IMAGE EVALUATION
TEST TARGET (MT-3)

6"

Ca

Technical and Bibliographic Notes/Notes techniques et bibliographiques

The Institute has attempted to obtain the best original copy available for filming. Features of this copy which may be bibliographically unique, which may alter any of the images in the reproduction, or which may significantly change the usual method of filming, are checked below.

L'Institut a microfilmé le meilleur exemplaire qu'il lui a été possible de se procurer. Les détails de cet exemplaire qui sont peut-être uniques du point de vue bibliographique, qui peuvent modifier une image reproduite, ou qui peuvent exiger une modification dans la méthode normale de filmage sont indiqués ci-dessous.

- [x] Coloured covers/ Couverture de couleur
- [ ] Covers damaged/ Couverture endommagée
- [ ] Covers restored and/or laminated/ Couverture restaurée et/ou pelliculée
- [ ] Cover title missing/ Le titre de couverture manque
- [ ] Coloured maps/ Cartes géographiques en couleur
- [ ] Coloured ink (i.e. other than blue or black)/ Encre de couleur (i.e. autre que bleue ou noire)
- [ ] Coloured plates and/or illustrations/ Planches et/ou illustrations en couleur
- [ ] Bound with other material/ Relié avec d'autres documents
- [ ] Tight binding may cause shadows or distortion along interior margin/ La reliure serrée peut causer de l'ombre ou de la distortion le long de la marge intérieure
- [ ] Blank leaves added during restoration may appear within the text. Whenever possible, these have been omitted from filming/ Il se peut que certaines pages blanches ajoutées lors d'une restauration apparaissent dans le texte, mais, lorsque cela était possible, ces pages n'ont pas été filmées.
- [ ] Additional comments:/ Commentaires supplémentaires:

- [ ] Coloured pages/ Pages de couleur
- [x] Pages damaged/ Pages endommagées
- [ ] Pages restored and/or laminated/ Pages restaurées et/ou pelliculées
- [x] Pages discoloured, stained or foxed/ Pages décolorées, tachetées ou piquées
- [ ] Pages detached/ Pages détachées
- [x] Showthrough/ Transparence
- [ ] Quality of print varies/ Qualité inégale de l'impression
- [ ] Includes supplementary material/ Comprend du matériel supplémentaire
- [ ] Only edition available/ Seule édition disponible
- [ ] Pages wholly or partially obscured by errata slips, tissues, etc., have been refilmed to ensure the best possible image/ Les pages totalement ou partiellement obscurcies par un feuillet d'errata, une pelure, etc., ont été filmées à nouveau de façon à obtenir la meilleure image possible.

This item is filmed at the reduction ratio checked below/
Ce document est filmé au taux de réduction indiqué ci-dessous.

10X	12X	14X	16X	18X	20X	22X	24X	26X	28X	30X	32X
				✓							

The co
to the

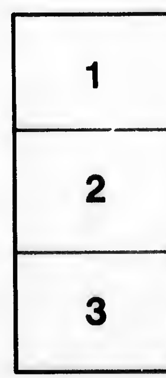
The in
possib
of the
filmin

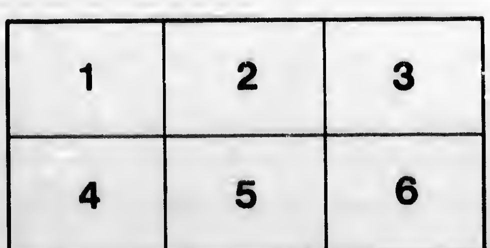
Origin
begin
the la
sion,
other
first p
sion,
or illu

The la
shall
TINU
which

Maps,
differ
entire
begin
right
requi
meth


1
2
3


1
2
3


1
2
3
4
5
6

ELE

EU

THEORIE
ELEMENTAIRE DES NOMBRES

D'APRÈS

EULER, LEGENDRE, GAUSS ET CAUCHY.

1ER FASCICULE.

MONTRÉAL
EUSÈBE SENÉCAL, IMPRIMEUR-ÉDITEUR
Nos. 6, 8 et 10, Rue St. Vincent.
1870.

ELE

E

THEORIE

ELEMENTAIRE DES NOMBRES

D'APRÈS

BULER, LEGENDRE, GAUSS ET CAUCHY.

1ER FASCICULE.

MONTRÉAL
EUSÈBE SENÉCAL, IMPRIMEUR-ÉDITEUR
Nos. 6, 8 et 10, Rue St. Vincent.

1870.

603

683
426
172

1281

2861

1992
15

29
15

142
135

9

115
119

8

(4)

4

(10)

(9)

493
426
683

2740
2861
1992

7392
6082

1392
1352

40
45

16
5

80

THÉORIE

ELEMENTAIRE DES NOMBRES.

1. Pour donner plus d'ensemble à cette exposition, nous croyons utile de remonter aux notions et aux propositions primitives. Dans tout ce qui suit, on emploie les lettres pour représenter des nombres *entiers positifs;* observation essentielle qu'il ne faut jamais perdre de vue.

2. L'*unité*, c'est l'idée abstraite d'un objet quelconque considéré comme existant seul.

3. *Compter*, c'est ajouter l'unité successivement à elle-même et donner un nom à cette agrégation ; le *nombre* est cette agrégation d'unités. L'équation suivante contient la définition du nombre :

$$a.1 = 1.a \qquad (1)$$

Il n'existe pas de dernier nombre.

4 La *numération parlée* est un système limité de signes vocaux (mots) au moyen desquels on peut nommer tous les nombres dont peuvent avoir besoin les sciences, les arts et diverses professions sociales.

5. La *numération écrite* est un système limité de signes graphiques (chiffres) au moyen desquels on peut représenter tous les nombres.

6. La série des nombres *naturels* est la suite des nombres 0, 1, 2, 3..... ∞. Il faut se représenter cette suite comme écrite sur une demi-circonférence de rayon infini, de sorte que + ∞ est diamétralement opposé à zéro ; et sur l'autre demi-circonférence, aussi à partir de zéro, on écrit la suite naturelle des nombres né-

gatifs 0, -1, -2..... $-\infty$, de sorte que $+0$ et -0, $+\infty$ et $-\infty$ se confondent. C'est une observation essentielle dont l'oubli entraîne à d'étranges hérésies.

7. La série des nombres naturels donne lieu à deux opérations principales : 1° *compter en avant*, en allant vers $+\infty$, c'est l'*addition ;* 2° *compter en arrière*, en allant vers $-\infty$, c'est la *soustraction*. Quel est le septième nombre après 13 ? *Réponse :* 20. Quel est le treizième nombre après 7 ? *Réponse :* 20 ; et le résultat s'écrit : $13+7=7+13$, et en général

$$a+b=b+a \tag{2}$$

Quel est le septième nombre après 13 en allant vers $-\infty$? *Réponse :* $+6$, ou $13-7=+6$. Quel est le vingtième nombre après 13 en marchant vers $-\infty$? *Réponse :* -7, ou $13-20=-7$. L'addition et la soustraction sont deux opérations *inverses* et peuvent servir à se contrôler mutuellement.

8. *Problème* 1. Etant donné le polynôme $a_1+a_2+a_3+\ldots a_n$, les nombres étant positifs ou négatifs, combien y a-t-il de manières d'obtenir le résultat ? Nous donnerons plus bas une solution simple de ce problême difficile (§ 12).

9. Lorsque dans l'*addition* de plusieurs nombres tous les nombres sont égaux, l'opération prend le nom de *multiplication* et le résultat se nomme *produit*.

Théorème 1. $ab=ba$ (3)

Démonstration. On a $a.1=1.a$, donc $a.1+a.1=1.a+1.a$, ou $a(1+1)=(1+1)a$, et en continuant, on parvient à $ab=ba$. On peut aussi imaginer a rangées de b carrés chacune ; le nombre total de carrés sera représenté par ab et par ba. Le même genre de raisonnement sert à démontrer que les six permutations de abc donnent le même produit : on imagine un assemblage de cubes égaux rangés en forme de parallélipipède, on en compte un nombre a dans le sens de la longueur, un nombre b dans le sens de la largeur, et un nombre c dans le sens de la hauteur ; il y aura six manières, correspondant aux six permutations, de trouver le nombre total des cubes, qui est toujours le même. (Legendre, *Théorie des nombres*, Introduction, § 2.)

10. *Théorème* 2. Dans quelque ordre qu'on effectue les multiplications de n facteurs, on parvient toujours au même produit.

Démonstration. Supposons que le théorème soit vrai pour un nombre de facteurs moindre que n ; de quelque manière qu'on s'y prenne, l'opération se termine toujours par la multiplication de deux facteurs, qui sont généralement eux-mêmes produits de facteurs simples. Soient, pour un de ces modes d'opérer, P_r et P_s deux de ces derniers facteurs composés, les indices r et s indiquent le nombre de facteurs simples qui entrent respectivement dans ces facteurs multiples ; on a évidemment $r+s=n$. Soient $P_{r'}$ et $P_{s'}$ les deux derniers facteurs correspondant à un autre mode d'opérer, on a encore $r'+s'=n$; P_r a nécessairement un certain nombre de facteurs simples en commun avec $P_{r'}$ ou avec $P_{s'}$; admettons le premier cas et désignons par P_t le produit des t facteurs communs : r étant plus petit que n, on peut multiplier d'abord entre eux ces facteurs communs, on a donc :

$$P_r = P^{t'}.P_{r-t}\ ;\ P_{r'} = P_{t'}.P_{r'-t}\ ;$$
$$P_r.P_s = P_t.P_{r-t}.P_s$$
$$P_{r'}\,P_{s'} = P_t\ .\ P_{r'-t}\,.\ P_{s'}\ ;$$

or $P_{r-t}\,.\,P_s = P_{r'-t}.\ P_{s'}$, car ces deux produits renferment les mêmes facteurs simples et en nombre moindre que n ; de quelque manière qu'on effectue le produit, il doit donc, d'après la supposition, rester le même ; donc aussi $P_r.P_s = P_{r'}.P_{s'}$. Or le théorème est vrai pour trois facteurs, il subsiste donc aussi pour quatre facteurs, etc.

11. *Problème* 2. De combien de manières peut-on effectuer le produit de n facteurs inégaux ?

Solution. Désignons par le symbole P_n ce nombre de manières ; et par P_{n+1} ce nombre lorsqu'il survient un nouveau facteur K, et que l'on a $n+1$ facteurs ; cherchons la relation entre P_{n+1} et P_n. De quelque manière qu'on s'y prenne pour effectuer P_n, il faudra toujours exécuter $n-1$ multiplications. Ceci est évident lorsqu'on multiplie le premier facteur par le second ; ce premier produit par le troisième facteur ; ce second produit par le quatrième facteur, et ainsi de suite : il en est encore de même lorsqu'on exécute par groupes. Exemples : soit $n=12$, il faut onze multiplications, par le mode successif; et si on décompose en trois groupes de trois, quatre et cinq facteurs, le premier groupe nécessite deux multiplications, le second en exige trois et le troisième quatre; à quoi il faut ajouter deux multiplications pour les trois groupes; ainsi, en tout, encore onze; et le même raisonnement s'applique à un nombre quelconque de facteurs.

Cela posé, soient d'abord deux facteurs a, b, on a évidemment $P_2 = 2$, savoir: ab, ba; prenons un troisième facteur c; on peut le combiner comme multiplicateur, ou multiplicande avec ab entièrement effectué, ce qui donne deux manières, cab, abc; ou bien encore faire intervenir c pendant la multiplication; ainsi, $ac \times b$, $ca \times b$, $a \times bc$, $a \times cb$, ce qui donne quatre manières, en tout six manières; raisonnant de même sur ba, on voit que l'on a $P_3 = 12 = 2.6$; prenons un quatrième facteur d, et combinons-le avec le produit abc; d'abord entièrement effectué, on obtient deux manières $dabc$, $abcd$; ensuite pendant l'opération, abc exige deux multiplications; en introduisant d pendant la première, celle de a par bc, on obtient quatre manières: $ad.\ bc$, $da.\ bc$, $a.\ dbc$, $a.\ bcd$, et autant pendant la seconde multiplication, celle de ab par c; en tout dix manières. On en dit autant d'un produit quelconque, d'où $P_4 = 120 = 2.\ 6.\ 10$; on trouverait de même $P_5 = 2.\ 6.\ 10.\ 14$; et ainsi de suite.

En général, soit M une des manières employées pour obtenir le produit de n facteurs. Le nouveau facteur K peut se combiner, multiplicande ou multiplicateur avec M, ce qui donne deux manières; si on l'introduit pendant l'exécution, il y a $n-1$ multiplications dont chacune donne quatre manières, et en tout $4(n-1) + 2 = 4n-2$: ce qu'on dit pour M peut s'appliquer à toute manière d'obtenir le produit de n facteurs; donc

$$P_{n+1} = (4n-2)P_n, \text{ ou bien } P_n = (4n-6)\, P_{n-1}\,.$$

Faisant successivement $n = 2, 3, 4, \ldots. n$, et considérant que $P_1 = 1$, on a

$$P_2 = 2\,;\; P_3 = 2.6\,;\; P_4 = 2.6.10\,;\; P_5 = 2.6.10.14\,;$$
$$P_6 = 2.6.10.14.18\,:$$

$$\text{et } P_n = 2.6.10\ldots(4n-6) = 2^{n-1}.1.3.5\ldots.(2n-3) = \frac{2^n[2n-3]}{2}\,;$$

les crochets désignent un produit continuel.

Observation. Cette ingénieuse solution est due à M. Rodrigues (Olinde). La formule avait été trouvée auparavant par M. Catalan à l'aide de considérations combinatoires. (*Journal* de Liouville, t. III, p. 315 et 549. 1838.)

12. *Problème* 3. De combien de manières peut-on effectuer un produit de n facteurs, lorsqu'il y a des facteurs égaux ?

Solution. Soit $a^a b^b c^c \ldots.$, et $a + b + c, \ldots. = n$ on aura

$$P_n = \frac{2.6.10\ldots\ldots(4n-6)}{(1.2.3\ldots a)\,(1.2.3\ldots b)\,(1.2.3\ldots c)\ldots}$$

Cette formule, déduite de la théorie combinatoire est aussi de M. Catalan. (*Journal* de Liouville, t. VI, p. 74. 1841.)

Observation. Ces solutions conviennent aussi au problème 1 (§ 8).

Division, diviseurs, résidus.

13. La division est une opération par laquelle on trouve combien de fois on peut soustraire un nombre d'un autre jusqu'à ce que le reste soit devenu plus petit que le nombre soustrait. Le *dividende* est le nombre duquel on soustrait; le *diviseur*, le nombre qu'on soustrait; le *quotient* marque le nombre de soustractions à effectuer; le *résidu* de deux nombres est le reste de la division du grand nombre par le petit. Ainsi, pour les deux nombres 19 et 5, 19 est le dividende, 5 le diviseur, 3 le quotient et 4 le résidu.

Soient a, dividende; p, diviseur ; q, quotient; r, résidu, on a l'identité $a = pq + r$.

Observation. La division et la multiplication sont deux opérations *inverses* et peuvent se contrôler mutuellement.

14. Lorsque le résidu de deux nombres est zéro, le dividende est dit *multiple* du diviseur, et le diviseur est un *sous-multiple* du dividende. On dit aussi, dans un sens restreint, qu'un nombre est *diviseur* d'un autre, lorsque leur résidu est nul; ainsi 5 est diviseur de 15, et 15 est un multiple de 5. Zéro est divisible par un nombre quelconque.

15. *Notation.* Nous proposons de désigner le multiple quelconque d'un nombre par un point placé sur ce nombre ; ainsi $\dot{5}, \dot{p}$

désignent des multiples quelconques de 5 ou de p, et l'équation $a = \dot{p}$ signifie que a est un multiple de p.

Observation. Le point est déjà employé pour désigner une multiplication quand il est placé à côté du nombre.

$E\left(\frac{a}{b}\right)$ désigne la partie entière du quotient de a divisé par b ; ainsi $E\left(\frac{20}{7}\right) = 2$, $E\left(\frac{31}{5}\right) = 6$.

16. Lorsque le même nombre divise d'autres nombres, on dit qu'il est *diviseur commun* à ces deux nombres ; ainsi 3 est diviseur commun à 15, 21, 36.

Un est diviseur commun à tous les nombres.

17. Un nombre premier est celui qui n'est divisible que par lui-même, 7, 11, 13, 17, etc., sont des nombres premiers ; les autres nombre sont dits non premiers ou composés. 2 est le seul nombre premier pair ; 1.2.3 sont trois nombres premiers consécutifs, il ne saurait y en avoir d'autres aussi consécutifs.

18. Deux nombres sont premiers entre eux lorsqu'ils n'ont d'autres diviseurs communs que l'unité ; ainsi 25 et 36 sont *premiers entre eux.*

Corollaire 1. *Un* est premier à l'égard de tous les autres nombres.

Corollaire 2. Un nombre premier est nécessairement premier avec tout nombre plus petit ; avec un nombre plus grand, il est premier ou il en est un sous-multiple.

19. *Théorème* 3. La somme algébrique de tant de nombres qu'on voudra, multiples chacun du même nombre, est un multiple de ce nombre.

Ce théorème peut s'écrire ainsi : $a = \dot{p}$, $b = \dot{p}$, $c = \dot{p}$, etc. ; on a $a + b + c + \ldots\ldots = \dot{p}$.

20. *Théorème* 4. La somme algébrique de tant de multiples d'un même nombre qu'on voudra, et affectés chacun d'un coefficient entier, est un multiple de ce même nombre.

Ce théorème peut s'écrire ainsi : $a = \dot{p}$, $b = \dot{p}$, $c = \dot{p}$, etc., on a aussi $ma + nb + rc + \ldots\ldots = \dot{p}$.

Corollaire. Si $a = \dot{p}$, $b = \dot{p}$, $c = \dot{p} \ldots$ on a $a^m b^n c^r \ldots\ldots = \dot{p}$, m, n, r étant des exposants entiers positifs.

Observation. Nous omettons la démonstration trop facile de ces théorèmes.

21. *Théorème* 5. Le diviseur commun à deux nombres est aussi commun à leur résidu.

Démonstration. Ce résidu est égal au dividende, moins le diviseur multiplié par le quotient ; donc...... (théorème 4).

Corollaire. Le résidu de deux nombres premiers entre eux est toujours premier avec le diviseur.

22. *Théorème* 6. Le résidu de la somme algébrique de plusieurs nombres relativement à un même diviseur, est égal à la somme des résidus.

Démonstration. Soit $a = \dot{p} + r$, $b = \dot{p} + s$, $c = \dot{p} + t$, etc. ; p étant le diviseur et r, s, t les résidus, on a

$$a + b + c + \ldots\ldots = \dot{p} + r + s + t + \ldots ;$$

donc, etc.

Observation. Si la somme des résidus surpasse le diviseur p, on prend le résidu de cette somme.

23. *Théorème* 7. Le résidu d'un produit est égal au produit des résidus des facteurs.

Démonstration. Soient a, b, c les facteurs, p un diviseur $a = \dot{p} + r$, $b = \dot{p} + s$, $c = \dot{p} + t$, on a $abc \ldots\ldots = \dot{p} + rst \ldots\ldots$: si $rst \ldots\ldots$ est plus grand que p, on en prend le résidu.

Observation. Les preuves dites par 9 dont on se sert pour contrôler les opérations de l'arithmétique sont fondées sur les deux théorèmes précédents.

24. *Théorème* 8. Le produit de deux facteurs premiers avec un troisième est premier avec ce troisième nombre.

Démonstration. Soient a, b les deux facteurs premiers avec p, et admettons, s'il est possible, que q soit un facteur commun entre ab et p, de sorte qu'on a $ab = \dot{q}$, $p = \dot{q}$. Supposons d'abord $p < a$, on a donc $p = \dot{a} + r$; le résidu r est plus petit que a. Cette équation donne celle-ci : $pb = \dot{ab} + br$; pb et $\dot{ab}$, par hypothèse, ont le facteur commun q ; ce même facteur divise donc br. De ce produit, on déduirait semblablement un produit br' divisible par q, et où $r' < r$, on parviendrait donc enfin à un produit $1 \times b$, divisible par q ; p et b auraient donc le diviseur commun q, ce qui est impossible ; donc ab et p n'ont pas de diviseur commun.

2° Si $a > p$, on a $a = \dot{p} + r$, où r est plus petit que p et premier avec p ; $ab = b\dot{p} + br$; si ab n'est pas premier avec p, alors br ne serait pas non plus premier avec p ; mais r étant plus petit que p, br est nécessairement premier avec p ; donc, etc.

Ce théorème 8 est la proposition 26 du septième livre d'Euclide.

25. *Théorème* 9. Si tous les facteurs d'un produit sont premiers avec le nombre p, le produit sera premier aussi avec ce nombre p.

Ce théorème est un corollaire du précédent ; propositions 16, 17, 18, 19 du neuvième livre d'Euclide.

Corollaire. Si a est premier avec p, a^m est aussi premier avec p ; on en déduit qu'il est impossible que la racine d'un indice quelconque d'un nombre entier soit un nombre fractionnaire, et de là l'existence des quantités irrationnelles.

26. *Théorème* 10. Un nombre composé ne peut se résoudre que d'une seule manière, en facteurs premiers.

Démonstration. Soient a, b, c, d...... les nombres premiers, suivant l'ordre de grandeur, qui divisent le nombre composé N ; ainsi $N = a^{\mathrm{a}} b^{\mathrm{b}} c^{\mathrm{c}} d^{\mathrm{d}}$......; soit un autre nombre premier a', différent de a, b, c, d...... ; étant premier avec a, b, c, d...... il sera premier avec N ; ainsi N n'admet pas d'autres nombres premiers. Soit donc $N = a^{\mathrm{a}'} b^{\mathrm{b}'} c^{\mathrm{c}'}$......, et $\mathrm{a}' > \mathrm{a}$; on aura $b^{\mathrm{b}'} c^{\mathrm{c}'}$...... $= a^{\mathrm{a}' - \mathrm{a}} b^{\mathrm{b}'} c^{\mathrm{c}'}$...... Mais cette équation est impossible, car le second membre est divisible par a et le premier ne l'est pas ; donc, etc.

27. *Problème* 4. Combien un nombre composé a-t-il de diviseurs, et quelle est la somme de ces diviseurs ?

Solution. Soit comme dans le théorème précédent,

$$N = a^{a}\, b^{b}\, c^{c}\ldots\ldots$$

Effectuant le produit des polynômes

$$(1 + a + a^2 + \ldots\ldots a^{a})\ (1 + b + b^2 + \ldots\ldots\ldots b^{b})\ (1 + \ldots\ldots c^{c})\ldots\ldots\ldots$$

tous les termes de ce produit sont inégaux ; chacun est diviseur de N, et réciproquement tout diviseur de N est nécessairement un de ces termes ; or le nombre de ces termes est évidemment $(1 + \mathrm{a})$ $(1 + \mathrm{b})$ $(1 + \mathrm{r})$....... tel est donc le nombre des diviseurs de N, l'unité comprise, et la somme de tous ces diviseurs est donc égale à

$$\frac{(a^{a+1} - 1)\ (b^{b+1} - 1)\ (c^{c+1} - 1)\ldots}{(a - 1)\ (b - 1)\ (c - 1)\ldots}$$

Coroll. Soit $N = 2^{a}\ (2^{a+1} - 1)$, et supposons que $2^{a+1} - 1$ soit un nombre premier ; ainsi $a = 2$; $b = 2^{a+1} - 1$; $\mathrm{b} = 1$; la la somme de tous les diviseurs est donc, toute réduction faite, égale à 2N ; le nombre, qui jouit de cette propriété d'être égal à la somme de ses diviseurs, est dit un nombre *parfait* ; ces nombres sont ainsi dénommés à raison de leur rareté ; voici les 11 premiers nombres :

Valeurs de a.	Nombres parfaits.
0—	1
1—	6
2—	28
4—	496
6—	8128
12—	33 550 336
16—	85 898 691 328
18—	137 438 691 328
30—	2 305 843 008 139 952 128
40—	2 417 851 639 228 158 837 784 756
46—	9 903 520 314 282 971 830 448 816 128.

Si dans un nombre parfait, on ajoute ensemble tous les chiffres, on obtient un second nombre ; si on a fait de même pour ce second nombre, on obtient un troisième nombre qui est divisible par 10. Observation de Kraft. (M. de Pét^{s}, 1734—35). Sans démonstration.

Entre 1 et un sextillion, il n'y a que 10 nombres parfaits.

Cette solution se trouve dans Euclide. (Prop. 36, liv. 9.)

28. $a+1$ est un nombre premier ; car, s'il était le produit de deux facteurs mn, alors $2^{mn}-1$ serait divisible par $2^{m}-1$ et par $2^{n}-1$; et par conséquent $2^{a+1}-1$ n'étant plus un nombre premier, N ne sera plus un nombre parfait. Faisons $2^{a}=x$; alors $N=2x^2-x$; lorsque $x=1$, N devient égal à l'unité ; donc $N-1$ est divisible par $x-1$; et l'on a $N-1=(x-1)\ (2x+1)$; remplaçant x par sa valeur, on a l'identité $N=2^{a}(2^{a+1}-1)=(2^{a}-1)(2^{a+1}+1)+1$, a est essentiellement pair, et $2^{a}=(3-1)^{a}$; donc 2^{a} est de la forme $\dot{3}+1$; par conséquent $2^{a}-1$ est divisible par 3 ; il en est de même de $2^{a+1}+1$; donc N est de la forme $\dot{9}+1$. Soit N la somme des chiffres de N ; N_2 la somme des chiffres de N_1 ; N_3 la somme des chiffres N_2 et ainsi de suite ; tous les nombres, en vertu de la propriété connue du diviseur 9 dans la numération décimale, sont de la forme $\dot{9}+1$. Ces nombres vont toujours en diminuant ; le dernier de ces nombres est donc l'unité, et l'avant-dernier est dix ou une puissance de dix.

Nous devons à l'obligeance de M. le professeur Wantzel la démonstration de cette observation de Krafft (27).

Le premier chiffre à droite de 2^{a} étant 4 ou 6, il en résulte que le premier chiffre à droite d'un nombre parfait est 6 ou 8.

RÉSIDUS NÉGATIFS ; DIVISEUR COMMUN MAXIMUM ; MULTIPLE MINIMUM.

29. Dans la division, si la partie entière du quotient est trop faible à moins d'une unité près, on dit que la division se fait *en dedans*, et dans ce cas le résidu est positif ; si la partie entière est trop forte à moins d'une unité près, la division est dite *en dehors*, et le résidu est négatif.

L'équation $a=bq+r$ (§ 13,) peut s'écrire

$$a=b\,(q+1)+r-b\,;$$

$q+1$ est le quotient en dehors, et $r-b$ est le résidu négatif correspondant; exemple :

$$15=4.3+3=4.4-1\,;$$

ainsi dans la division de 15 par 4, 3 est le résidu positif et -1 le résidu négatif. Les théorèmes 5, 6, 7 ont également lieu pour les résidus négatifs.

30. La somme du résidu positif et du résidu négatif pris positivement, est égale au diviseur ; car $r+(b-r)=b$; donc, lorsqu'un de ces résidus est plus grand que la moitié du diviseur, l'autre est nécessairement plus petit que cette moitié ; ils ne peuvent être égaux que lorsque le diviseur est pair.

31. *Problème* 5. Trouver le plus grand commun diviseur de deux nombres A et B.

1re *Solution. Méthode d'Euclide.* Elle est fondée sur le théorème 5 ; si $A=B$, le diviseur commun maximum est A ; si $A>B$, soit r_1 leur résidu ; ainsi le diviseur, cherché divise r_1 (théor. 5), et *vice versâ*, le diviseur de r_1 et de B divise A ; soit r_2 le résidu de B et de r_1. On démontre de même que le diviseur commun cherché appartient aussi à r_1 et r_2 ; les résidus r_1, r_2, r_3.... allant en diminuant, on parviendra nécessairement à zéro ou à l'unité. Dans le premier cas, le diviseur correspondant au résidu nul est le diviseur commun maximum cherché ; dans le second cas, les deux nombres n'ayant d'autres diviseurs que l'unité, sont premiers entre eux. (Euclide, liv. VII, prop. 2 : liv. X, prop. 3.)

2e *Solution. Méthode de décomposition.* On décompose chaque nombre en ses facteurs premiers. On prend tous les facteurs communs aux deux ; on donne à chacun de ces facteurs le plus petit exposant qu'il a dans les deux nombres ; le produit de ces puissances est le plus grand commun diviseur cherché. Exemple :

$$504=2^3.3^2.7: \quad 2880=2^6.3^2.5,$$

ainsi le diviseur commun maximum de 504 et de 2880 est $2^3.3^2=72$.

32. *Problème* 6. Trouver une limite pour le nombre d'opérations à effectuer dans la recherche du plus grand commun diviseur, par la méthode d'Euclide.

Solution. Soient A et B les deux nombres; $A > B$; et $r_1, r_2, r_3 \ldots r_n$ les résidus; n indique le nombres d'opérations et r_n le dernier résidu. On suppose qu'on prend toujours les résidus les plus petits, et au besoin des résidus négatifs. On a donc

$$r_1 < \frac{B}{2};\quad r_2 < \frac{r_1}{2};\ r \ldots r_n < \frac{r_{n-1}}{2};$$

sans exclure l'égalité (30). Donc

$$r_2 < \frac{B}{2^2};\quad r_3 < \frac{B}{2^3};\ \ldots\ r_n < \frac{B}{2^n};$$

or r_n étant un nombre entier, on a nécessairement

$$2^n < B;\ \text{ou}\ n < \frac{\log.B}{\log.2};\ \text{or,}\ \frac{1}{\log.2} < \frac{10}{3};$$

donc
$$n < \frac{10}{3}\log.B;$$

si B a m chiffres, alors $m > \log.B$; donc $n < \frac{10}{3}m$.

(Voir plus loin REMARQUE I.)

Le plus souvent, le nombre d'opérations est bien au-dessous de cette limite; ainsi dès qu'on parvient à un résidu premier avec le diviseur correspondant, l'opération se termine là.

32 (*bis.*) *Théorème de M. Gauss.* Les carrés des modules des termes de la série A, B, r_1, r_2, $r_3 \ldots r_n$ vont toujours en diminuant.

Démonstration. La proposition est évidente quand A et B sont des nombres réels. Si A et B sont imaginaires, soit $\frac{A}{B} = b + ci$, b et c sont réels, et $i = \sqrt{-1}$; soient b' et c' les entiers les plus rapprochés à $\frac{1}{2}$ près de b et c; de sorte que $(b-b')^2 < \frac{1}{4}$; $(c-c')^2 < \frac{1}{4}$; on a $A = Bq_1 + r_1$. Faisons

$$q_1 = b' + c'i;\quad B = h + ki;\quad r_1 = f + gi;$$

h, k, f, g sont des nombres réels. De ces diverses équations on tire

$$\frac{r_1}{\mathrm{B}} = b - b' + i\ (c - c') = \frac{f + gi}{h + ki};$$

et passant aux modules,

$$(b - b')^2 + (c - c') = \frac{f^2 + g^2}{h^2 + k^2}$$

Le premier membre est plus petit que $\frac{1}{2}$; donc $f^2 + g^2$, carré du module de r_1, ne surpasse pas la moitié de $h^2 + k^2$, carré du module de B. Ce qu'il fallait démontrer.

Observation. M. Gauss appelle *norme* le carré d'un module : cette expression abrège beaucoup d'énoncés. Le théorème précédent sert de base à la théorie des racines complexes des équations.

Corollaire. r_n est diviseur commun de A et B, et si l'on a $r = \pm 1$ ou bien $r_n = \pm i$, les nombres A et B n'ont pas de diviseur commun.

33. PROBLÈME 7. Trouver le plus grand commun diviseur des nombre A, B, C, D, etc.

1re *Solution. Méthode d'Euclide.* Soit M le plus grand commun diviseur entre A et B ; on cherche le plus grand commun diviseur entre M et C, et ainsi de suite. (Euclide, liv. VII, prop. 3 ; liv. X, prop. 2-4.)

2e *Solution. Méthode de décomposition.* On prend les facteurs premiers communs, avec leurs plus petits exposants : on en forme un produit qui est le plus grand commun diviseur cherché.

Corollaire. En divisant tous ces nombres par leur plus grand commun diviseur, les quotients n'ont plus de commun diviseur.

34. PROBLÈME 8. Trouver le plus petit multiple de deux nombres A et B.

1re *Solution. Méthode d'Euclide.* Soit D le plus grand commun diviseur, a le quotient de $\frac{\mathrm{A}}{\mathrm{D}}$ et b le quotient de $\frac{\mathrm{B}}{\mathrm{D}}$, le plus petit multiple est abD. (Euclide, liv. VII, prop. 36.)

2e *Solution. Méthode de décomposition.* On fait le produit de tous les facteurs premiers élevés chacun au plus haut exposant.

35. Problème 9. Trouver le plus petit multiple des nombres A, B, C, D......

1^re^ *Solution. Méthode d'Euclide.* Soit M le petit multiple de A et B ; on cherche le plus petit multiple M_1 de M et C, et ainsi de suite. Le dernier plus petit multiple satisfait à la question. (Euclide, liv. VII, prop. 38, seulement pour trois nombres.)

2^e^ *Solution. Méthode de décomposition.* Comme pour le problème précédent.

Observation. Les problèmes 5, 7, 8, 9 servent à simplifier les fractions et à les ramener au moindre dénominateur commun.

Nombres congruents, modules et congruences.

36. *Définition.* Deux nombres sont dits *congruents* relativement à un troisième nombre, lorsque, étant divisés chacun par ce troisième nombre, ils laissent des résidus égaux, et ce troisième nombre est dit le *module* des deux nombres *congruents.*

37. Si a et b sont congruents par rapport au module p, on aura $a-b=\dot{p}$ (th. 6, 16) ; et réciproquement, si l'on a $a-b=\dot{p}$, a et b sont congruents par rapport au module p. Une telle équation se nomme une *congruence.*

Pour exprimer que $a-b$ n'est pas divisible par p, nous écrirons $a-b>\dot{p}$; et dans ce cas, a et b ne sont pas congruents relativement à p. Ainsi $a>\dot{p}$ signifie que a n'est pas divisible par p. Si $a>\dot{x}$, x désignant un nombre quelconque supérieur à l'unité, a est un nombre premier (1).

Remarque. Euclide, au livre X, prop. 80, dit qu'une ligne est *congrue* à une autre, lorsqu'elle satisfait à certaine condition de commensurabilité. M. Gauss a transporté cette locution en arithmétique et en a fait la base d'une doctrine qui fait époque dans la théorie des nombres ; l'illustre géomètre écrit ainsi les congruences $a\equiv b$ (mod. p) ; les notations étant purement conventionnelles, lorsqu'elles n'ont pas encore acquis la sanction

(1) Voir plus loin Remarque II.

des siècles, on peut et on doit les changer, s'il y a avantage. Legendre a adopté cette forme $a—b=M(p)$, où M est la lettre initiale du mot *multiplicateur*; quelquefois encore, il emploie cette forme $\frac{a—b}{p}=e$, e étant la lettre initiale du mot *entier*. Nous avons pensé que le point, étant déjà admis pour désigner une multiplication, pourrait par analogie encore servir dans les congruences. On fait ce signe facilement et promptement; ce qui est un avantage pour le caculateur et aussi sous le rapport typographique.

M. Cauchy s'est servi des mots *équivalents* et *équivalence*, pour remplacer les mots *congruents* et *congruence*. Ces nouvelles dénominations ne paraissent pas avoir été adoptées.

Théorie des résidus dans les progressions arithmétiques ; congruences du 1er degré.

38. LEMME 1. Etant données n quantité quelconques, disposées dans un ordre quelconque sur une ligne horizontale, la dernière moins la première est égale à la somme des $n—1$ restes qu'on obtient en retranchant chaque quantité de celle qui la précède.

Démonstration. Soient a, a_1, a_2, $a_3 \ldots a_{n-1}$, a_n les n quantités, on a l'identité

$$a_n—a=(a_1—a)+(a_2—a_1)+(a_3—a_2)+\ldots(a_n—a_{n-1}).$$

Corrollaire. Si ces différences sont toutes égales, on a

$$a_n—a=(n—1)\ (a_1—a);$$

ce qui a lieu dans les progressions arithmétiques.

Observation. Ce lemme est la base du calcul aux différences finies.

39. LEMME 2. Lorsque les n quantités étant réelles sont écrites suivant leur ordre de grandeur, la différence des quantités extrêmes est plus grande qu'aucune différence entre des quantités intermédiaires.

Démonstration. Soient a_1, a_2, $a_3 \ldots a_p \ldots a_q \ldots a_n$, n quantités écrites suivant un ordre ascendant, on aura

$$a_n—a_1>a_q—a_p;$$

car $a_q—a_p$ est égal à la somme de toutes les différences intermédiaires, et $a_n - a_1$, est égal à cette même somme, plus les différences comprises entre a_p et a_1 ; et encore entre a_n et a_q. Donc, etc.

40. Lemme 3. Si n nombres inégaux se succèdent suivant un ordre ascendant, deux quelconques de ces nombres ne peuvent être congruents par rapport à un module plus grand que la différence des nombres extrêmes.

Démonstration Le module étant plus grand que la différence des extrêmes, est plus grand *à fortiori* qu'une différence entre deux nombres intermédiaires (lemme 2) ; le module ne peut donc diviser cette différence ; les deux nombres ne sont donc pas congruents.

Corollaire. Divisant donc tous les nombres par ce module, on obtient n restes différents.

41. Théorème 11. n nombres entiers consécutifs étant divisés chacun par n, donnent les résidus 0, 1, 2, 3,....$n-1$, dans un ordre quelconque.

Démonstration. Ce théorème est une conséquence immédiate du lemme précédent. (Disq. arith., sec. 4, §3.)

42. Théorème 12. Soit la progression arithmétique a, $2a$, $3a$....$(n-1)a$, n étant premier avec a ; si l'on divise chaque terme par n, on obtient les résidus 1, 2, 3....$n-1$.

Démonstration. La différence de deux termes quelconques est ka, où $k<n$; et a étant premier avec n, ka n'est donc pas divisible par n. Par conséquent, aucune différence n'est divisible par n ; tous les restes sont donc différents et moindres que n, et aucun reste n'est nul. Donc, etc.

Terquem.

[Remarque I. Mais n devant être entier quelque soit m, M. Nievengloski avait cru pouvoir conclure, comme limite, $n<3m$. Il suffit de remarquer que le reste de $\frac{10}{3}$ multiplié par un nombre $m>2$ devient $\dot{3}$. Cependant, la formule donnée par M. Terquem n'est pas, non plus assez exacte. Pour l. p. g. c. d. de 1597 et 957, elle n'indiquerait que 10 opérations : il y en a 14.

Voici la limite à laquelle M. Lamé est arrivé. Son procédé peut faire voir comment on résout ces sortes de questions.

Soient $B\ldots, D_5, D_4, D_3, D_2, 1$ tous les nombres qui ont servi successivement de diviseurs. Si l'on en prend trois consécutifs, D_5, D_4, D_3, on sait que le 3ᵉ est le reste de la division du premier par le second. Donc le premier est au moins égal à la somme des deux autres. Donc D_2 égale au moins 2, $D_3 =$ au moins 3, $D_4 =$ au moins 5.........$D_6 =$ au moins 13, $D_7 =$ au moins 21.

On a donc

$$(1) \qquad D_6 > 10\,;\; D_7 > 10 \times 2.\; D_8 > 10 \times 3\ldots\ldots$$
$$D_{11} > 10 \times 13.\; D_{12} > 10 \times 21.$$

Ou, à plus forte raison,

$$(2) \quad D_{11} > 10^2\,;\; D_{12} > 10^2 \times 2\ldots\; D_{16} > 10^3,\; D_{17} > 10^3 \times 2$$

Ou bien encore

$$D_{5+1} > 10^1,\; D_{5+2} > 10^1 \ldots . D_{2.5+1} > 10^2,\; D_{2.5+2} > 10^2 \times 2\ldots .$$
$$D_{3.5+1} > 10^3,\; D_{3.5+2} > 10^3 \times 2.$$

D'une manière générale

$$D_{5n+1} > 10^n$$

Mais 10 étant la base de notre système numéral, 10^n renferme $n+1$ chiffres ; d'ailleurs $5n+1$ est le nombre total de divisions effectuées quand on prend D_{5n+1} pour B. Donc, quand on effectue plus de $5n$ divisions, B renferme plus de n chiffres, ou autrement :

Le nombre de divisions à effectuer ne peut excéder 5 *fois le nombre de chiffres de* B,

$$n \leqq 5m$$

Remarque II. En d'autres termes a est premier quand il n'existe aucune quantité entière x qui le divise exactement.

Tous les nombres de la suite naturelle 1, 2, 3....9 appartiennent à l'une ou l'autre des deux expressions $a \equiv b \pmod p$ ou $a - b = p$ (ou $a > \dot{x}$.) C'est-à-dire que certains nombres sont produits par sommation et graduation, ex :

$8 = 2 \times 4 = 2 + 6 = 3 + 5$, etc., $10 - 1 = 3 \times 3 = 3 + 3 + 3$, etc.; tandis que d'autres ne paraissent produits que par sommation, ex: $5 = 3 + 2$, $5 > \dot{x}$; $11 = 2 + 9 = 2 + 3 + 4 + 2, =$ etc., $11 > \dot{x}$.

Jusqu'à présent on n'a pu obtenir l'expression qui détermine directement les nombres premiers, il a fallu les calculer séparément. Les tables de Buckhart s'étendent guères au-delà de 3000000. C'est ce qui fait dire à Wronski que ces nombres ont un caractère purement *négatif*. Ceux qui sont composés de facteurs ont un caractère *positif* qui les soumet à des lois et leur permet de recevoir une expression générale.

Celle que Wronski a donnée détermine la relation qui existe entre la génération par sommation et la génération par graduation au moyen des nombres quelconques $a_1, a_2, a_3, a_4 \ldots a_n$: on peut la regarder comme la loi fondamentale de la possibilité de la théorie des nombres. Comme elle ne renferme rien de difficile pour ceux qui ont vu les éléments de l'algèbre, (*Combinaisons*, *Binome*, etc.,) nous la donnons ici.

Soient $a_1, a_2, a_3, \ldots a_n$ des nombres quelconques entiers, positifs ou négatifs. Faisons d'abord $a_1 + a_2 + a_3 \ldots + a_n = N_n$.

Combinons ensuite ces mêmes nombres m à m sans permutation, nous aurons

$$a_1{}^m + a_2{}^m + a_3{}^m + \ldots a_n{}^m + a_1{}^{m-1} a_2 + a_1{}^{m-1} a_3 + \ldots$$
$$\ldots + a_1\ a_2\ a_3 \ldots = N_{n,m}.$$

$N_{n,m}$ est une fonction de N_n, laquelle a reçu l'influence réciproque de la sommation et de la graduation, ce qui est un élément essentiel de la question. On aurait pu l'obtenir par la formule du *Binome* $(a+b)^m$ etc., en réduisant à l'unité les coëfficients m, $\frac{m\,(m-1)}{1.2.}$ etc. : ce qu'on peut exprimer de cette manière

$$(a_1 + a_2 + \ldots + a_n)^m = \aleph\,[N_n]^m$$

Si l'on retranche de N_n des quantités quelconques a_i, a_l, de la suite, on aura

$$\Sigma \left[(N_n)^m = (N_n - a_i)^m + a_i (N_n - a_i)^{m-1} + a_i^2 (N_n - a_i)^{m-2} + \ldots + a_i^m \right]$$

$$\text{et } \Sigma \left[(N_n)^m = (N_n - a_l)^m + a_l (N_n - a_l)^{m-1} + a_l^2 (N_n - a_l)^{m-2} + \ldots + a_l^m \right]$$

Un peu d'attention fait voir que les seconds membres de ces équations se réduisent à

$$\Sigma \left[(N_n - a_i)^m + a_i (N_n)^{m-1} \right]$$

$$\Sigma \left[(N_n - a_l)^m + a_l (N_n)^{m-1} \right] :$$

Nous avons donc :

$$\Sigma \left[(N_n - a_i)^m + a_i (N_n)^{m-1} = (N_n - a_l)^m + a_l (N_n)^{m-1} \right]$$

Et définitivement

$$\Sigma \left[(N_n - a_i)^m - (N_n - a_l)^m = (a_l - a_i)\,(N_n)^{m-1} \right]$$

" Les deux termes du premier membre sont composés d'une manière identique. C'est cette identité qui est le principe premier de la congruence de ces deux quantités par rapport au module $(a_l - a_i)$ et par conséquent toute congruence, car cette loi est générale."

Ainsi on a $a \equiv b \pmod{p}$ lorsque a et b admettent une génération identique au moyen d'éléments $a_1, a_2, \ldots a_n$, dont deux forment le module p de leur différence.

Disons, en passant, que la solution des équations du second degré et des équations indéterminées, se rattache à la question de la théorie des nombres : il n'est pas nécessaire d'ajouter combien cette théorie tient à l'étude de l'arithmétique.

DIVISION FACILITÉE PAR LES COMPLÉMENTS.

1. *Premier procédé.* Soit D le diviseur, q le chiffre du quotient, et R le reste précédent; le reste suivant est $R-qD$; or, on a l'identité $R-qD = R + q(10^n-D) - q10^n$, n étant le nombre total des chiffres de quotient, 10^n-D est le complément du diviseur. Au moyen de cette identité, pour obtenir les restes, au lieu de *soustractions*, on n'a que des *additions* à faire, car la soustraction de $q.\ 10^n$ s'opère en effaçant du reste le premier chiffre à gauche, et si le complément est moindre que le diviseur, les multiplications sont aussi moins pénibles.

2. *Second procédé.* On a encore l'identité.

$$R-qD = R + q(p.10^{n-1}-D)-qp.10^{n-1},$$

en prenant par p le chiffre surpassant d'une unité le premier chiffre à gauche du diviseur, alors $p.10^{n-1}-D$ a toujours un chiffre de moins que le diviseur, ce qui facilite les multiplications et la soustraction de $qp10^{n-1}$ s'opère à vue sous les deux premiers chiffres à gauche du reste.—Nous supprimons les explications.

(*Nouvelles Annales Mathématiques, passim.*)

du quo-
D ; or,
le nom-
nent du
stes, au
, car la
premier
diviseur,

premier
ours un
ications
eux pre-
s expli-

sim.)