée toutes les fois que le nombre m sera premier au module n; et, dans cette supposition, on résoudra en nombres entiers l'équation

$$mx \pm ny = \pm l,$$

en prenant

$$x \equiv \pm m^{\mathrm{I}-1} l \pmod{n}. \tag{21}$$

Il nous reste à déterminer, pour chaque module n, l'indicateur maximum I. Cette détermination de l'indicateur maximum se trouve intimement liée à la recherche des valeurs correspondantes de la base m, valeurs que nous appellerons *racines primitives* du module n, en géné-

ralisant une définition admise par les géomètres pour le cas où ce module est la première puissance ou même une puissance quelconque d'un nombre premier impair. D'ailleurs la détermination dont il s'agit se déduit aisément des propositions déjà établies, jointes à quelques autres théorèmes que nous allons énoncer.

THÉORÈME IX. — *Soient n un nombre premier et* X *une fonction entière de x, dans laquelle les coefficients numériques des diverses puissances de x se réduisent à des nombres entiers. Si l'on nomme r une racine de l'équivalence*

$$X \equiv 0 \pmod{n}, \tag{22}$$

et X_1 *un second polynome semblable au polynome* X, *mais du degré immédiatement inférieur; on pourra choisir ce second polynome de manière qu'on ait, pour toute valeur entière de x,*

$$X \equiv (x - r)X_1 \pmod{n}. \tag{23}$$

Démonstration. — En effet, soit R ce que devient X pour $x = r$. La différence $X - R$ sera divisible algébriquement par $x - r$, et le quotient sera un polynome X_1 semblable au polynome X, mais du degré immédiatement inférieur. Comme on aura d'ailleurs identiquement

$$X - R = (x - r)X_1,$$

et, de plus,

$$R \equiv 0 \pmod{n},$$

on en conclura, en attribuant à x une valeur entière quelconque,

$$X \equiv (x - r)X_1 \pmod{n}.$$

Corollaire I. — En vertu de la formule (23), l'équivalence (22), réduite à

$$(x - r)X_1 \equiv 0 \pmod{n},$$

se décomposera en deux autres, savoir :

$$x - r \equiv 0, \quad X_1 \equiv 0 \pmod{n}. \tag{24}$$

Il est d'ailleurs aisé de voir que le coefficient de la plus haute puissance de x restera le même dans les deux polynomes X, X_1. Cela posé, concevons que, ce coefficient étant premier au module n, la racine r se réduise à l'un des entiers inférieurs à ce module, et nommons

$$r, \quad r', \quad r'', \quad \ldots$$

les diverses racines de l'équivalence (22), représentées par divers entiers inférieurs à n. Une racine r' distincte de r, ne pouvant vérifier la première des formules (24), vérifiera nécessairement la seconde. Si d'ailleurs le polynome X est du premier degré ou de la forme $ax + b$, a étant premier à n, on aura

$$X_1 = a;$$

et, la seconde des formules (24) ne pouvant être vérifiée, l'équation (21) n'admettra point de racine distincte de r et inférieure à n. Si le polynome X est du second degré, alors, le polynome X_1 étant du premier degré, la seconde des formules (24) admettra une seule racine inférieure à n, et par suite l'équation (22) admettra au plus deux racines distinctes inférieures à n. En continuant ainsi à faire croître le degré du polynome X, on déduira évidemment des formules (24) la proposition suivante :

THÉORÈME X. — *Soient n un nombre premier et* X *une fonction entière de x, dans laquelle les coefficients numériques des diverses puissances de x se réduisent à des nombres entiers, le coefficient de la puissance la plus élevée étant premier au module n. Le degré du polynome* X *ne pourra être surpassé par le nombre des racines distinctes et inférieures à n qui vérifieront l'équivalence*

$$X \equiv 0 \pmod{n}.$$

Corollaire I. — Le module n étant un nombre premier, et I étant l'indicateur maximum relatif à ce module, chacun des nombres

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

inférieurs et premiers au module n, représentera une valeur de m

propre à vérifier la formule (20), et sera par conséquent une racine de l'équivalence

$$x^{\mathrm{I}} - 1 \equiv 0 \pmod{n}.$$

Donc, en vertu du théorème X, l'indicateur maximum I ne pourra être inférieur au nombre des entiers

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

c'est-à-dire au nombre

$$\mathrm{N} = n - 1;$$

et puisque, en vertu du théorème IV, joint au théorème de Fermat, I devra diviser ce même nombre, on aura nécessairement

$$\mathrm{I} = \mathrm{N} = n - 1. \tag{25}$$

Corollaire II. — La formule (25) s'étend au cas même où l'on aurait

$$n = 2$$

et par suite

$$\mathrm{I} = \mathrm{N} = 1.$$

Supposons maintenant que le module n cesse d'être un nombre premier; alors on établira facilement les propositions suivantes :

Théorème XI. — *ν étant un module quelconque, i un nombre entier, x une quantité entière qui vérifie l'équivalence*

$$x \equiv 1 \pmod{\nu}, \tag{26}$$

et z le quotient de $x - 1$ par ν, l'équation

$$x = 1 + \nu z$$

entraînera l'équivalence

$$x^i \equiv 1 + \nu i z \pmod{\nu^2}. \tag{27}$$

Démonstration. — En effet, dans le développement de

$$x^i = (1 + \nu z)^i,$$

tous les termes, à l'exception des deux premiers, seront divisibles par ν^2.

Corollaire I. — Si z ou i sont divisibles par ν, la formule (27) se réduira simplement à la suivante :

$$x^i \equiv 1 \pmod{\nu^2}. \tag{28}$$

Mais cette réduction ne pourra plus s'effectuer si z et i sont premiers à ν.

Corollaire II. — Si i est premier à ν, la valeur de x fournie par l'équation

$$x = 1 + \nu z$$

ne pourra vérifier la formule (28), à moins que z ne devienne divisible par ν, c'est-à-dire à moins que l'on n'ait

$$x \equiv 1 \pmod{\nu^2}. \tag{29}$$

Corollaire III. — Supposons que ν devienne un nombre premier, et que la quantité entière x soit équivalente à l'unité suivant le module ν, mais non suivant le module ν^2, en sorte que x vérifie la condition (26), sans vérifier la condition (29) : on ne pourra satisfaire à l'équivalence (28) qu'en attribuant à l'exposant i une valeur divisible par ν. Donc, parmi les puissances de x qui deviendront équivalentes à l'unité suivant le module ν^2, la moins élevée sera x^ν. En d'autres termes, ν sera l'indicateur correspondant au module

$$n = \nu^2$$

et à la base

$$x = 1 + \nu z,$$

tant que z restera premier à ν.

Corollaire IV. — Si, le module ν étant un nombre premier, la quantité

$$x = 1 + \nu z$$

devient positive et inférieure à ν^2, elle ne pourra être qu'un terme de la progression arithmétique

$$1, \quad 1 + \nu, \quad 1 + 2\nu, \quad \ldots, \quad 1 + (\nu - 1)\nu. \tag{30}$$

Or, comme le premier terme de cette progression vérifie seul la formule (29), il résulte du corollaire précédent que l'indicateur correspondant à l'un quelconque des autres termes et au module ν^2 sera le nombre premier ν.

Corollaire V. — Si, dans les formules (26), (28), (29), on remplace x par $\frac{x}{y}$, x et y désignant deux nombres entiers premiers à ν, ces formules deviendront

$$(31)\qquad \begin{cases} x \equiv y & (\text{mod. } \nu), \\ x^i \equiv y^i & (\text{mod. } \nu^2), \\ x \equiv y & (\text{mod. } \nu^2). \end{cases}$$

Donc, lorsque i sera premier à ν, non seulement les formules (26) et (28) entraîneront la formule (29); mais de plus les deux premières des formules (31) entraîneront la troisième, d'où il résulte qu'elles ne pourront subsister en même temps, si x, y sont tous deux positifs et inférieurs à ν^2.

Corollaire VI. — ν étant un nombre premier, r une racine primitive de ν et x l'une des quantités entières qui vérifient la formule

$$(32)\qquad x \equiv r \quad (\text{mod. } \nu),$$

nommons i l'indicateur correspondant à la base r et au module

$$n = \nu^2;$$

on aura

$$x^i \equiv 1 \quad (\text{mod. } \nu^2),$$

par conséquent

$$x^i \equiv 1 \quad (\text{mod. } \nu);$$

et, comme la formule (32) donnera

$$x^i \equiv r^i \quad (\text{mod. } \nu^2),$$

on aura encore

$$r^i \equiv 1 \quad (\text{mod. } \nu).$$

Donc, en vertu du théorème IV, i sera le nombre $\nu - 1$ qui représente l'indicateur correspondant au module ν et à la racine primitive r, ou

un multiple de ce nombre. Mais, d'autre part, l'indicateur i devra diviser le nombre N des entiers inférieurs et premiers à ν^2, savoir, le produit

$$N = \nu(\nu - 1).$$

Or, ν étant premier, les seuls multiples de $\nu - 1$ qui diviseront ce produit seront

$$\nu - 1 \quad \text{et} \quad N.$$

Donc, dans l'hypothèse admise, on aura

$$i = \nu - 1 \qquad \text{ou} \qquad i = N = \nu(\nu - 1).$$

Observons maintenant que, parmi les valeurs de x propres à vérifier la formule (32), celles qui seront positives et inférieures à ν^2 se réduiront aux termes de la progression arithmétique

$$(33)\qquad r, \quad r + \nu, \quad r + 2\nu, \quad \ldots, \quad r + (\nu - 1)\nu,$$

et qu'en vertu du corollaire précédent, si l'on désigne par x, y deux de ces termes, l'équation

$$x^i \equiv y^i \quad (\text{mod. } \nu^2)$$

ne pourra subsister, quand i sera premier à ν. Donc la valeur $\nu - 1$ de l'indicateur i ne pourra correspondre qu'à un seul des termes de la progression (33), et pour chacun des autres termes, on aura nécessairement $i = N$.

Corollaire VII. — Le module

$$n = \nu^2$$

étant le carré d'un nombre premier ν, un seul terme de la progression (33) peut représenter une racine de l'équation

$$(34)\qquad x^{\nu-1} \equiv 1 \quad (\text{mod. } \nu^2).$$

Pour chacun des autres, l'indicateur i acquiert la plus grande valeur N qu'il puisse atteindre, puisqu'il doit diviser N. Donc tous les termes de la progression (33) qui ne vérifient pas la condition (34) sont des

racines primitives de ν^2, et l'indicateur maximum I relatif au module ν^2 est

$$\text{I} = \text{N} = \nu(\nu - 1). \tag{35}$$

Corollaire VIII. — La formule (35) s'étend au cas même où l'on aurait

$$\nu = 2, \qquad n = \nu^2 = 4,$$

et par suite

$$\text{N} = 2.$$

On a donc, en prenant 4 pour module,

$$\text{I} = \text{N} = 2.$$

Alors aussi l'on obtient une seule racine primitive r inférieure à 4, savoir,

$$r = 3.$$

THÉORÈME XII. — *$\nu > 1$ étant un nombre premier et x une quantité entière qui vérifie l'équivalence*

$$x \equiv 1 \pmod{\nu};$$

si l'on représente par n la puissance la plus élevée de ν qui divise la différence

$$x - 1,$$

le produit $n\nu$ représentera la puissance la plus élevée de ν qui divisera la différence

$$x^\nu - 1,$$

à moins que l'on n'ait

$$n = \nu = 2.$$

Démonstration. — Nommons z le quotient de $x - 1$ par n. On aura

$$x = 1 + nz,$$

z étant, par hypothèse, premier à ν. Or, dans le développement de

$$x^\nu = (1 + nz)^\nu,$$

les termes extrêmes seront

$$1, \quad n^\nu z^\nu,$$

et tous les autres seront évidemment divisibles par le produit $n\nu$. D'ailleurs, ν étant facteur de n, le terme

$$n^\nu z^\nu = n.n^{\nu-1}z^\nu$$

sera lui-même divisible par le produit $n\nu$. Donc ce produit divisera la différence

$$x^\nu - 1.$$

Il y a plus, ν étant un facteur de n, ν^2 sera un facteur de $n^{\nu-1}$, à moins que l'on n'ait

$$n = \nu = 2; \tag{36}$$

et, par suite, si la condition (36) n'est pas remplie, tous les termes qui suivront les deux premiers dans le développement de

$$(1 + nz)^\nu$$

seront divisibles ou par $n^2\nu$ ou au moins par $n\nu^2$. On aura donc alors

$$x^\nu \equiv 1 + n\nu z \pmod{n\nu^2}.$$

Donc, z étant premier à ν, le produit $n\nu$ sera la puissance la plus élevée de ν qui divise la différence

$$x^\nu - 1.$$

Corollaire I. — Si, dans le théorème XII, on remplace successivement x par x^ν, puis par x^{ν^2}, etc., on en conclura que, dans l'hypothèse admise, les puissances les plus élevées de ν, propres à diviser les différences

$$x^\nu - 1, \quad x^{\nu^2} - 1, \quad x^{\nu^3} - 1, \quad \ldots,$$

sont respectivement

$$n\nu, \quad n\nu^2, \quad n\nu^3, \quad \ldots.$$

On doit toujours excepter le cas où l'on aurait $n = \nu = 2$.

Corollaire II. — En remplaçant dans le corollaire précédent x par x^i,

on obtiendra une proposition dont voici l'énoncé : Si, $\nu > 1$ étant un nombre premier, on représente par n la plus élevée des puissances de ν qui divisent

$$x^{i} - 1,$$

alors les puissances les plus élevées de ν qui diviseront les différences

$$x^{i\nu} - 1, \quad x^{i\nu^2} - 1, \quad x^{i\nu^3} - 1, \quad \ldots$$

seront respectivement

$$n\nu, \quad n\nu^2, \quad n\nu^3, \quad \ldots,$$

à moins que l'on n'ait $n = \nu = 2$.

Corollaire III. — ν étant un nombre premier impair, et r une racine primitive de ν^2, la puissance

$$r^{\nu-1} - 1$$

sera divisible une seule fois par ν. Donc, en vertu du corollaire II, les puissances les plus élevées de ν qui diviseront les différences

$$r^{\nu(\nu-1)} - 1, \quad r^{\nu^2(\nu-1)} - 1, \quad r^{\nu^3(\nu-1)} - 1, \quad \ldots$$

seront respectivement

$$\nu^2, \quad \nu^3, \quad \nu^4, \quad \ldots.$$

Donc

$$r^{\nu^3(\nu-1)}$$

sera le premier des termes de la suite

$$(37) \qquad r^{\nu-1}, \quad r^{\nu(\nu-1)}, \quad r^{\nu^2(\nu-1)}, \quad r^{\nu^3(\nu-1)}, \quad \ldots$$

qui seront équivalents à l'unité, suivant le module ν^3. D'autre part, si l'on nomme i l'indicateur correspondant à la base r et au module ν^3, on aura

$$r^{i} \equiv 1 \pmod{\nu^3},$$

et à plus forte raison

$$r^{i} \equiv 1 \pmod{\nu};$$

d'où il résulte que i devra être un multiple de l'indicateur $\nu - 1$ correspondant à la base r et au module ν. Donc i, qui devra en outre

diviser le produit

$$N = \nu^{3-1}(\nu - 1),$$

représentera l'exposant de r dans le premier des termes de la suite (37) qui seront équivalents à l'unité suivant le module ν^3. On aura donc nécessairement

$$i = N = \nu^{3-1}(\nu - 1).$$

Cette dernière valeur de i étant la plus grande que puisse acquérir un indicateur relatif au module ν^3, nous devons conclure, des observations précédentes, qu'une racine primitive r de ν^2 sera en même temps une racine primitive de ν^3, et que, dans le cas où le module

$$n = \nu^3$$

se réduit à une puissance d'un nombre premier impair, l'indicateur maximum I est déterminé par la formule

$$(38) \qquad I = N = \nu^{3-1}(\nu - 1).$$

Corollaire IV. — Considérons en particulier le cas où l'on aurait

$$n = \nu = 2,$$

et supposons en conséquence la différence

$$x - 1$$

divisible une seule fois par le module 2. La différence

$$x^2 - 1 = (x - 1)(x + 1)$$

sera composée de deux facteurs $x - 1$, $x + 1$, divisibles l'un par 2, l'autre par 4. Elle sera donc divisible au moins par le nombre 8, c'est-à-dire par le cube de 2. Cela posé, nommons n la plus haute puissance de 2 qui divisera $x^2 - 1$. En vertu du corollaire II, les puissances les plus élevées de 2 qui diviseront les différences

$$x^{2i} - 1, \quad x^{2i^2} - 1, \quad \ldots$$

seront respectivement

$$2n, \quad 2^2 n, \quad \ldots.$$

Donc, si a surpasse 2, le premier terme de la suite

$$x^2,\quad x^{2^2},\quad x^{2^3},\quad \ldots,$$

qui deviendra équivalent à l'unité suivant le module 2^a, sera

$$x^i,$$

la valeur de i étant

$$i = \frac{2^{a+1}}{n}. \tag{39}$$

D'autre part, l'indicateur correspondant à la base x et au module 2^a devra être un diviseur de

$$N = 2^{a-1}.$$

Il se trouvera donc compris dans la suite

$$2,\quad 2^2,\quad 2^3,\quad \ldots,$$

et ne pourra être que la valeur précédente de i. Cette même valeur deviendra la plus grande possible, lorsque le nombre n se réduira simplement à 8, ce qui arrivera si l'on prend

$$x = 3 \quad \text{ou} \quad x = 5,$$

puisqu'on a

$$3^2 - 1 = 8 \quad \text{et} \quad 5^2 - 1 = 3.8.$$

Par conséquent

$$I = \frac{1}{2}N = 2^{a-2} \tag{40}$$

sera l'indicateur maximum relatif au module

$$n = 2^a > 4.$$

La formule (40) s'étend au cas même où l'on aurait $a = 3$, et donne alors, comme on devait s'y attendre,

$$I = \frac{1}{2}N = 2,$$

A l'aide des diverses propositions que nous venons de rappeler, et qui pour la plupart étaient déjà connues (*voir* les *Recherches arithmétiques* de M. Gauss et le *Canon arithmeticus* de M. Jacobi), il nous sera maintenant facile de résoudre la question suivante :

Problème II. — *Trouver l'indicateur maximum* I *correspondant à un module donné n.*

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

Si le module n est un nombre premier ν, ou une puissance d'un nombre premier impair, ou l'une des deux premières puissances de 2, alors, en nommant N le nombre des entiers inférieurs à n et premiers à n, on aura généralement, d'après ce qui a été dit ci-dessus,

$$I = N = n\left(1 - \frac{1}{\nu}\right);$$

et, en particulier, si n se réduit à 2 ou 4,

$$I = N = \frac{1}{2}n.$$

Si le module n est une puissance de 2 supérieure à la seconde, on aura simplement

$$I = \frac{1}{2}N = \frac{1}{4}n.$$

Enfin, si le module n est un nombre quelconque, on pourra le décomposer en facteurs

$$n_1,\quad n_2,\quad \ldots,$$

dont chacun soit un nombre premier ou une puissance d'un nombre premier. Soient alors

$$I_1,\quad I_2,\quad \ldots$$

les indicateurs maxima correspondant aux modules

$$n_1,\quad n_2,\quad \ldots.$$

En vertu des théorèmes III et V, une base donnée r sera une racine

primitive de n, si cette base, divisée successivement par chacun des nombres n_1, n_2, ..., fournit pour restes des racines primitives de ces mêmes nombres; et I sera le plus petit nombre entier divisible à la fois par chacun des indicateurs

$$I_1, \quad I_2, \quad \ldots.$$

La solution du problème précédent fournit, pour la résolution des équivalences du premier degré, une règle très simple qui se réduit à la règle donnée par M. Libri et par M. Binet, dans le cas particulier où le module est un nombre premier. La nouvelle règle, d'après ce que nous a dit M. Poinsot, coïncide, au moins lorsque le module est pair, avec celle que lui-même avait indiquée dans la Note manuscrite, remise à M. Legendre. Appliquée au cas où l'on prend pour module un nombre composé, elle n'exige pas, comme les méthodes présentées par M. Libri et M. Binet, la décomposition de ce module en facteurs premiers; et ce qu'il y a de remarquable, c'est qu'alors l'application devient d'autant plus facile que le module est un nombre plus composé. Montrons la vérité de cette assertion par quelques exemples.

Pour que toute équation indéterminée à deux inconnues puisse être résolue immédiatement à la seule inspection des coefficients de ces inconnues, dans le cas où l'un des coefficients ne dépasse pas 1000, il suffit que l'on construise une Table qui, pour tout module renfermé entre les limites 1 et 1000, fournisse l'indicateur correspondant à ce module. Or, à l'aide de cette Table, dont la construction est facile (*voir* la solution du problème II), et que nous donnons à la suite de ce Mémoire, on reconnaît que l'indicateur 2 correspond aux modules

$$3, \quad 4, \quad 6, \quad 8, \quad 12, \quad 24.$$

Donc, pour chacun de ces modules, l'inverse d'un nombre donné est équivalent à ce nombre même.

Ainsi, en particulier, l'inverse du nombre 19 suivant le module 24 est équivalent à 19. En d'autres termes, 19 est une des valeurs entières

de x qui vérifient l'équation indéterminée

$$19x - 24y = 1.$$

Effectivement, le carré de 19 ou 361, divisé par 24, donne 1 pour reste.

De ce que l'indicateur 4 correspond aux modules

$$5, \quad 10, \quad 15, \quad 16, \quad 20, \quad 30, \quad 40, \quad 48, \quad 60, \quad 80, \quad 120, \quad 240,$$

il résulte immédiatement que, pour chacun de ces modules, l'inverse d'un nombre donné est équivalent au cube de ce même nombre. Ainsi, en particulier, l'inverse du nombre 67, suivant le module 120, est équivalent au cube de 67, par conséquent au produit de 67 par 49, ou à 43. En d'autres termes, 43 est une des valeurs de x qui vérifient l'équation

$$67x - 120y = 1.$$

Effectivement,

$$67 \times 43 = 2881 = 24 \times 120 + 1.$$

De ce que l'indicateur 6 correspond aux modules

$$7, \quad 9, \quad 14, \quad 18, \quad 21, \quad 28, \quad 36, \quad 42, \quad 56, \quad 63, \quad 72, \quad 84, \quad 168, \quad 504,$$

il résulte immédiatement que, pour chacun de ces modules, l'inverse d'un nombre donné est équivalent à la cinquième puissance de ce nombre. Ainsi, en particulier, l'inverse du nombre 17 sera équivalent, suivant le module 504, à

$$17^5 = 1419857,$$

par conséquent à 89. En d'autres termes, 89 est une valeur de x propre à vérifier l'équation indéterminée

$$17x - 504y = 1.$$

Effectivement,

$$17 \times 89 = 1513 = 3 \times 504 + 1.$$

Comme, dans la méthode ci-dessus exposée, la valeur de x est toujours exprimée par une puissance connue du nombre donné, le calcul pourra s'exécuter commodément, à l'aide des Tables de logarithmes, même quand l'indicateur sera composé de plusieurs chiffres.

Supposons, pour fixer les idées, que, le nombre donné étant 29, on demande un autre nombre équivalent à l'inverse du premier, suivant le module 192. L'indicateur étant alors égal à 16, le nombre cherché sera

$$29^{15} = (29^5)^3.$$

D'ailleurs les sept premiers chiffres de la valeur approchée de 29^5, déterminés à l'aide des Tables de logarithmes, sont ceux que présente le nombre

$$2051115,$$

attendu que l'on a

$$5 \log 29 = 7,3119900.$$

De plus, le dernier chiffre de 29^5, comme celui de 9^5, sera nécessairement 9. On aura donc par suite

$$29^5 = 2051114\,9 \equiv 173 \equiv -19 \pmod{192},$$
$$29^{15} \equiv -19^3 \pmod{192};$$

puis, en se servant de nouveau des Tables de logarithmes,

$$29^{15} \equiv -6859 \equiv -139 \equiv 53 \pmod{192}.$$

Donc, 29^{15} et 53 seront deux valeurs de x propres à vérifier la formule

$$29x - 192y = 1.$$

Effectivement,

$$29 \times 53 = 1537 = 8 \times 192 + 1.$$

Table pour la détermination de l'indicateur maximum I *correspondant à un module donné n.*

n	I	n	I	n	I	n	I	n	I	n	I	n	I	n	I
		26	12	51	16	76	18	101	100	126	6	151	150	176	20
2	1	27	18	52	12	77	30	102	16	127	126	152	18	177	58
3	2	28	6	53	52	78	12	103	102	128	32	153	48	178	88
4	2	29	28	54	18	79	78	104	12	129	42	154	30	179	178
5	4	30	4	55	20	80	4	105	12	130	12	155	60	180	12
6	2	31	30	56	6	81	54	106	52	131	130	156	12	181	180
7	6	32	8	57	18	82	40	107	106	132	10	157	156	182	12
8	2	33	10	58	28	83	82	108	18	133	18	158	78	183	60
9	6	34	16	59	58	84	6	109	108	134	66	159	52	184	22
10	4	35	12	60	4	85	16	110	20	135	36	160	8	185	36
11	10	36	6	61	60	86	42	111	36	136	16	161	66	186	30
12	2	37	36	62	30	87	28	112	12	137	136	162	54	187	80
13	12	38	18	63	6	88	10	113	112	138	22	163	162	188	46
14	6	39	12	64	16	89	88	114	18	139	138	164	40	189	18
15	4	40	4	65	12	90	12	115	44	140	12	165	20	190	36
16	4	41	40	66	10	91	12	116	28	141	46	166	82	191	190
17	16	42	6	67	66	92	22	117	12	142	70	167	166	192	16
18	6	43	42	68	16	93	30	118	58	143	60	168	6	193	192
19	18	44	10	69	22	94	46	119	48	144	12	169	156	194	96
20	4	45	12	70	12	95	36	120	4	145	28	170	16	195	12
21	6	46	22	71	70	96	8	121	110	146	72	171	18	196	42
22	10	47	46	72	6	97	96	122	60	147	42	172	42	197	196
23	22	48	4	73	72	98	42	123	40	148	36	173	172	198	30
24	2	49	42	74	36	99	30	124	30	149	148	174	28	199	198
25	20	50	20	75	20	100	20	125	100	150	20	175	60	200	20

Table pour la détermination de l'indicateur maximum I *correspondant à un module donné n.*

n	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I
201	66	226	112	251	250	276	22	301	42	326	162	351	36	376	46
202	100	227	226	252	6	277	276	302	150	327	108	352	40	377	84
203	84	228	18	253	110	278	138	303	100	328	40	353	352	378	18
204	16	229	228	254	126	279	30	304	36	329	138	354	58	379	378
205	40	230	44	255	16	280	12	305	60	330	20	355	140	380	36
206	102	231	30	256	64	281	280	306	48	331	330	356	88	381	126
207	66	232	28	257	256	282	46	307	306	332	82	357	48	382	190
208	12	233	232	258	42	283	282	308	30	333	36	358	178	383	382
209	90	234	12	259	36	284	70	309	102	334	166	359	358	384	32
210	12	235	92	260	12	285	36	310	60	335	132	360	12	385	60
211	210	236	58	261	84	286	60	311	310	336	12	361	342	386	192
212	52	237	78	262	130	287	120	312	12	337	336	362	180	387	42
213	70	238	48	263	262	288	24	313	312	338	156	363	110	388	96
214	106	239	238	264	10	289	272	314	156	339	112	364	12	389	388
215	84	240	4	265	52	290	28	315	12	340	16	365	72	390	12
216	18	241	240	266	18	291	96	316	78	341	30	366	60	391	176
217	30	242	110	267	88	292	72	317	316	342	18	367	366	392	42
218	108	243	162	268	66	293	292	318	52	343	294	368	44	393	130
219	72	244	60	269	268	294	42	319	140	344	42	369	120	394	196
220	20	245	84	270	36	295	116	320	16	345	44	370	36	395	156
221	48	246	40	271	270	296	36	321	106	346	172	371	156	396	30
222	36	247	36	272	16	297	90	322	66	347	346	372	30	397	396
223	222	248	30	273	12	298	148	323	144	348	28	373	372	398	198
224	24	249	82	274	136	299	132	324	54	349	348	374	80	399	18
225	60	250	100	275	20	300	20	325	60	350	60	375	100	400	20

Table pour la détermination de l'indicateur maximum I *correspondant à un module donné n.*

n	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I
401	400	426	70	451	40	476	48	501	166	526	262	551	252	576	48
402	66	427	60	452	112	477	156	502	250	527	240	552	22	577	576
403	60	428	106	453	150	478	238	503	502	528	20	553	78	578	272
404	100	429	60	454	226	479	478	504	6	529	506	554	276	579	192
405	108	430	84	455	12	480	8	505	100	530	52	555	36	580	28
406	84	431	430	456	18	481	36	506	110	531	174	556	138	581	246
407	180	432	36	457	456	482	240	507	156	532	18	557	556	582	96
408	16	433	432	458	228	483	66	508	126	533	120	558	30	583	260
409	408	434	30	459	144	484	110	509	508	534	88	559	84	584	72
410	40	435	28	460	44	485	96	510	16	535	212	560	12	585	12
411	136	436	108	461	460	486	162	511	72	536	66	561	80	586	292
412	102	437	198	462	30	487	486	512	128	537	178	562	280	587	586
413	174	438	72	463	462	488	60	513	18	538	268	563	562	588	42
414	66	439	438	464	28	489	162	514	256	539	210	564	46	589	90
415	164	440	20	465	60	490	84	515	204	540	36	565	112	590	116
416	24	441	42	466	232	491	490	516	42	541	540	566	282	591	196
417	138	442	43	467	466	492	40	517	230	542	270	567	54	592	36
418	90	443	442	468	12	493	112	518	36	543	180	568	70	593	592
419	418	444	36	469	66	494	36	519	172	544	16	569	568	594	90
420	12	445	88	470	92	495	60	520	12	545	108	570	36	595	48
421	420	446	222	471	156	496	60	521	520	546	12	571	570	596	148
422	210	447	148	472	58	497	210	522	84	547	546	572	60	597	198
423	138	448	48	473	210	498	82	523	522	548	136	573	190	598	132
424	52	449	448	474	78	499	498	524	130	549	60	574	120	599	598
425	80	450	60	475	180	500	100	525	60	550	20	575	220	600	20

Table pour la détermination de l'indicateur maximum I *correspondant à un module donné n.*

n	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I
601	600	626	312	651	30	676	156	701	700	726	110	751	750	776	96
602	42	627	90	652	162	677	676	702	36	727	726	752	92	777	36
603	66	628	156	653	652	678	112	703	36	728	12	753	250	778	388
604	150	629	144	654	108	679	96	704	80	729	486	754	84	779	360
605	20	630	12	655	260	680	16	705	235	730	72	755	300	780	12
606	100	631	630	656	40	681	226	706	352	731	336	756	18	781	70
607	606	632	78	657	72	682	30	707	300	732	60	757	756	782	176
608	72	633	210	658	138	683	682	708	58	733	732	758	378	783	252
609	84	634	316	659	658	684	18	709	708	734	366	759	110	784	84
610	60	635	252	660	20	685	136	710	140	735	84	760	36	785	156
611	276	636	52	661	660	686	294	711	78	736	88	761	760	786	130
612	48	637	84	662	330	687	228	712	88	737	330	762	126	787	786
613	612	638	140	663	48	688	84	713	330	738	120	763	108	788	196
614	306	639	210	664	82	689	156	714	48	739	738	764	190	789	262
615	40	640	32	665	36	690	44	715	60	740	36	765	48	790	156
616	30	641	640	666	36	691	690	716	178	741	36	766	382	791	336
617	616	642	106	667	308	692	172	717	238	742	156	767	348	792	30
618	102	643	642	668	166	693	30	718	358	743	742	768	64	793	60
619	618	644	66	669	222	694	346	719	718	744	30	769	768	794	396
620	60	645	84	670	132	695	276	720	12	745	148	770	60	795	52
621	198	646	144	671	60	696	28	721	102	746	372	771	256	796	198
622	310	647	646	672	24	697	80	722	342	747	246	772	192	797	796
623	264	648	54	673	672	698	348	723	240	748	80	773	772	798	18
624	12	649	290	674	337	699	232	724	180	749	318	774	42	799	368
625	500	650	60	675	180	700	60	725	140	750	100	775	60	800	40

Table pour la détermination de l'indicateur maximum I *correspondant à un module donné n.*

n	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I	*n*	I
801	264	826	174	851	396	876	72	901	208	926	462	951	316	976	60
802	400	827	826	852	70	877	876	902	40	927	102	952	48	977	976
803	360	828	66	853	852	878	438	903	42	928	56	953	952	978	162
804	66	829	828	854	60	879	292	904	112	929	928	954	156	979	440
805	132	830	164	855	36	880	20	905	180	930	60	955	380	980	84
806	60	831	276	856	106	881	880	906	150	931	126	956	238	981	108
807	268	832	48	857	856	882	42	907	906	932	232	957	140	982	490
808	100	833	336	858	60	883	882	908	226	933	310	958	478	983	982
809	808	834	138	859	858	884	48	909	300	934	466	959	408	984	40
810	108	835	332	860	215	885	116	910	12	935	80	960	16	985	196
811	810	836	90	861	120	886	442	911	910	936	12	961	930	986	112
812	84	837	90	862	430	887	886	912	36	937	936	962	36	987	138
813	270	838	418	863	862	888	36	913	410	938	66	963	318	988	36
814	180	839	838	864	72	889	126	914	456	939	312	964	240	989	462
815	324	840	12	865	172	890	88	915	60	940	92	965	192	990	60
816	16	841	812	866	432	891	270	916	228	941	940	966	66	991	990
817	126	842	420	867	272	892	222	917	390	942	156	967	966	992	120
818	408	843	280	868	30	893	414	918	144	943	440	968	110	993	330
819	12	844	210	869	390	894	148	919	918	944	116	969	144	994	210
820	40	845	156	870	28	895	356	920	44	945	12	970	96	995	198
821	820	846	138	871	66	896	96	921	306	946	210	971	970	996	82
822	136	847	330	872	108	897	132	922	460	947	946	972	162	997	996
823	822	848	52	873	96	898	448	923	70	948	78	973	138	998	498
824	102	849	282	874	198	899	420	924	30	949	72	974	486	999	36
825	20	850	80	875	300	900	60	925	180	950	180	975	60	1000	100