ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

T.-J. STIELTJES

# Étude bibliographique. Sur la théorie des nombres

*Annales de la faculté des sciences de Toulouse 1re série*, tome 4, nº 3 (1890), p. 1-103
<http://www.numdam.org/item?id=AFST_1890_1_4_3_1_0>

© Université Paul Sabatier, 1890, tous droits réservés.

L'accès aux archives de la revue « Annales de la faculté des sciences de Toulouse » (http://picard.ups-tlse.fr/~annales/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
*Article numérisé dans le cadre du programme*
*Numérisation de documents anciens mathématiques*
http://www.numdam.org/

# ÉTUDE BIBLIOGRAPHIQUE.

SUR LA

# THÉORIE DES NOMBRES,

PAR M. T.-J. STIELTJES,

Professeur à la Faculté des Sciences de Toulouse.

## CHAPITRE I.

### SUR LA DIVISIBILITÉ DES NOMBRES.

1. L'idée de nombre a son origine dans la considération de plusieurs objets distincts.

C'est une notion qui s'attache à cette considération, où l'on fait abstraction de la nature des objets, et qui est, d'après notre conviction intime, indépendante de l'ordre dans lequel on envisage successivement les objets donnés.

Ce dernier point est essentiel et constitue, à proprement dire, le seul axiome de toute la science des nombres. Peut-être même est-il possible de ramener cet axiome à quelque chose de plus simple encore.

Si l'on se rappelle, en effet, que l'on peut passer d'une permutation à une autre par une série de transpositions opérées sur deux éléments voisins, il semble qu'au fond il suffit d'adopter l'axiome dans le cas de deux objets.

Mais, sans insister sur cette question, nous nous bornerons à observer que les relations exprimées par les équations

$$a+b=b+a, \qquad a+b+c=a+(b+c), \qquad \ldots,$$
$$abc=bac=c(ab), \qquad \ldots,$$
$$a(b+c)=ab+ac, \qquad \ldots,$$

doivent être considérées comme des théorèmes qui découlent de l'axiome fondamental qui donne naissance à l'idée de nombre.

2. En comparant un nombre $a$ avec les multiples $0, b, 2b, \ldots$ d'un second nombre $b$, deux cas peuvent se présenter. Ou bien $a$ est égal à un multiple de $b$, alors $a$ est divisible par $b$, $b$ un diviseur de $a$, ou bien le nombre $a$ tombe entre deux multiples consécutifs de $b$. Dans ce dernier cas, il existe un nombre $m$ tel que $a = mb + c$, $c$ étant positif, mais inférieur à $b$.

3. Étant donnés plusieurs nombres $a, b, c, \ldots, l$, on peut toujours trouver des nombres qui sont en même temps divisibles par $a$, par $b$, ..., par $l$. Parmi ces nombres qu'on appelle *communs multiples* de $a, b, c, \ldots, l$, il y en a un nécessairement qui est le plus petit et qui s'appelle le *plus petit commun multiple* des nombres $a, b, c, \ldots, l$.

Théorème I. — *Le plus petit commun multiple $m$ des nombres $a, b, c, \ldots, l$ divise exactement tout autre commun multiple* M *de ces nombres.*

En effet, si M n'était pas un multiple de $m$, la division de M par $m$ donnerait lieu à une relation

$$\mathrm{M} = km + m',$$

où $m'$ serait positif, mais inférieur à $m$. Or on reconnaît immédiatement que $m'$ serait encore un commun multiple de $a, b, c, \ldots, l$, ce qui est absurde, puisqu'on suppose qu'il n'existe pas un tel commun multiple inférieur à $m$.

Il est clair qu'on peut énoncer ce théorème encore de cette manière :

Théorème I$^a$. — *Si un nombre* M *admet pour diviseurs les nombres $a, b, c, \ldots, l$, le plus petit commun multiple de $a, b, c, \ldots, l$ sera encore un diviseur de* M.

4. Le plus petit commun multiple des nombres

$$a > b > c > \ldots > l$$

est évidemment au moins égal à $a$, et il ne peut être égal à $a$ que dans le cas où $b, c, \ldots, l$ sont des diviseurs de $a$.

5. Un nombre qui divise à la fois $a, b, c, \ldots, l$ s'appelle un *commun diviseur* de ces nombres. Parmi ces communs diviseurs, il y en a nécessairement un, plus grand que les autres, et qui s'appelle le *plus grand commun diviseur* de $a, b, c, \ldots, l$.

Théorème II. — *Le plus grand commun diviseur $\delta$ des nombres $a, b, c, \ldots, l$ est un multiple de tout autre commun diviseur $\delta'$ de ces nombres.*

Soient, en effet, $\delta, \delta', \delta'', \ldots$ les communs diviseurs des nombres donnés.

Puisque $a$ est divisible par $\delta, \delta', \delta'', \ldots$, il est encore divisible par le plus petit commun multiple de $\delta, \delta', \delta'', \ldots$, et il en est de même pour $b, c, \ldots, l$. Par conséquent, le plus petit commun multiple de $\delta, \delta', \delta'', \ldots$ est encore un commun diviseur de $a, b, c, \ldots, l$. Ce plus petit commun multiple est donc nécessairement égal à $\delta$, et $\delta', \delta'', \ldots$ sont les diviseurs de $\delta$. L'ensemble des communs diviseurs de $a, b, c, \ldots, l$ est identique avec l'ensemble des diviseurs de $\delta$.

6. Pour chercher le p. g. c. d. (p. p. c. m.) de $a, b, c, \ldots, l$, on peut diviser ces nombres en divers groupes, chercher le p. g. c. d. (p. p. c. m.) des nombres contenus dans ces groupes, ensuite le p. g. c. d. (p. p. c. m.) des nombres ainsi obtenus.

On pourra donc ramener le problème toujours au cas où il n'y a que deux nombres $a$ et $b$, et, dans ce cas, l'algorithme d'Euclide conduit de la façon la plus simple à la connaissance du p. g. c. d. Par une suite de divisions, on obtient les relations

$$\begin{aligned}
a &= qb &&+ r,\\
b &= q'r &&+ r',\\
r &= q''r' &&+ r'',\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
r^{(k-1)} &= q^{(k+1)} r^{(k)} &&+ r^{(k+1)},\\
r^{(k)} &= q^{(k+2)} r^{(k+1)},
\end{aligned}$$

et $r^{(k+1)}$ est le p. g. c. d. de $a$ et $b$.

Soit $\delta$ le p. g. c. d. de $a, b, c, \ldots, l$, alors les nombres $ma, mb, \ldots, ml$ sont tous divisibles par $m\delta$, leur p. g. c. d. est donc nécessairement divisible par $m\delta$, mais on reconnaît immédiatement que ce p. g. c. d. est exactement $m\delta$.

Pour abréger, nous emploierons quelquefois les symboles

$$(a, b, c, \ldots, l),$$
$$|a, b, c, \ldots, l|$$

pour désigner respectivement le p. g. c. d. et le p. p. c. m. de $a, b, \ldots, l$.

On a donc

$$(ma, mb, \ldots, ml) = m \times (a, b, \ldots, l)$$

et de même

$$|ma, mb, \ldots, ml| = m \times |a, b, \ldots, l|.$$

De là on peut conclure le lemme suivant qui est souvent utile.

Lemme. — *Soient $d$ le p. g. c. d. (p. p. c. m.) des $\alpha$ nombres*

$$a, \quad a', \quad a'', \quad \ldots,$$

*e le p. g. c. d. (p. p. c. m.) des* $\beta$ *nombres*

$$b, \quad b', \quad b'', \quad \ldots,$$

*alors le p. g. c. d. (p. p. c. m.) des* $\alpha\beta$ *produits*

$$ab, \quad ab', \quad ab'', \quad \ldots, \qquad a'b, \quad a'b', \quad \ldots, \qquad a''b, \quad a''b', \quad \ldots$$

*est de.*

En effet, les p. g. c. d. (p. p. c. m.) des divers groupes

$$\begin{array}{llll} ab, & ab', & ab'' & \ldots, \\ a'b, & a'b', & a'b'', & \ldots, \\ a''b, & a''b', & a''b'', & \ldots, \\ \ldots, & \ldots, & \ldots, & \ldots \end{array}$$

sont respectivement $ae$, $a'e$, $a''e$, ..., et le p. g. c. d. (p. p. c. m.) de ces derniers nombres est $de$.

7. La recherche du p. p. c. m. peut se ramener toujours à celle du p. g. c. d., et réciproquement.

Le p. p. c. m. de $a$, $b$, $c$ est de la forme

$$\frac{abc}{d} = a \times \frac{bc}{d} = b \times \frac{ca}{d} = c \times \frac{ab}{d},$$

donc $d$ doit être un commun diviseur de $bc$, $ca$, $ab$. Pour avoir le p. p. c. m., il faut évidemment prendre pour $d$ le p. g. c. d. de $bc$, $ca$, $ab$.

Théorème III. — *Le p. p. c. m. (p. g. c. d.) de* $a, b, c, \ldots, l$ *est égal au produit* $abc\ldots l$ *divisé par le p. g. c. d. (p. p. c. m.) des produits*

$$bc\ldots l, \quad ac\ldots l, \quad \ldots, \quad abc\ldots k.$$

8. Dans le cas de deux nombres $a$ et $b$, le produit du p. g. c. d. et du p. p. c. m. est $ab$. Cette relation n'a plus lieu dans le cas où l'on a $n$ nombres. Cependant on peut rétablir l'analogie, et il faut, pour cela, considérer, non seulement le p. g. c. d. et le p. p. c. m., mais une suite de $n$ nombres qui dérivent d'une façon particulière des nombres donnés.

Nous allons entrer dans quelques détails sur cette théorie, comprise dans des recherches plus générales de M. Smyth dont nous aurons à parler plus loin.

Considérons $n$ nombres

$$\text{(A)} \qquad a, \quad b, \quad c, \quad \ldots, \quad l.$$

Prenons deux nombres, par exemple $a$ et $b$, de ce système et remplaçons-les par leur p. g. c. d. et leur p. p. c. m. On aura ainsi un second système $(A_1)$

$$a', \quad b', \quad c, \quad \ldots, \quad l.$$

En répétant la même opération sur $(A_1)$ pour en déduire un système $(A_2)$, puis un système $(A_3)$, ..., on finira toujours par obtenir un système dans lequel deux nombres quelconques sont eux-mêmes leur p. g. c. d. et p. p. c. m., c'est-à-dire l'un de ces nombres divise l'autre. Si l'on ordonne les nombres de ce système définitif par ordre de grandeur croissante

$$e_1, \quad e_2, \quad e_3, \quad \ldots, \quad e_n,$$

$e_k$ divise $e_{k+1}$, et nous dirons que ces nombres forment le système *réduit*, $e_k$ est le $k^{\text{ième}}$ nombre réduit. En effet, on verra que ce système réduit est unique et indépendant de la manière dont on a dirigé les opérations.

9. Pour faciliter un peu le langage, nous dirons que deux nombres forment un couple réduit lorsque l'un de ces nombres divise l'autre. Il est clair que, si $a$ et $b$ sont un couple réduit, les groupes (A) et $(A_1)$ sont identiques; on peut donc se dispenser de combiner les couples réduits. Si tous les couples de (A) étaient réduits, ce groupe serait déjà le système réduit.

Nous allons faire voir qu'en combinant deux nombres qui ne forment pas un couple réduit, on augmente toujours le nombre total des couples réduits.

Considérons, pour cela, les divers couples réduits de (A). On peut distinguer les quatre catégories suivantes :

1° Les couples réduits $f$, $g$ qui ne renferment ni $a$, ni $b$. Il est bien clair que ces couples réduits se retrouvent dans $(A_1)$.

2° Les couples réduits $a$, $f$ qui renferment le nombre $a$ et qui sont tels que $b$, $f$ n'est pas un couple réduit. Dans ce cas, au moins un des couples $a'$, $f$ et $b'$, $f$ sera réduit, et ils peuvent l'être tous les deux. En effet, si $f$ divise $a$, il est clair qu'il divise aussi $b'$, et, si $f$ est multiple de $a$, il sera aussi multiple de $a'$. [On suppose $a' = (a, b)$, $b' = |a, b|$.]

3° Les couples réduits $b$, $f$ qui renferment le nombre $b$ et qui sont tels que $a$, $f$ n'est pas un couple réduit. Il est clair que ce que nous venons de dire pour le second cas s'applique encore ici.

4° Les couples réduits $a$, $f$ qui sont tels que $b$, $f$ est en même temps un couple réduit. Dans ce cas, on reconnaît facilement que les couples $a'$, $f$ et $b'$, $f$ sont aussi réduits tous les deux. Il suffit d'examiner successivement les trois hypothèses possibles : $f$ divise $a$ et $b$; $f$ est multiple de $a$ et de $b$; $f$ divise l'un des nombres $a$, $b$ et est multiple de l'autre.

Nous avons ainsi énuméré déjà dans le système $(A_1)$ au moins autant de couples réduits que dans (A). Mais le système $(A_1)$ renferme encore le couple réduit $a'$, $b'$, par conséquent le nombre des couples réduits du système $(A_1)$ surpasse au moins d'une unité le nombre des couples réduits de (A).

Par un nombre fini d'opérations, on arrivera donc nécessairement à un groupe de $n$ nombres dont tous les couples sont des couples réduits, et qui est ainsi le système réduit. Il reste à faire voir que ce système réduit est unique.

**10.** On constate d'abord qu'en remplaçant $a$ et $b$ par $a'$ et $b'$, on ne change ni le p. g. c. d., ni le p. p. c. m. des nombres du système.

Envisageons maintenant les divers produits $k$ à $k$ des nombres (A), pour voir quelles modifications résultent, pour ces produits, par le remplacement de $a$ et $b$ par $a'$ et $b'$.

Les divers produits $k$ à $k$ se composent :

1° Des produits qui ne renferment ni $a$, ni $b$;
2° Des produits qui renferment $a$ et $b$;
3° Des produits qui renferment un seul des nombres $a$ et $b$.

Il est clair que ce sont les derniers produits seulement qui sont affectés par le remplacement de $a$ et $b$ par $a'$ et $b'$. Ces produits sont, d'ailleurs, en nombre pair et peuvent être écrits ainsi

$$\begin{array}{llllll} aP, & aP', & aP'', & aP''', & \ldots, \\ bP, & bP', & bP'', & bP''', & \ldots, \end{array}$$

P, P', P'', ... étant les divers produits $k-1$ à $k-1$ des nombres $c, \ldots, l$.

En remplaçant maintenant $a$ et $b$ par $a'$ et $b'$, cela revient évidemment à remplacer chaque couple

$$(aP, bP), \quad (aP', bP'), \quad (aP'', bP''), \quad \ldots$$

par son p. g. c. d. et son p. p. c. m. Cette opération, nous l'avons déjà remarqué, n'influe ni sur le p. g. c. d., ni sur le p. p. c. m. des divers produits $k$ à $k$.

Par conséquent, le p. g. c. d. $D_k$ et le p. p. c. m. $M_k$ des divers produits $k$ à $k$ des nombres (A) ne changent pas en passant aux nombres $(A_1)$. $D_k$ et $M_k$ sont aussi le p. g. c. d. et le p. p. c. m. des produits $k$ à $k$ du système réduit

$$e_1, \quad e_2, \quad \ldots, \quad e_n,$$

c'est-à-dire

$$D_k = e_1 e_2 \ldots e_k, \qquad M_k = e_n e_{n-1} \ldots e_{n-k+1}.$$

De là on conclut les relations suivantes

$$e_1 = D_1, \quad e_2 = \frac{D_2}{D_1}, \quad \ldots, \quad e_k = \frac{D_k}{D_{k-1}}, \quad \ldots, \quad e_n = \frac{D_n}{D_{n-1}},$$
$$e_n = M_1, \quad e_{n-1} = \frac{M_2}{M_1}, \quad \ldots, \quad e_{n-k+1} = \frac{M_k}{M_{k-1}}, \quad \ldots, \quad e_1 = \frac{M_n}{M_{n-1}},$$

qui mettent en évidence ce fait que le système réduit est unique et donnent l'expression des nombres réduits en fonction de $a$, $b$, $c$, ..., $l$. Les relations

$$e_1 = D_1 = M_n : M_{n-1}, \qquad e_n = M_1 = D_n : D_{n-1}$$

reproduisent le théorème III. Puisque $e_k$ divise $e_{k+1}$, on voit que $D_k^2$ divise $D_{k+1} D_{k-1}$, $M_k^2$ est multiple de $M_{k+1} M_{k-1}$; on pourrait le démontrer directement en s'appuyant sur le lemme du n° 6. On voit que $D_k$ ne peut être égal à $D_{k-1}$, à moins qu'on n'ait $D_1 = D_2 = \ldots = D_k = 1$.

11. Lemme. — *$a'$ et $b'$ étant le p. g. c. d. et le p. p. c. m. de $a$ et $b$, le p. g. c. d. et le p. p. c. m. de*

$$(m, a) \quad \text{et} \quad (m, b)$$

*sont respectivement*

$$(m, a') \quad \text{et} \quad (m, b').$$

*De même, le p. g. c. d. et le p. p. c. m. de*

$$|m, a| \quad \text{et} \quad |m, b|$$

*sont respectivement*

$$|m, a'| \quad \text{et} \quad |m, b'|.$$

Pour démontrer la première partie, on remarque d'abord que le p. g. c. d. de $(m, a)$ et $(m, b)$ est évidemment $(m, a, b) = (m, a')$. Cela étant, pour démontrer que $(m, b')$ est le p. p. c. m. de $(m, a)$ et $(m, b)$, il suffira de faire voir que

$$(m, a) \times (m, b) = (m, a') \times (m, b').$$

Mais cela est évident; car, d'après le lemme du n° 6, on a

$$(m, a) \times (m, b) = (m^2, ma, mb, ab) = (m^2, ma', ab),$$
$$(m, a') \times (m, b') = (m^2, ma', mb', a'b') = (m^2, ma', a'b').$$

Pour la seconde partie, on remarque d'abord que le p. p. c. m. de $|m, a|$ et $|m, b|$ est évidemment $|m, a, b| = |m, b'|$; et ensuite il est clair que

$$|m, a| \times |m, b| = |m, a'| \times |m, b'|.$$

On conclut de ce lemme que les nombres réduits de

$$(m, a), \quad (m, b), \quad (m, c), \quad \ldots, \quad (m, l)$$

sont

$$(m, e_1), \quad (m, e_2), \quad (m, e_3), \quad \ldots, \quad (m, e_n).$$

De même, les nombres réduits de

$$|m, a|, \quad |m, b|, \quad |m, c|, \quad \ldots, \quad |m, l|$$

sont

$$|m, e_1|, \quad |m, e_2|, \quad |m, e_3|, \quad \ldots, \quad |m, e_n|.$$

**12.** Nous avons considéré, dans le n° **10**, les divers produits $k$ à $k$ des nombres $a, b, c, \ldots, l$. Si, au lieu de cela, on avait considéré simplement les divers groupes $k$ à $k$, non pour en former les produits, mais pour en prendre le p. g. c. d. ou le p. p. c. m., on serait arrivé aux résultats suivants :

$e_1$ est le p. g. c. d. de $|a|, |b|, |c|, \ldots, |l|$;
$e_2$ » $|a, b|, |a, c|, \ldots, |k, l|$;
$e_3$ » $|a, b, c|, |a, b, d|, \ldots$;
.....;

puis aussi

$e_n$ est le p. p. c. m. de $(a), (b), \ldots, (l)$;
$e_{n-1}$ » $(a, b), (a, c), \ldots, (k, l)$;
$e_{n-2}$ » $(a, b, c), (a, b, d), \ldots$;
.....

Cette recherche n'offre aucune difficulté en s'appuyant sur le lemme du n° **11**.

**13.** On dit que deux nombres sont premiers entre eux (ou bien $a$ est premier avec $b$) lorsque leur p. g. c. d. est égal à l'unité; leur p. p. c. m. est alors égal à leur produit.

Lemme. — *On a*

$$(a, bc) = (a, c \times (a, b)).$$

En effet, il est clair que

$$(a, bc) = (a, bc, ac),$$

or

$$(bc, ac) = c \times (a, b).$$

Théorème IV. — *Lorsque a et b sont premiers entre eux, tout commun diviseur de a et bc est aussi commun diviseur de a et c.*

Il suffit évidemment de montrer que

$$(a, bc) = (a, c),$$

mais cela est évident d'après le lemme précédent, puisque $(a, b) = 1$ par hypothèse.

On déduit de ce théorème les conséquences suivantes : 1° Si $c$ est aussi premier avec $a$, $bc$ est premier avec $a$. Il est facile de généraliser ce résultat ainsi. Les nombres

$$\begin{array}{llll} a, & a', & a'', & \ldots, \\ b, & b', & b'', & \ldots, \end{array}$$

étant tels que chaque nombre $a, a', \ldots$ est premier avec tous les nombres $b, b', \ldots$, le produit $aa'a''\ldots$ est premier avec $bb'b''\ldots$, $a^m$ est premier avec $b^n$. 2° Lorsque $bc$ est divisible par $a$ ($a$ et $b$ étant premiers entre eux), $c$ est divisible par $a$.

**14.** On dit que plusieurs nombres $a, b, c, \ldots, l$ sont premiers entre eux lorsque deux quelconques d'entre eux le sont. On peut remplacer cette définition par la suivante qui lui est équivalente. Plusieurs nombres $a, b, c, \ldots, l$ sont premiers entre eux lorsque $a$ est premier avec $bc\ldots l$, $b$ avec $cd\ldots l$, ..., enfin $k$ avec $l$.

Le p. p. c. m. des nombres $a, b, c, \ldots, l$, qui sont premiers entre eux, est égal à leur produit, et cette propriété est caractéristique. En effet, ayant

$$|a, b, c, \ldots, l| = abc\ldots l,$$

il est impossible que deux de ces nombres aient un diviseur commun $> 1$. Car, si $\delta$ divise $a$ et $b$,

$$\frac{ab}{\delta} \times cd\ldots l$$

est un commun multiple de $a, b, c, \ldots, l$.

Un nombre admettant les diviseurs $a, b, c, \ldots, l$ premiers entre eux, est divisible par leur produit $abc\ldots l$.

On peut dire encore : les nombres $a, b, c, \ldots, l$ sont premiers entre eux lorsque le $(n-1)^{\text{ième}}$ nombre réduit $e_{n-1} = 1$. En effet, $e_{n-1}$ est le p. p. c. m. des nombres

$$(a, b), \quad (a, c), \quad (b, c), \quad \ldots, \quad (k, l).$$

On a alors aussi

$$e_1 = e_2 = \ldots = e_{n-2} = e_{n-1} = 1,$$
$$e_n = abc\ldots l.$$

Pour que plusieurs nombres $a, b, c, \ldots, l$ soient premiers entre eux, il ne suffit pas que leur p. g. c. d. soit égal à l'unité, il faut que le p. g. c. d. $D_{n-1}$ des produits

$$bc\ldots l, \quad ac\ldots l, \quad \ldots, \quad abc\ldots k$$

soit égal à l'unité. (*Voir* le théorème III et la fin du n° 10.)

Lemme. — *Le p. g. c. d. des nombres $m$, $a$, $b$ étant l'unité, on a*

$$(m, ab) = (m, a) \times (m, b).$$

En effet, d'après le lemme du n° 6,

$$(m, a) \times (m, b) = (m^2, ma, mb, ab).$$

Or

$$(m^2, ma, mb) = m \times (m, a, b) = m$$

d'après l'hypothèse.

Plus particulièrement, on aura

$$(m, ab) = (m, a) \times (m, b)$$

lorsque $a$ et $b$ sont premiers entre eux. Ce résultat peut se généraliser immédiatement ainsi.

Théorème V. — *Les nombres $a$, $b$, $c$, ..., $l$ étant premiers entre eux, on a*

$$(m, abc\ldots l) = (m, a) \times (m, b) \times (m, c) \times \ldots \times (m, l).$$

*Remarque.* — Ce résultat est compris aussi comme cas particulier dans les propositions obtenues dans le n° 11. En effet, le $n^{\text{ième}}$ nombre réduit de

$$(m, a), \quad (m, b), \quad (m, c), \quad \ldots, \quad (m, l),$$

c'est-à-dire leur p. p. c. m. est égal à

$$(m, e_n) = (m, | a, b, c, \ldots, l |).$$

En supposant $a, b, c, \ldots, l$ premiers entre eux, on retrouve le théorème ci-dessus. On peut en tirer la conséquence que voici. Les nombres $a$, $b$, $c$, ..., $l$ étant premiers entre eux, un diviseur $\delta$ de leur produit peut être toujours mis d'une seule façon sous la forme

$$\delta = a' b' c' \ldots l',$$

où $a'$ divise $a$, $b'$ divise $b$, ..., $l'$ divise $l$. En effet, si cette décomposition en facteurs est possible, $a'$ doit diviser $a$ et $\delta$, et par conséquent $(a, \delta)$.

Mais, d'après le théorème V, on a

$$\delta = (a, \delta) \times (b, \delta) \times \ldots \times (l, \delta);$$

d'où il est clair que la décomposition est possible, et d'une seule manière.

D'autre part, on obtient toujours un diviseur de $abc\ldots l$, en multipliant un diviseur quelconque $a'$ de $a$ par un diviseur $b'$ de $b$, etc.

On peut donc conclure :

THÉORÈME VI. — *Les nombres $a$, $b$, $c$, ..., $l$ étant premiers entre eux, on obtient tous les diviseurs de leur produit $abc\ldots l$, et chaque diviseur une seule fois, en multipliant chaque diviseur de $a$ par chaque diviseur de $b$, ..., par chaque diviseur de $l$.*

*Corollaire.* — En désignant par $f(m)$ le nombre des diviseurs de $m$ (ou la somme de ces diviseurs, ou la somme de leurs $k^{\text{ièmes}}$ puissances), on a

$$f(abc\ldots l) = f(a) \times f(b) \times f(c) \times \ldots \times f(l)$$

lorsque $a$, $b$, $c$, ..., $l$ sont premiers entre eux.

15. Tout nombre $a$ (excepté l'unité) a au moins les deux diviseurs $a$ et 1. Tout nombre qui n'admet pas d'autres diviseurs s'appelle nombre *premier*. Nous ne compterons pas l'unité parmi les nombres premiers : les plus petits nombres premiers sont

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ \ldots.$$

Tout nombre qui n'est pas premier est dit *composé*. Un nombre composé $a$ est toujours égal à un produit $bc$ dont les facteurs sont $> 1$ tous les deux.

Soient $p$ un nombre premier, $a$ un nombre quelconque; si $p$ ne divise pas $a$, $a$ et $p$ seront premiers entre eux.

Lorsqu'un nombre premier $p$ divise le produit $abc\ldots l$, $p$ doit diviser au moins un des facteurs $a$, $b$, $c$, ..., $l$; car, dans le cas contraire, $p$ serait premier avec $a$, avec $b$, ..., avec $l$, par conséquent premier avec $abc\ldots l$ et ne pourrait diviser ce produit.

THÉORÈME VII. — *Tout nombre composé admet un diviseur premier.*

En effet, il est clair que le plus petit diviseur, surpassant l'unité, d'un nombre composé, est nécessairement un nombre premier.

THÉORÈME VIII. — *Tout nombre composé est égal à un produit de facteurs premiers ou, comme on dit, il est décomposable en facteurs premiers. Cette décomposition ne peut se faire que d'une seule manière.*

En effet, mettons le nombre composé $a$ sous la forme d'un produit

$$bc\ldots l$$

de facteurs $> 1$, de toutes les manières possibles. Le nombre de ces facteurs sera toujours inférieur à $n$, en supposant $2^n > a$. Parmi ces produits égaux à $a$, il y en aura donc un, au moins, dans lequel le nombre des facteurs est le plus grand.

Soit

$$p_1 p_2 \cdots p_k$$

un tel produit, il est clair que tous les facteurs sont des nombres premiers; car, si par exemple $p_1$ était composé, on pourrait obtenir un produit égal à $a$ et renfermant $k+1$ facteurs.

*Remarque.* — Il est clair qu'on obtient toujours par un nombre fini d'essais les divers produits égaux à $a$ que nous considérons. Il suffit d'écrire les nombres

$$2, \quad 3, \quad 4, \quad \ldots, \quad a,$$

de prendre leurs divers produits un à un, deux à deux, ..., $n-1$ à $n-1$ (avec répétitions) et de ne conserver que ceux de ces produits qui sont égaux à $a$.

La première partie du théorème se trouve ainsi démontrée; quant à la seconde partie, supposons deux décompositions en facteurs premiers

$$a = p_1 p_2 p_3 \cdots = q_1 q_2 q_3 \cdots.$$

Il est clair que $q_1$ doit diviser le produit $p_1 p_2 p_3 \ldots$, et, par conséquent, un des nombres $p_1, p_2, p_3, \ldots$ : donc $q_1$ est égal à un de ces nombres, par conséquent $p_1 = q_1$.

On en conclut

$$p_2 p_3 \cdots = q_2 q_3 \cdots;$$

d'où

$$p_2 = q_2, \qquad \ldots.$$

Le théorème étant ainsi complètement démontré, on voit qu'on peut mettre un nombre quelconque, et cela d'une seule manière, sous la forme

$$p^\alpha q^\beta r^\gamma \ldots,$$

$p, q, r, \ldots$ étant des nombres premiers distincts, $\alpha, \beta, \gamma, \ldots$ des nombres quelconques.

On peut déduire ce théorème aussi du théorème VII.

16. Pour que deux nombres soient divisibles l'un par l'autre, il faut et il suffit qu'en ayant décomposé les deux nombres en facteurs premiers le diviseur n'ait pas d'autres facteurs premiers que le dividende, et que ces facteurs ne figurent pas dans le diviseur avec de plus grands exposants que dans le dividende. Cela est évident d'après ce qui précède.

A l'aide de ce résultat, on peut reconnaître immédiatement la vérité de tous les théorèmes que nous avons obtenus sur le p. p. c. m., le p. g. c. d., etc., en supposant tous les nombres décomposés en facteurs premiers. Nous n'insisterons pas sur ce sujet, cependant on doit remarquer que ce n'est là, à proprement

parler, qu'une espèce de vérification; cela devient sensible surtout lorsqu'il s'agit de propositions plus compliquées, comme celles du n° **11** sur les nombres réduits. Mais nous devons expliquer encore comment on obtient immédiatement les nombres réduits de $a$, $b$, $c$, ..., $l$, lorsqu'on a décomposé ces nombres en facteurs premiers.

Supposons donc

$$\begin{aligned} a &= p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \\ b &= p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}, \\ c &= p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}, \\ &\ldots\ldots\ldots\ldots\ldots, \\ l &= p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k}. \end{aligned}$$

Pour plus de symétrie, nous avons introduit partout les mêmes nombres premiers $p_1, p_2, \ldots, p_k$, ce qui peut se faire en admettant pour les exposants aussi la valeur 0.

Considérons les exposants de $p_i$

$$\alpha_i, \quad \beta_i, \quad \gamma_i, \quad \ldots, \quad \lambda_i.$$

Supposons qu'en les écrivant par ordre de grandeur croissante on ait

$$a_i \leqq b_i \leqq c_i \leqq \ldots \leqq l_i.$$

Alors on aura

$$\begin{aligned} e_1 &= p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}, \\ e_2 &= p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}, \\ e_3 &= p_1^{c_1} p_2^{c_2} \ldots p_k^{c_k}, \\ &\ldots\ldots\ldots\ldots\ldots, \\ e_n &= p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}. \end{aligned}$$

C'est ce qu'on vérifie directement en remarquant, par exemple, que

$$e_1 e_2 \ldots e_k = D_k$$

est bien, avec ces valeurs de $e_1, e_2, \ldots, e_n$, le p. g. c. d. des produits $k$ à $k$ des nombres $a$, $b$, $c$, ..., $l$. On vérifie encore sans peine les expressions des $e_k$ que nous avons obtenues dans le n° **12**.

Les diviseurs de $p^\alpha$ sont

$$1, \quad p, \quad p^2, \quad \ldots, \quad p^\alpha,$$

leur nombre est $\alpha + 1$, leur somme

$$\frac{p^{\alpha+1} - 1}{p - 1}.$$

Un nombre quelconque

$$p^\alpha q^\beta r^\gamma \ldots$$

admet donc

$$(\alpha+1)\times(\beta+1)\times(\gamma+1)\ldots$$

diviseurs, et leur somme est

$$\frac{p^{\alpha+1}-1}{p-1}\times\frac{q^{\beta+1}-1}{q-1}\times\frac{r^{\gamma+1}-1}{r-1}\times\ldots.$$

**17.** Décomposer un nombre donné en facteurs premiers, c'est un problème dont la solution exige un grand nombre de tâtonnements. On a imaginé de nombreux artifices pour abréger le travail; mais, quoi qu'on fasse, cette décomposition est, en réalité, impraticable pour un nombre un peu grand. Aussi serait-il, par exemple, à peu près impossible d'obtenir de cette façon le p. g. c. d. de deux nombres de douze à quinze chiffres; l'algorithme d'Euclide conduit sans trop de peine au but.

On voit par là que ce n'est pas seulement en se plaçant au point de vue théorique qu'on peut exiger de ne pas faire intervenir la décomposition en nombres premiers dans des questions où ces nombres premiers ne figurent pas expressément.

Il y a une infinité de nombres premiers. En effet, $p$ étant un nombre premier, on peut toujours trouver un nombre premier plus grand que $p$. Soit, pour le montrer,

$$P = 2\times 3\times\ldots\times p$$

le produit de tous les nombres premiers qui ne surpassent pas $p$. Mettons le nombre P d'une façon quelconque sous la forme d'un produit de deux facteurs

$$P = AB,$$

alors il est clair que le nombre $N = A + B$ n'est divisible ni par 2, ni par 3, ..., ni par $p$. En décomposant donc N en facteurs premiers, on trouvera nécessairement des nombres premiers qui surpassent $p$.

Remarquons avec M. Cayley que, si l'on prend $A = P$, $B = 1$, les nombres $N+1$, $N+2$, ..., $N+p-1$ sont tous composés; d'où l'on voit que la différence de deux nombres premiers consécutifs peut surpasser un nombre donné.

**18.** Voici une proposition dont on a besoin quelquefois. Il est toujours possible de mettre le p. p. c. m. des nombres $a$, $b$, $c$, ..., $l$ sous la forme d'un produit

$$a'b'c'\ldots l',$$

dont les facteurs sont premiers entre eux et divisent respectivement $a$, $b$, $c$, ..., $l$. Adoptons les notations du n° 16, le p. p. c. m. est

$$p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}.$$

Écrivons les nombres $a, b, c, \ldots, l$ l'un au-dessous de l'autre. Écrivons ensuite le facteur $p_1^{l_1}$ à côté d'un des nombres $a, b, c, \ldots, l$ qu'il divise (un au moins de ces nombres est divisible par $p_1^{l_1}$). Faisons de même pour $p_2^{l_2} \ldots p_k^{l_k}$. Alors on prendra pour $a'$ le produit des nombres qu'on aura écrits à côté de $a$ ($a' = 1$ lorsque aucun nombre ne se trouverait à côté de $a$), de même pour $b', c', \ldots, l'$.

Il est clair qu'on obtiendra toujours au moins une solution; elle est unique dans le cas où, parmi les nombres $a, b, \ldots, l$, il n'y en a qu'un seul divisible, soit par $p_1^{l_1}$, soit par $p_2^{l_2}$, etc. Dans le cas contraire, le problème admet toujours plusieurs solutions.

19. On peut toujours obtenir une solution, sans décomposer les nombres $a$, $b$, $c$, ..., $l$ en facteurs premiers et uniquement à l'aide de l'algorithme d'Euclide.

Mais, pour abréger, nous nous bornerons au cas de deux nombres $a$ et $b$, d'où il est facile, du reste, de remonter au cas général. Soit $(a, b) = d$, et calculons

$$\left(\frac{a}{d}, d\right) = a', \qquad \left(\frac{b}{d}, d\right) = b':$$

$a'$ et $b'$ seront premiers entre eux, puisque $\frac{a}{d}$ et $\frac{b}{d}$ le sont; $d$ sera donc divisible par leur produit, soit

$$d = a' b' d'$$

et puis

$$\left(\frac{a}{d}, d'\right) = a'', \qquad \left(\frac{b}{d}, d'\right) = b'',$$

$$d' = a'' b'' d'',$$

$$\left(\frac{a}{d}, d''\right) = a''', \qquad \left(\frac{b}{d}, d''\right) = b''',$$

$$d'' = a''' b''' d''',$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \ldots\ldots$$

En continuant ainsi, on finira toujours par arriver à un couple

$$a^{(k+1)} = 1, \qquad b^{(k+1)} = 1,$$

car

$$d = a' b' d' = a' a'' b' b'' d'' = a' a'' a''' b' b'' b''' d''' = \ldots.$$

On aura alors

$$d = (a' a'' \ldots a^{(k)}) \times (b' b'' \ldots b^{(k)}) \times d^{(k)}$$

et, pour le p. p. c. m.,

$$m = \frac{ab}{d},$$

$$m = \left(\frac{a}{d} \times a'a''\ldots a^{(k)}\right) \times \left(\frac{b}{d} \times b'b''\ldots b^{(k)}\right) \times d^{(k)}.$$

Les nombres $\frac{a}{d}$ et $\frac{b}{d}$ sont premiers entre eux, et, $a'$, $a''$, ..., $a^{(k)}$ étant des diviseurs de $\frac{a}{d}$, $b'$, $b''$, ..., $b^{(k)}$ des diviseurs de $\frac{b}{d}$, il est clair que les deux facteurs

$$\frac{a}{d} \times a'a''\ldots a^{(k)} \quad \text{et} \quad \frac{b}{d} \times b'b''\ldots b^{(k)}$$

sont premiers entre eux. Ensuite $d^{(k)}$ est premier avec chacun de ces facteurs, car

$$\left(\frac{a}{d}, d^{(k)}\right) = a^{(k+1)} = 1, \qquad \left(\frac{b}{d}, d^{(k)}\right) = b^{(k+1)} = 1.$$

En prenant donc

$$A = \frac{a}{d} \times a'a''\ldots a^{(k)},$$

$$B = \frac{b}{d} \times b'b''\ldots b^{(k)} \times d^{(k)},$$

on aura $m = AB$, A et B seront premiers entre eux, puis A divise $a$ et B divise $b$. Plus généralement, si l'on a $d^{(k)} = pq$, $p$ et $q$ étant premiers entre eux, on pourra prendre

$$A = \frac{a}{d} \times a'a''\ldots a^{(k)} \times p,$$

$$B = \frac{b}{d} \times b'b''\ldots b^{(k)} \times q.$$

Si l'on suppose $a$ et $b$ décomposés en facteurs premiers, on verra facilement que

$$\frac{a}{d} \times a'a''\ldots a^{(k)}$$

est le produit des puissances de nombres premiers qui figurent dans la décomposition de $a$ avec des exposants plus grands que dans la décomposition de $b$, tandis que $d^{(k)}$ est le produit des puissances de nombres premiers qui figurent avec le même exposant dans les décompositions de $a$ et de $b$. Lorsqu'on a $d^{(k)} > 1$, on obtient toujours deux solutions au moins, en prenant soit $p = 1$, $q = d^{(k)}$, soit $p = d^{(k)}$, $q = 1$. Mais, dans ce cas, il peut arriver que le problème admet encore d'autres solutions, et cela a lieu lorsque $d^{(k)}$ est divisible par plus d'un nombre premier.

Mais, pour obtenir ces solutions, il faut absolument recourir à la décomposition de $d^{(k)}$ en facteurs premiers : l'algorithme d'Euclide seul ne peut pas les faire connaître.

20. En jetant maintenant un coup d'œil sur le chemin que nous avons parcouru, on reconnaîtra que la théorie de la divisibilité des nombres repose sur ce fait, qu'étant donnés deux nombres $a$ et $b$, on peut toujours déterminer un nombre $m$, tel que

$$a = mb + c,$$

où

$$0 \leqq c < b.$$

Si l'on considère les nombres complexes $a + bi (i = \sqrt{-1})$, on peut établir une relation analogue, et de là découle, pour ces nombres, une théorie de la divisibilité parfaitement analogue à celle des nombres ordinaires. Nous aurons à revenir plus tard sur cette question et d'autres de la même nature.

Les propositions les plus essentielles sur la divisibilité des nombres se trouvent déjà dans les *Éléments d'Euclide;* notamment on y trouve : l'algorithme pour la recherche du plus grand commun diviseur, la proposition qu'un produit ne peut être divisible par un nombre premier, à moins qu'un des facteurs ne le soit, la proposition qu'il y a un nombre infini de nombres premiers.

# CHAPITRE II.

## DES CONGRUENCES.

1. Si la différence des deux nombres $a$ et $b$ est divisible par un nombre M, $a$ et $b$ sont dits *congrus* par rapport à M; le diviseur M est appelé le *module;* $a$ et $b$ sont *résidus l'un de l'autre* suivant le module M. Pour exprimer cette relation, on écrit, d'après la notation de Gauss,

$$a \equiv b \pmod{M};$$

cette formule est une *congruence*. Il y a avantage, dans cette théorie, à admettre, pour $a$ et $b$, non seulement les valeurs entières positives, mais aussi les valeurs entières négatives.

Si $r$ est le reste de la division de $a$ par M, on a

$$a \equiv r \pmod{M}:$$

le reste $r$ est ordinairement un des nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1,$$

mais on pourrait le prendre aussi entre $-\frac{M}{2}$ et $+\frac{M}{2}$; d'où il suit que tout nombre a un résidu qui ne surpasse pas en valeur absolue la moitié du module. C'est là le *résidu minimum*.

2. Nous allons indiquer ici les propriétés les plus élémentaires des congruences, il sera à peine nécessaire d'insister sur les démonstrations. Si l'on n'indique pas le module, il sera sous-entendu que ce module est toujours M.

Si l'on a

$$a \equiv b, \qquad a' \equiv b', \qquad a'' \equiv b'', \qquad \ldots,$$

on aura ainsi

$$a + a' + a'' + \ldots \equiv b + b' + b'' + \ldots,$$

$$ma \equiv mb.$$

De même, on aura

$$aa' \equiv ba' \equiv bb'$$

et plus généralement

$$aa'a'' \ldots \equiv bb'b'' \ldots,$$

$$a^m \equiv b^m.$$

Ainsi

$$f(x, y, z, \ldots) = \sum A_{m,n,p,\ldots} x^m y^n x^p \ldots$$

étant un polynôme à coefficients entiers, on aura

$$f(a, a', a'', \ldots) \equiv f(b, b', b'', \ldots).$$

3. Supposons qu'on ait

$$ma \equiv mb \pmod{M},$$

ce qui signifie que $m(a - b)$ est divisible par M ; soit

$$(m, M) = d,$$

$\frac{m}{d}(a - b)$ sera divisible par $\frac{M}{d}$, et, puisque $\frac{m}{d}$ et $\frac{M}{d}$ sont premiers entre eux, $a - b$ sera divisible par $\frac{M}{d}$ : donc

$$a \equiv b \quad \left(\bmod \frac{M}{d}\right).$$

On peut donc diviser les deux membres d'une congruence par un nombre $m$, à condition de diviser en même temps le module par le p. g. c. d. de $m$ et M. On aura à appliquer cette proposition le plus souvent dans les cas particuliers suivants : 1° $m$ est premier avec M, alors $d = 1$; 2° $m$ divise M, alors $d = m$.

Supposons encore qu'on ait

$$aa' \equiv bb' \pmod{M},$$
$$a \equiv b \pmod{M}.$$

En multipliant la seconde congruence par $a'$, il vient, en faisant attention à la première,

$$ba' \equiv bb' \pmod{M},$$

donc

$$a' \equiv b' \quad \left(\bmod \frac{M}{d}\right),$$

où $d = (b, M) = (a, M)$, car il est clair que des nombres congrus ont même p. g. c. d. avec le module.

Si deux nombres sont congrus suivant le module M, ils seront congrus encore en prenant pour module un diviseur de M. Si deux nombres sont congrus suivant plusieurs modules A, B, C, ..., L, ils seront congrus encore en prenant pour module le p. p. c. m. de ces nombres

$$M = |A, B, C, \ldots, L|.$$

Le cas particulier le plus intéressant est celui où les modules A, B, C, ..., L sont premiers entre eux, alors $M = ABC\ldots L$.

4. On peut distribuer l'ensemble des nombres entiers en M *classes,* en considérant deux nombres comme appartenant à la même classe ou non, selon qu'ils sont congrus ou non suivant le module M. En prenant dans chaque classe un nombre, on obtient un groupe de M nombres, qu'on appelle un *système complet de résidus*. Un tel système jouit évidemment de la propriété qu'un nombre quelconque est congru à un et à un seul de ses nombres. Un nombre quelconque $a$ pris dans une classe peut être considéré comme représentant la classe entière qui se compose des nombres $a + Mx$, $x = 0, \pm 1, \pm 2, \pm 3, \ldots$. On désigne ainsi souvent la classe par un quelconque des nombres qu'il renferme, et l'on peut ainsi remplacer un nombre par un nombre congru.

Tous les nombres d'une classe ont le même p. g. c. d. avec le module M, et ce p. g. c. d. peut être un diviseur quelconque $d$ de M.

On peut, d'après cela, distribuer les classes en familles, en considérant diverses classes comme appartenant à une même famille, si elles ont le même p. g. c. d. avec le module M.

Combien de classes y a-t-il qui sont premières avec M? Il est clair qu'il y en a autant qu'on trouve parmi les nombres

$$(A) \qquad 1, \quad 2, \quad 3, \quad \ldots, \quad M$$

des nombres qui sont premiers avec M. Nous désignerons ce nombre par $\varphi(M)$, en sorte que

$$\varphi(1) = 1, \qquad \varphi(2) = 1, \qquad \varphi(3) = 2, \qquad \varphi(4) = 2, \qquad \varphi(5) = 4, \qquad \ldots.$$

Le nombre des classes qui ont avec M le p. g. c. d. $d$ est évidemment le même que celui des nombres du groupe (A) qui ont $d$ pour p. g. c. d. avec M. Il faudra donc les chercher parmi les nombres

$$d, \quad 2d, \quad 3d, \quad \ldots, \quad kd, \quad \ldots, \quad \frac{M}{d}d.$$

Or, pour que $(kd, M) = d$, il faut et il suffit que $k$ soit premier avec $\frac{M}{d}$. Le nombre cherché indique donc combien, parmi les nombres

$$1, \quad 2, \quad 3, \quad \ldots, \quad \frac{M}{d},$$

il y en a qui sont premiers avec $\frac{M}{d}$, c'est-à-dire ce nombre est $\varphi\left(\frac{M}{d}\right)$.

Il y a ainsi $\varphi\left(\frac{M}{d}\right)$ classes qui ont $d$ pour p. g. c. d. avec M, le nombre total des classes étant M, on a

$$\sum \varphi\left(\frac{M}{d}\right) = M,$$

$d$ parcourant tous les diviseurs de M. Il est clair qu'on peut écrire cette relation plus simplement ainsi

$$\sum \varphi(d) = M.$$

Il est facile de déduire de là la valeur de $\varphi(M)$.

5. Supposons plus généralement que deux fonctions numériques $f$ et F soient liées par la relation

$$F(M) = \sum f(d), \tag{1}$$

$d$ parcourant tous les diviseurs de M. Nous allons exprimer réciproquement la fonction $f$ au moyen de F.

Soit

$$M = p^\alpha q^\beta r^\gamma \ldots u^\lambda$$

la décomposition de M en facteurs premiers. On obtient l'ensemble des diviseurs $d$ de M en développant le produit

$$M\left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^\alpha}\right)\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right),$$

et nous pouvons écrire d'une manière symbolique

$$F(M) = f\left|M\left(1 + \frac{1}{p} + \ldots + \frac{1}{p^\alpha}\right)\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right)\right|.$$

On doit développer le produit du second membre et remplacer ensuite chaque terme $d$ par $f(d)$. En remplaçant M par $M:p$ (donc $\alpha$ par $\alpha - 1$), on aura

$$F\left(\frac{M}{p}\right) = f\left|M\left(\frac{1}{p} + \ldots + \frac{1}{p^\alpha}\right)\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right)\right|.$$

En retranchant, il vient, si l'on fait usage dans le premier membre de la même notation symbolique

$$F\left|M\left(1 - \frac{1}{p}\right)\right| = f\left|M\left(1 + \frac{1}{q} + \ldots + \frac{1}{q^\beta}\right)\left(1 + \frac{1}{r} + \ldots + \frac{1}{r^\gamma}\right)\ldots\left(1 + \frac{1}{u} + \ldots + \frac{1}{u^\lambda}\right)\right|.$$

En remplaçant M par $\frac{M}{q}$ et retranchant, il vient ensuite

$$F\left|M\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\right| = f\left|M\left(1+\frac{1}{r}+\ldots+\frac{1}{r^{\gamma}}\right)\ldots\left(1+\frac{1}{u}+\ldots+\frac{1}{u^{\lambda}}\right)\right|.$$

En continuant ainsi, on obtient finalement

$$(2) \qquad F\left|M\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots\left(1-\frac{1}{u}\right)\right| = f(M):$$

c'est l'expression cherchée; on peut l'écrire plus explicitement

$$(2') \qquad f(M) = F(M) - \sum F\left(\frac{M}{p}\right) + \sum F\left(\frac{M}{pq}\right) - \sum F\left(\frac{M}{pqr}\right) + \ldots.$$

On rencontre souvent des fonctions numériques qui jouissent de la propriété

$$(3) \qquad f(ab) = f(a) \times f(b)$$

lorsque $a$ et $b$ sont premiers entre eux (*voir* Chap. I, n° 14). Il est clair qu'une telle fonction est parfaitement déterminée lorsqu'on connaît sa valeur pour les puissances des nombres premiers, mais ces valeurs-là peuvent être prises arbitrairement.

On voit facilement que, si la fonction $f$ qui figure dans la relation (1) jouit de cette propriété (3), on aura aussi, $a$ et $b$ étant premiers entre eux,

$$(4) \qquad F(ab) = F(a) \times F(b),$$

et l'on reconnaît maintenant par les formules (2) ou (2') que, réciproquement, si deux fonctions $f$ et F sont liées par la relation (1), et si la fonction F satisfait à la relation (4), la fonction $f$ satisfera à la relation analogue (3).

Le théorème, souvent utile, de ce numéro est dû à M. Dedekind (*Journal de Crelle,* t. 54, p. 21). On l'établit ordinairement par une simple vérification. En exprimant au second membre de (2') partout la fonction F par la fonction $f$, on constate qu'il ne reste que le terme $f(M)$ : tous les autres termes se détruisent.

6. En revenant au cas particulier de la fonction $\varphi(M)$, $F(M) = M$, on trouve

$$\varphi(M) = M\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\ldots\left(1-\frac{1}{u}\right),$$
$$\varphi(M) = p^{\alpha-1}q^{\beta-1}\ldots u^{\lambda-1}(p-1)(q-1)\ldots(u-1).$$

Ayant $\varphi(ab) = \varphi(a)\varphi(b)$ lorsque $a$ et $b$ sont premiers entre eux, on peut remar-

quer que, $a$ étant impair, on a, à cause de $\varphi(2) = 1$,

$$\varphi(2a) = \varphi(a).$$

A l'exception de $\varphi(1) = \varphi(2) = 1$, $\varphi(a)$ est toujours pair.

7. Dans la théorie des nombres, on se propose, sur les congruences, des problèmes analogues à ceux qu'on traite en Algèbre sur les équations.

Ainsi on pose la question de trouver les nombres $x$ qui satisfont à une congruence, telle que

$$f(x) \equiv 0 \pmod{M},$$

où le premier membre est un polynôme à coefficients entiers en $x$.

Si l'on satisfait à cette congruence en faisant $x = x_0$, $x_0$ est une *racine* de la congruence. Il est clair que tout nombre congru à $x_0$ suivant le module M satisfera alors aussi à la congruence, mais on a l'habitude de ne pas considérer comme différentes ces solutions. Aussi, si l'on dit qu'une congruence admet $k$ racines, cela veut dire $k$ racines *incongrues,* ou encore, ce qui revient au même, l'ensemble des nombres qui satisfont à la congruence se répartit en $k$ classes. Il est clair, d'après cela, qu'on obtient toutes les racines d'une congruence, en essayant successivement tous les nombres d'un système complet de résidus, par exemple les nombres

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1,$$

mais ce moyen devient impraticable dès que M est un peu grand.

Si tous les coefficients du polynôme $f(x)$ sont divisibles par M, la congruence est *identique,* un nombre quelconque y satisfait. La congruence est impossible évidemment lorsque tous les coefficients de $f(x)$ sont divisibles par M, à l'exception du terme indépendant de $x$.

Il est clair, du reste, qu'il est permis de remplacer un coefficient quelconque de $f(x)$ par un nombre congru suivant le module M.

8. Considérons la congruence du premier degré

$$ax + b \equiv 0 \pmod{M}.$$

Supposons d'abord $a$ premier avec M. Pour voir si la congruence admet des racines, mettons pour $x$ successivement les valeurs

$$0, \quad 1, \quad 2, \quad \ldots, \quad M-1$$

ou, si l'on veut, M valeurs quelconques formant un système complet de résidus. Il est clair que les valeurs correspondantes de $ax + b$ sont incongrues, car la re-

lation

$$ax + b \equiv ay + b$$

exige qu'on ait $ax \equiv ay$ ou encore $x \equiv y$, puisque $a$ est premier avec M.

Les valeurs de $ax + b$ forment donc également un système complet de résidus, et, parmi ces valeurs, il y en a donc *une* qui est congrue avec 0. La congruence proposée admet donc *une* racine.

Supposons maintenant $(a, \mathrm{M}) = d$. Dans ce cas, il est clair que $b$ doit être divisible par $d$; dans le cas contraire, la congruence est impossible évidemment. Admettant donc que $b$ soit divisible par $d$, la condition imposée à $x$ revient à celle-ci

$$\frac{a}{d}x + \frac{b}{d} \equiv 0 \qquad \left[\mathrm{mod}\left(\frac{\mathrm{M}}{d}\right)\right].$$

Puisque $\frac{a}{d}$ et $\frac{\mathrm{M}}{d}$ sont premiers entre eux, nous savons qu'il existe une seule racine par rapport au module $\frac{\mathrm{M}}{d}$. Soit $x_0$ cette racine, l'ensemble des valeurs de $x$ qui satisfont à la question est comprise dans l'expression

$$x_0 + \frac{\mathrm{M}}{d}y, \qquad y = 0, \ \pm 1, \ \pm 2, \ \pm 3, \ \ldots.$$

Mais il est clair que, suivant le module M, ces nombres se répartissent en $d$ *classes*, car les $d$ nombres

$$x_0, \quad x_0 + \frac{\mathrm{M}}{d}, \quad x_0 + 2\frac{\mathrm{M}}{d}, \quad x_0 + 3\frac{\mathrm{M}}{d}, \quad \ldots, \quad x_0 + (d-1)\frac{\mathrm{M}}{d}$$

sont incongrus suivant le module M, mais un nombre quelconque $x_0 + \frac{\mathrm{M}}{d}y$ est congru, suivant le module M, avec un de ces $d$ nombres.

Théorème I. — *La congruence*

$$ax + b \equiv 0 \qquad (\mathrm{mod}\,\mathrm{M})$$

*est possible seulement lorsque $b$ est divisible par $d = (a, \mathrm{M})$. Si cette condition se trouve satisfaite, elle admet exactement $d$ racines.*

On voit que cet énoncé renferme aussi le résultat particulier qui a lieu pour $d = 1$.

9. Il nous reste à donner une méthode pour trouver effectivement, sans trop de peine, la racine de la congruence

$$ax + b \equiv 0 \qquad (\mathrm{mod}\,\mathrm{M}).$$

Il est clair que nous pourrons nous borner au cas où $a$ et M sont premiers entre eux, puisque le cas général se ramène immédiatement à ce cas particulier. Ensuite il suffira de considérer la congruence

$$ax \equiv 1 \pmod{M};$$

car, la racine de cette congruence étant obtenue, il suffira évidemment de la multiplier par $-b$ pour obtenir la racine de la congruence proposée. Le problème revient donc à satisfaire à l'équation indéterminée

$$ax - My = 1.$$

On développe en fraction continue le rapport $M:a$ ou, ce qui revient au même, on applique à $a$ et M l'algorithme d'Euclide. On peut alors exprimer de proche en proche comme fonctions linéaires homogènes de $a$ et M tous les restes obtenus et finalement le p. g. c. d. lui-même qui est 1. Comme ce mode de calcul est encore utile dans d'autres circonstances, nous allons l'expliquer avec détails.

Supposons qu'on ait une suite de nombres $N, N_1, N_2, \ldots$ liés par les relations

$$(1) \qquad \begin{cases} N = a_1 N_1 + N_2, \\ N_1 = a_2 N_2 + N_3, \\ N_2 = a_3 N_3 + N_4, \\ \ldots\ldots\ldots\ldots\ldots, \\ N_{k-1} = a_k N_k + N_{k+1}, \end{cases}$$

alors on peut exprimer successivement N par $N_1$ et $N_2$, par $N_2$ et $N_3$, ...,

$$\begin{aligned} N &= a_1 N_1 + N_2, \\ N &= (a_1 a_2 + 1) N_2 + a_1 N_3, \\ N &= (a_1 a_2 a_3 + a_1 + a_3) N_3 + (a_1 a_2 + 1) N_4, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Introduisons un symbole

$$[a_1, a_2, \ldots, a_k],$$

déterminé par les relations

$$(2) \qquad \begin{cases} [a_1] = a_1, \qquad [a_1, a_2] = a_1 a_2 + 1, \\ [a_1, a_2, \ldots, a_k] = [a_1, a_2, \ldots, a_{k-1}] a_k + [a_1, a_2, \ldots, a_{k-2}], \end{cases}$$

alors on aura généralement

$$(3) \qquad N = [a_1, a_2, \ldots, a_k] N_k + [a_1, a_2, \ldots, a_{k-1}] N_{k+1}.$$

Il est clair qu'on aura aussi

$$\begin{aligned} N_1 &= [a_2, a_3, \ldots, a_k]N_k + [a_2, a_3, \ldots, a_{k-1}]N_{k+1}, \\ N_2 &= [a_3, \ldots, a_k]N_k \quad\;\; + [a_3, \ldots, a_{k-1}]N_{k+1}, \end{aligned}$$

et, si l'on substitue ces valeurs dans la première relation (1), on obtient une expression de N par $N_k$ et $N_{k+1}$ qui doit être identique avec (3). D'où l'on conclut

$$(4) \qquad [a_1, a_2, \ldots, a_k] = a_1[a_2, a_3, \ldots, a_k] + [a_3, \ldots, a_k],$$

ce qui donne un nouveau moyen pour obtenir par récurrence la valeur du symbole. A l'aide de ces relations (2) et (4), on démontrera facilement cette formule

$$(5) \qquad [a_1, a_2, \ldots, a_k] = [a_k, a_{k-1}, \ldots, a_2, a_1].$$

En joignant à l'équation (3) celle-ci

$$(6) \qquad N_1 = [a_2, a_3, \ldots, a_k]N_k + [a_2, a_3, \ldots, a_{k-1}]N_{k+1},$$

on a deux équations; d'où l'on pourra tirer la valeur de $N_k$ en fonction de N et $N_1$. Mais cette valeur s'obtient aussi directement, car on obtient de proche en proche

$$\begin{aligned} +N_2 &= N - a_1 N_1, \\ -N_3 &= a_2 N - [a_1, a_2]N_1, \\ +N_4 &= [a_2, a_3]N - [a_1, a_2, a_3]N_1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Généralement,

$$(7) \qquad (-1)^k N_k = [a_2, a_3, \ldots, a_{k-1}]N - [a_1, a_2, \ldots, a_{k-1}]N_1.$$

En comparant cette valeur de $N_k$ avec celle tirée de (3) et (6), on a

$$(8) \quad [a_1, a_2, \ldots, a_k] \times [a_2, a_3, \ldots, a_{k-1}] - [a_1, a_2, \ldots, a_{k-1}] \times [a_2, a_3, \ldots, a_k] = (-1)^k.$$

Ce sont là les formules dont nous aurons besoin; nous en donnons encore quelques autres qui sont quelquefois utiles. On a

$$\begin{aligned} N_k &= [a_{k+1}, a_{k+2}, \ldots, a_{k+l}]N_{k+l} + [a_{k+1}, \ldots, a_{k+l-1}]N_{k+l+1}, \\ N_{k+1} &= [a_{k+2}, \ldots, a_{k+l}]N_{k+l} \quad\;\; + [a_{k+2}, \ldots, a_{k+l-1}]N_{k+l+1}. \end{aligned}$$

Substituant ces valeurs dans (3), on a l'expression de N par $N_{k+l}$ et $N_{k+l+1}$, expression qu'on peut obtenir aussi en remplaçant $k$ par $k+l$ dans la même formule. On trouve, par comparaison,

$$\begin{aligned} (9) \quad & [a_1, a_2, \ldots, a_{k+l}] \\ & = [a_1, a_2, \ldots, a_k] \times [a_{k+1}, \ldots, a_{k+l}] + [a_1, a_2, \ldots, a_{k-1}] \times [a_{k+2}, \ldots, a_{k+l}]. \end{aligned}$$