Théorie des nombres [Document électronique] / par Adrien-Marie Legendre

p1

Notre objet, dans cette introduction, est de présenter quelques considérations générales sur la nature des nombres, et particulièrement sur celle des nombres premiers. Mais, avant tout , nous croyons devoir nous occuper de quelques propositions fondamentales, dont la démonstration ne se trouve pas dans les traités ordinaires d' arithmétique, ou du moins n' y est présentée que d' une manière peu rigoureuse. I nous examinerons d' abord pourquoi le produit de deux nombres demeure le même, en changeant l' ordre des facteurs, c' est-à-dire, pourquoi *(..)* .
Soit A le plus grand des deux nombres *(..)* , soit C leur différence, et en conséquence *(..)* . On accordera aisément que le produit de *(..)* , c' est-à-dire A pris B fois, est composé du produit de B par B et du produit de C par B, de sorte qu' en écrivant le multiplicateur le dernier, on a *(..)* . Mais le produit de B par A ou par *(..)* , est composé aussi de *(..)* , de sorte qu' on a *(..)* . De là on voit que le produit *(..)* sera le même que le produit *(..)* , si le produit partiel *(..)* est égal à *(..)* . Mais par la même raison l' égalité entre *(..)* se prouvera par l' égalité entre

p2

deux produits plus petits Cd et Dc ; et en continuant ainsi on parviendra nécessairement, soit au cas où les deux facteurs sont égaux, soit au cas où l' un des deux est égal à l' unité. Dans le premier cas, l' égalité est manifeste ; dans le second, elle se conclut de ce que *(..)* , ainsi que *(..)* . Donc le produit *(..)* est toujours égal au produit *(..)* . Ii on suppose ordinairement qu' en multipliant un nombre donné C par un autre nombre N qui est lui -même le produit de deux facteurs *(..)* , il revient au même de multiplier *(..)* tout d' un coup, ou bien de multiplier *(..)* , ensuite le produit par B. Pour démontrer cette proposition, j' observe d' abord que le produit Ab n' est autre chose que *(..)* etc., le nombre de ces termes étant B. Lors donc qu' on multiplie un troisième nombre C par le produit Ab, on est censé

répéter B fois l' opération de multiplier C par A, c' est-à-dire qu' on a *(..)* etc., le terme Ca étant écrit B fois. Le résultat est donc *(..)* , de sorte qu' on a *(..)* . Iii d' après ces deux propositions, on démontrera facilement que *le produit de tant de facteurs qu' on* voudra, demeure toujours le même, en quelque ordre *que les facteurs soient multipliés* . Pour prouver, par exemple, que le produit *(..)* est égal au produit *(..)* , je commence par faire en sorte que la même lettre occupe la dernière place dans les deux. Or on a, en vertu des propositions précédentes, *(..)* ; donc *(..)* ; la lettre B est à la dernière place dans ce produit, comme elle l' est dans l' autre produit donné Cadb. ôtant la dernière lettre, il suffira de prouver l' égalité *(..)* ; or celle-ci résulte de ce que *(..)* . Iv " le produit de deux nombres *(..)* est divisible par tout nombre qui divise exactement l' un des deux facteurs *(..)* . "

p3

car soit *(..)* un nombre qui divise B, et soit en conséquence *(..)* , on aura *(..)* ; donc Ab divisé par *(..)* donne le quotient exact Ac . V " si le nombre *(..)* divise à-la-fois les deux nombres Aetb, il divisera la somme et la différence de deux multiples quelconques de ces nombres. " car si l' on a *(..)* , il en résulte , quantité qui, divisée par *(..)* , donne le quotient exact *(..)* . Vi " tout nombre premier qui ne divise ni l' un ni l' autre des facteurs Aetb, ne peut diviser leur produit Ab. " cette proposition étant l' une des plus importantes de la théorie des nombres, nous donnerons à sa démonstration tout le développement nécessaire. Soit, s' il est possible, *(..)* un nombre premier qui ne divise ni A ni B, mais qui divise le produit Ab, on pourra supposer qu' en divisant A par *(..)* on a le quotient M (qui pourrait être zéro) et le reste *(..)* ; on aura donc *(..)* , et semblablement *(..)* . Donc *(..)* . Cette quantité, d' après l' hypothèse, doit être divisible par *(..)* , et comme les trois premiers termes sont divisibles par *(..)* , il faudra que le quatrième *(..)* soit également divisible par *(..)* ; ainsi nous pourrons faire *(..)* . Dans ce premier résultat, nous remarquerons 1 que *(..)* ne sont zéro ni l' un ni l' autre, parce que Aetb sont supposés non divisibles par *(..)* ; 2 que *(..)* , comme restes de la division par *(..)* , sont moindres que *(..)* ; 3 qu' aucun des nombres *(..)* ne peut être égal à l' unité ; car si on avait *(..)* , le produit *(..)* se réduirait à *(..)* ; or *(..)* , il est impossible qu' on ait *(..)* . Nous avons donc deux nombres entiers, *(..)* , tous deux plus grands que l' unité, et tous deux moindres que *(..)* , dont le produit est divisible par *(..)* , de sorte qu' on a *(..)* . Voyons les conséquences qui en résultent. Puisque *(..)* est moindre que *(..)* , on peut diviser *(..)* ; soit P le quotient et *(..)* le reste, on aura *(..)* ; donc *(..)* .

p4

Le premier membre est divisible par *(..)* , il faut donc que le second le soit aussi. Mais la partie *(..)* est divisible d' elle-même par *(..)* , puisque *(..)* ; donc l' autre partie *(..)* doit être encore divisible par *(..)* . Le nombre *(..)* , comme reste de la division par *(..)* , est moindre que *(..)* , il ne peut d' ailleurs être zéro ; car si cela était, *(..)* serait divisible par *(..)* et ne serait plus un nombre premier. Donc du produit *(..)* , supposé divisible par *(..)* , on tire un autre produit *(..)* divisible encore par *(..)* , et qui est plus petit que *(..)* sans être zéro. En suivant le même raisonnement, on déduira du produit *(..)* un autre produit ou *(..)* , encore plus petit, et qui sera toujours divisible par sans être zéro. Et en continuant la suite de ces produits décroissants, on parviendra nécessairement à un nombre moindre que *(..)* . Or il est impossible qu' un nombre moindre que *(..)* , et qui n' est pas zéro, soit divisible par *(..)* ; donc l' hypothèse d' où l' on est parti ne saurait avoir lieu. Donc si les nombres Aetb ne sont divisibles, ni l' un ni l' autre, par *(..)* , leur produit Ab ne pourra non plus être divisible par *(..)* . Vii la doctrine des incommensurables repose entièrement sur le principe qu' on vient de démontrer. En effet, s' il existait, par exemple, une fraction rationnelle *(..)* égale à *(..)* , il faudrait que *(..)* fût égale à 2. Donc *(..)* devrait être divisible par chacun des nombres premiers qui divisent N. Mais la fraction *(..)* étant censée irréductible, M n' a aucun diviseur commun avec N ; donc , en vertu du théorème précédent, *(..)* ne peut avoir non plus aucun diviseur commun avec N ; donc il est impossible qu' on ait . En général une puissance quelconque du nombre A ne peut avoir pour diviseurs d' autres nombres premiers que ceux qui divisent A ; ainsi s' il n' y a point de nombre entier X tel que *(..)* , étant un

p5

nombre donné, il n' y a point non plus de fraction *(..)* telle que . Viii " un nombre quelconque N, s' il n' est pas premier, peut être représenté par le produit de plusieurs nombres premiers etc., élevés chacun à une puissance quelconque, de sorte qu' on peut toujours supposer *(..)* , etc. " la méthode à suivre pour opérer cette décomposition, consiste à essayer la division du nombre N par chacun des nombres premiers *(..)* etc, en commençant par les plus petits. Lorsque la division réussit par l' un de ces nombres *(..)* , on la répète autant de fois qu' elle est possible, par exemple, M fois, et en appelant le dernier quotient P, on a . Le nombre P ne pouvant plus être divisé par *(..)* , il est inutile d' essayer la division de P par un nombre premier moindre que *(..)* ; car si P était divisible par *(..)* moindre que , il est clair que N serait aussi divisible par *(..)* , ce qui est contraire à la supposition. On ne devra donc essayer de diviser P que ar des nombres premiers plus grands que *(..)* ; on trouvera ainsi successivement *(..)* , ce qui donnera *(..)* , etc. Ix " si, après avoir essayé la division d' un nombre donné N par les

nombres premiers plus petits que *(..)* , on n' en trouve aucun qui divise N, on en conclura avec certitude que N est un nombre premier. " car supposons que N soit divisible par un nombre premier *(..)* , on aurait donc, en appelant P le quotient, *(..)* . Mais puisque *(..)* , on aura *(..)* ; donc N serait divisible par un nombre P moindre que *(..)* ; donc, à plus forte raison, il serait divisible par un nombre premier *(..)* , ce qui est contre la supposition. On peut donc trouver, de cette manière, si un nombre donné N est premier, ou s' il ne l' est pas ; mais quoique cette méthode soit

p6

susceptible de quelques abrégés dont nous ferons mention ci-après , elle est en général longue et fastidieuse. Aussi plusieurs mathématiciens ont-ils jugé convenable de construire des tables de nombres premiers plus ou moins étendues. La manière la plus simple de construire ces tables, est de commencer par écrire de suite les nombres impairs 1, 3, 5, 7, etc. Jusqu' à 100 000, ou telle autre limite qu' on peut se proposer. Cette suite étant formée, on en efface successivement tous les multiples de 3, tous ceux de 5, tous ceux de 7, etc., en conservant seulement les premiers termes 3, 5, 7, etc., non effacés par les opérations antérieures. De cette manière, il est visible que tous les nombres restants n' ont d' autres diviseurs qu' eux-mêmes, et qu' ainsi ils sont des nombres premiers. On trouvera à la fin de cet ouvrage une table *(..)* , qui contient les nombres premiers jusqu' à 1229. Dans un livre intitulé, (...), on en trouve une qui s' étend jusqu' à 400000, et qui a de plus l' avantage d' indiquer pour chaque nombre composé, pris dans cette limite, le plus petit nombre premier qui en est diviseur. Mais les géomètres désiraient depuis long-temps que la table des nombres premiers fût prolongée au moins jusqu' à un million. M Chernac, professeur à Deventer, a le premier rempli leur voeu en donnant au public son *Cribrum Arithmeticum* , où l' on trouve tous les nombres premiers et les diviseurs des autres nombres jusqu' à un million. Peu de temps après, M Burckhardt ayant trouvé les moyens de simplifier beaucoup la construction de ces sortes de tables, en a publié une qui, sous un assez petit volume, contient les nombres premiers de 1 à 3036000, et les plus petits diviseurs des autres nombres. Les amateurs de l' analyse indéterminée ont donc le choix entre deux recueils qui peuvent leur être également utiles, l' un par un maniement plus facile, l' autre par une plus grande étendue. X un nombre N étant réduit à la forme *(..)* , etc., tout diviseur de ce nombre sera aussi de la forme *(..)* , etc., où les exposants

p7

, etc., ne pourront surpasser M, N, P, etc. Il suit de là que tous les diviseurs du nombre N seront les différents termes du produit développé *(..)* . Donc le nombre de tous ces diviseurs est *(..)* etc. Et en même temps la somme de ces mêmes diviseurs est égale à P et peut se mettre sous la forme *(..)* , etc. Par exemple, puisqu' on a *(..)* , le nombre des diviseurs de 360 est *(..)* , et leur somme *(..)* . Xi il est facile de trouver un nombre qui ait tant de diviseurs qu' on voudra. Cherchons, par exemple, un nombre qui ait 36 diviseurs ; on décomposera 36 en facteurs premiers ou non, tels que 4, 3, 3 ; on diminuera chaque facteur d' une unité, ce qui donnera 3, 2, 2 ; d' où l' on conclura que *(..)* est l' une des formes du nombre cherché, *(..)* étant des nombres premiers inégaux. Les facteurs 6, 3, 2 donneraient une autre forme *(..)* , dans laquelle le plus simple des nombres compris est *(..)* . Xii si on cherche en combien de manières le nombre *(..)* , etc. Peut être le produit de deux facteurs Aetb, on trouvera que ce nombre *(..)* etc. Car chaque diviseur A est accompagné de son inverse *(..)* ou B ; ainsi le nombre des quantités Ab ou Ba est la moitié de celui des diviseurs de N.

p8

Si le nombre N était un carré, tous les exposants M, N, P, etc. Seraient pairs, et alors la moitié du produit *(..)* etc. Contiendrait la fraction *(..)* , pour laquelle il faudrait prendre l' unité. Xiii si l' on veut que les deux facteurs dans lesquels on décompose le nombre N soient premiers entre eux, alors le nombre des combinaisons ne dépend plus des exposants M, N, P, etc., et il est le même que si le nombre N était simplement *(..)* , etc., de sorte qu' en appelant K le nombre des facteurs premiers inégaux *(..)* , etc., on aura *(..)* pour le nombre de manières de partager N en deux facteurs premiers entre eux. Par exemple, le nombre 1800 peut se partager de 18 manières en deux facteurs ; mais il ne peut se partager que de quatre manières en deux facteurs premiers entre eux ; car on a *(..)* , et *(..)* . Xiv un nombre N étant donné, soit proposé de trouver combien il y a de nombres premiers à N et plus petits que N. Pour cela, nous allons examiner successivement l' influence des différents facteurs premiers sur le résultat. Soit d' abord *(..)* , *(..)* étant un nombre premier et M un facteur quelconque qui pourrait être divisible par *(..)* ou par une puissance de *(..)* . Si l' on considère la suite des nombres naturels 1, 2, 3... N, les termes de cette suite qui sont divisibles par *(..)* forment eux-mêmes la suite *(..)* ; leur nombre *(..)* ; donc en appelant X le nombre des termes de la première suite qui ne sont pas divisibles par *(..)* , on aura *(..)* . Soit en second lieu *(..)* , *(..)* étant deux nombres premiers différents et M un facteur quelconque. Dans la suite 1, 2, 3... N, on peut distinguer trois sortes de termes, 1 les X termes qui ne sont divisibles ni par *(..)* ni par *(..)* ; 2 les termes qui sont divisibles par l' un de ces nombres premiers, sans l' être par l' autre ; 3 les termes divisibles par *(..)* .

p9

Les termes divisibles par *(..)* sont au nombre de *(..)* ou *(..)* ; mais si on en exclut les termes divisibles par *(..)* , leur nombre se réduira, suivant ce qu' on a déja trouvé, à *(..)* . De même les termes divisibles par *(..)* , sans l' être par *(..)* , sont au nombre de *(..)* . Enfin les termes divisibles par *(..)* sont au nombre de M. Donc on aura *(..)* ; d' où l' on tire *(..)* . Soit en troisième lieu ; nous distinguerons semblablement dans la suite 1, 2, 3 ... N, quatre sortes de termes, 1 les X termes qui ne sont divisibles par aucun des facteurs *(..)* ; 2 les termes qui sont divisibles par un de ces facteurs seulement ; 3 ceux qui le sont par deux seulement ; 4 enfin ceux qui le sont par trois. Les termes divisibles par *(..)* sont en général au nombre de *(..)* ou ; mais si parmi eux on ne considère que ceux qui sont premiers à *(..)* , leur nombre se réduit à *(..)* , ainsi qu' on l' a trouvé dans le second cas. Les termes divisibles par *(..)* sont en général au nombre de *(..)* ou *(..)* ; mais en ne considérant parmi ceux-ci que les termes premiers à *(..)* , leur nombre se réduit à *(..)* . Enfin les termes divisibles par *(..)* sont au nombre de *(..)* ou M. Donc on aura N ou *(..)* . Soit, pour un moment, *(..)* , le premier membre deviendra *(..)* , ou *(..)* .

p10

Et le second membre ne diffère de cette quantité que par le premier terme, qui est X au lieu de *(..)* . Donc on a *(..)* , ou *(..)* . Le même raisonnement s' étend aisément à un plus grand nombre de facteurs, et on voit que le résultat sera toujours de la même forme. Xv cela posé, tout nombre N pouvant être mis sous la forme *(..)* , etc., laquelle est comprise dans l' expression générale *(..)* , etc., il est clair que par la formule *(..)* , etc., on connaîtra combien il y a de nombres premiers à N et plus petits que N. Par exemple, on a *(..)* ; donc il y a 16 nombres plus petits que 60 et premiers à 60. Ces nombres sont *(..)* . Xvi cherchons maintenant combien de fois un nombre premier donné *(..)* est facteur dans la suite des nombres naturels depuis 1 jusqu' à N, ou, ce qui revient au même, quelle est la plus grande puissance de *(..)* qui divise le produit 1, 2, 3... N. Pour cela, désignons par *(..)* l' entier le plus grand contenu dans la fraction *(..)* , et le nombre cherché ou l' exposant de *(..)* étant nommé X, nous aurons *(..)* , cette suite étant prolongée tant que le numérateur est plus grand que le dénominateur. En effet, il est évident que *(..)* représente le nombre des termes

p11

de la suite 1, 2, 3... N, qui sont divisibles par *(..)* ;

pareillement, *(..)* représente le nombre des termes de la même suite qui sont divisibles par *(..)* , ainsi des autres. Or si dans le produit 1, 2, 3... N, il n' y avait point de termes divisibles par *(..)* , le nombre des facteurs *(..)* qui divisent ce produit serait simplement *(..)* ; s' il y a ensuite des termes divisibles par *(..)* , chacun de ces termes ajoute un nouveau facteur *(..)* à celui qui était déja compris dans *(..)* ; de sorte qu' à raison des termes divisibles par *(..)* , et des termes divisibles par *(..)* , le nombre des facteurs *(..)* devient *(..)* . Pareillement, chaque terme divisible par *(..)* ajoute un facteur de plus à ceux qui étaient déja dénombrés ; de sorte que le nombre total des facteurs *(..)* devient *(..)* ; ainsi de suite jusqu' à ce qu' on parvienne à une puissance *(..)* ; alors la série des E est terminée, puisque *(..)* étant plus petit que l' unité, l' entier compris *(..)* . Xvii cherchons par exemple, combien, dans le produit des nombres naturels de 1 à 10000, il y a de fois le facteur 7. Nous ferons l' opération suivante, qui se termine bientôt, *(..)* . La somme de tous ces nombres *(..)* ; donc le produit dont il s' agit est divisible par *(..)* . Si le nombre proposé N eût été une puissance entière de 7, on

p12

aurait eu exactement *(..)* . En général, si on a *(..)* , le nombre des facteurs *(..)* compris dans le produit 1, 2, 3... N sera *(..)* . Et si on fait, comme on peut toujours le supposer, *(..)* , les coefficients A, B, C, etc. étant plus petits que *(..)* , il en résultera *(..)* . Xviii dans le cas particulier où *(..)* , il en résultera *(..)* , et si l' on fait généralement *(..)* , on aura *(..)* , K étant le nombre des termes *(..)* etc. Dont se compose la valeur de N. Veut-on, par exemple, savoir combien de fois 2 est facteur dans la suite des nombres naturels de 1 à 1000 ? On décomposera 1000 en puissances de 2, savoir *(..)* ; et comme le nombre de ces termes est 6, le nombre cherché sera *(..)* ou 994. Le même résultat s' obtient non moins facilement par la formule générale, car on a *(..)* , et la somme de tous ces nombres *(..)* . Xix " tout nombre premier, excepté 2 et 3, est compris dans la formule *(..)* . "

p13

en effet, si l' on divise un nombre impair par 6, le reste ne peut être que l' un des nombres 1, 3, 5. Donc tout nombre impair peut être représenté par l' une des formules *(..)* . La seconde ne peut convenir aux nombres premiers, puisqu' elle est divisible par 3, et que 3 est excepté ; d' ailleurs la formule *(..)* contient les mêmes nombres que *(..)* ; donc tout nombre premier, hors 2 et 3, est compris dans la formule *(..)* . Il ne s' ensuit pas réciproquement que tout nombre compris dans la formule

soit un nombre premier ; on trouverait que cela n' a pas lieu lorsque *(..)* , etc. Xx en général il n' existe aucune formule algébrique propre à n' exprimer que des nombres premiers. Car soit, par exemple, la formule *(..)* , et supposons qu' en faisant , la valeur de P soit égale au nombre premier P : si on fait , Y étant un entier quelconque, on aura *(..)* , d' où l' on voit que P n' est pas un nombre premier, puisqu' il est divisible par P et différent de P. Il est néanmoins quelques formules remarquables par la multitude des nombres premiers qu' elles contiennent : telle est la formule *(..)* , dont Euler fait mention dans les mémoires de Berlin, 1772, Pag 36, et dans laquelle, si l' on fait successivement *(..)* , etc., on a la suite *(..)* , etc., dont les quarante premiers termes sont des nombres premiers. On peut citer dans le même genre la formule *(..)* , dont les dix-sept premiers termes sont des nombres premiers ; la formule *(..)* , dont les vingt-neuf premiers termes le sont, et une foule d' autres. Xxi si on ne peut pas trouver de formule algébrique qui renferme uniquement des nombres premiers, à plus forte raison n' en peut-on pas trouver une qui renferme absolument tous ces nombres et qui soit l' expression de leur loi générale. Cette loi paraît très-difficile

p14

à trouver, et il n' y a guère d' espérance qu' on y parvienne jamais. Cela n' empêche pas qu' on ne puisse découvrir et démontrer un grand nombre de propriétés générales des nombres premiers, lesquelles répandent un grand jour sur leur nature. Et d' abord nous pouvons démontrer rigoureusement que la multitude des nombres premiers est infinie. Car si la suite des nombres premiers *(..)* , etc. était finie, et que P fût le dernier ou le plus grand de tous, il faudrait qu' un nombre quelconque N fût toujours divisible par quelqu' un des nombres premiers 1, 2, 3, 5... P. Mais si on représente par P le produit de tous ces nombres, il est clair qu' en divisant *(..)* par l' un quelconque des nombres premiers jusqu' à P, le reste sera 1. Donc l' hypothèse que P est le plus grand des nombres premiers ne saurait avoir lieu ; donc la multitude des nombres premiers est infinie. Cette proposition se prouve encore d' une manière directe et fort élégante, en faisant voir que la suite réciproque des nombres premiers *(..)* etc. A une somme infinie. Xxii tous les nombres impairs se représentent par la formule *(..)* , laquelle, selon que X est pair ou impair, contient les deux

p15

formes *(..)* . De là deux grandes divisions des nombres premiers, l' une comprenant les nombres premiers *(..)* , savoir, *(..)* etc. ; l' autre comprenant les nombres premiers *(..)* , savoir, *(..)* , etc. La

forme générale *(..)* se subdivise en deux autres formes *(..)* ; de même la forme *(..)* se subdivise en deux autres *(..)* ; de sorte que, relativement aux multiples de 8, les nombres premiers se partagent en ces quatre formes principales : *(..)* , lesquelles donnent lieu à différents théorèmes qui caractérisent ces formes et que nous exposerons dans la suite. Xxiii nous avons déja vu que les nombres premiers, considérés par rapport aux multiples de 6, sont de l' une des formes *(..)* et *(..)* ; dans celles-ci X peut être pair ou impair, et de là résultent, par rapport aux multiples de 12, les quatre formes *(..)* , chacune renfermant une infinité de nombres premiers. En général, A étant un nombre donné à volonté, tout nombre impair peut être représenté par la formule *(..)* , dans laquelle B est impair et moindre que *(..)* , ou, ce qui revient au même, par la formule *(..)* , dans laquelle B est impair, positif et moindre que *(..)* . Si, parmi toutes les valeurs possibles de B, on retranche celles qui ont un diviseur commun avec A, les formes restantes *(..)* comprendront tous les nombres premiers (à l' exception de ceux qui divisent *(..)*) partagés, relativement aux multiples de *(..)* , en autant d' espèces ou formes que B aura de valeurs différentes. Le nombre de ces formes est évidemment le même que celui

p16

des nombres plus petits que 4 a et premiers à 4 a ; donc si on a *(..)* , etc., *(..)* , etc. étant des nombres premiers, le nombre de ces formes sera donné par la formule *(..)* , etc. Xxiv par exemple, si l' on a *(..)* , il en résulte *(..)* . Ainsi, relativement aux multiples de 60, tous les nombres premiers (excepté 2, 3, 5, diviseurs de 60), se partagent en seize formes, savoir : *(..)* ; on prouvera, de plus, par la suite, que la distribution des nombres premiers entre ces seize formes se fait également, ou suivant des rapports qui tendent de plus en plus vers l' égalité.

p47

Théorème. (27) " étant proposée l' équation *(..)* , dans laquelle les coefficients A, B, C, pris individuellement, ou deux à deux, n' ont ni diviseur carré, ni diviseur commun ; je dis que cette équation sera résoluble, si on peut trouver trois entiers

p48

tels que les trois quantités *(..)* soient des entiers : elle sera au contraire insoluble, si ces trois conditions ne peuvent être remplies à-la-fois. " *remarque I.* ces conditions se réduisent à deux, si l' un des trois nombres A, B, C, est égal

à l' unité, et elles se réduisent à une seule, comme dans le *(..)* , si deux de ces nombres sont égaux à l' unité. *remarque Ii.* on peut toujours arranger les trois termes de l' équation proposée, de manière que A, B, C soient positifs ; mais cette condition n' est pas de rigueur, et le théorème serait encore vrai, quand même quelqu' un de ces termes serait négatif. Il ne faudrait pas cependant conclure de là qu' une équation telle que est possible, par cela seul qu' on peut satisfaire aux conditions *(..)* , il faudrait conclure seulement qu' elle peut se ramener à la forme *(..)* . En général, toute équation résoluble pourra, par la méthode du *(..)* précédent, se ramener à la forme ; mais il suffit de la ramener à la forme *(..)* , dont la solution se trouve immédiatement.

p194

(131) ce théorème, dont Waring fait mention dans ses *Meditationes Algebraïcae* , et dont il attribue la découverte à Jean Wilson, a été démontré pour la première fois par Lagrange dans les mémoires de Berlin, année 1771, et ensuite par Euler dans ses *Opuscula Analytica* , Tomi. Il est surtout remarquable, en ce qu' il n' a lieu que lorsque N est un nombre premier. En effet, si N est composé de deux facteurs quelconques inégaux Aetb, ces deux facteurs se trouveront nécessairement tous deux parmi les nombres *(..)* , et la quantité *(..)* divisée par N, laissera pour reste *(..)* . La même chose aurait lieu, quand même N serait égal au produit des deux facteurs égaux *(..)* ; car alors A et *(..)* se trouveraient dans la suite *(..)* . Donc le produit de ces nombres serait divisible par *(..)* , et ce produit, augmenté d' une unité, laisserait pour reste I. On peut déduire de là une règle générale et infaillible, pour reconnaître si un nombre donné N est premier ou s' il ne l' est pas. Pour cela, il faut ajouter une unité au produit *(..)* ; si la somme est divisible par N, le nombre N sera premier ; si elle ne l' est pas, le nombre N sera composé. Mais quoique cette règle soit très-belle *In Abstracto* , elle ne peut avoir aucune utilité dans la pratique, attendu la grandeur énorme à laquelle s' élève bientôt le produit *(..)* .

p195

Observons que les nombres *(..)* , etc. Considérés comme restes de la division par N, sont équivalents aux restes *(..)* , etc. ; d' ailleurs N étant supposé impair, le nombre des facteurs *(..)* sera pair. Donc le produit *(..)* , divisé par N, laissera le même reste que *(..)* , le signe ambigu étant *(..)* lorsque N est de la forme *(..)* lorsqu' il est de la forme *(..)* . Donc 1 si le nombre premier N est de la forme *(..)* , la quantité *(..)* sera divisible par N. On connaît donc ainsi *a priori* une somme de deux carrés *(..)* dont

N doit être diviseur. 2 si le nombre premier N est de la forme *(..)* , la quantité *(..)* sera divisible par N, et par conséquent N doit diviser l' une ou l' autre des deux quantités . (132) Lemme. " soit C un nombre premier, et P un polynome du degré M dont les coefficients sont entiers, savoir, ; je dis qu' il ne peut y avoir plus de M valeurs de X, comprises entre *(..)* , qui rendent ce polynome divisible par C. " car soit K une première valeur de X qui rende P divisible par C, on pourra faire *(..)* , et on aura pour *(..)* un polynome en X du degré *(..)* . Soit *(..)* une seconde valeur de X qui rende P divisible par C, il faudra que cette valeur rende *(..)* divisible par C. Mais le facteur *(..)* , qui devient *(..)* , ne peut être divisible par C, puisque *(..)* sont supposés chacun plus petits que *(..)* ; donc P ne pourra être divisible une seconde fois par C, à moins que *(..)* ne le soit. Le polynome P du degré M n' admet par conséquent qu' une solution de plus que le polynome *(..)* du degré *(..)* ; donc il ne peut y avoir au plus que M valeurs différentes de X, comprises entre *(..)* , qui rendent P divisible par C.

p196

Nous regarderons comme *solution* ou *racine* de l' équation , toute valeur de X, comprise entre *(..)* , qui rend le premier membre égal à un entier. Le nombre de ces solutions, qu' on pourrait prendre aussi entre *(..)* , ne doit jamais surpasser l' exposant M, comme il vient d' être démontré ; mais d' après une solution telle que *(..)* , on peut faire plus généralement *(..)* , *(..)* étant un nombre entier positif ou négatif, et toutes les valeurs de X renfermées dans cette formule, satisferont à l' équation . (133) théorème. " soit toujours C un nombre premier, et P un polynome du degré M, lequel soit diviseur du binome *(..)* ; je dis qu' il y aura toujours M valeurs de X, comprises entre *(..)* et *(..)* , qui rendent ce polynome divisible par C. " car soit *(..)* , Q étant un autre polynome du degré *(..)* . Puisqu' il y a *(..)* valeurs de X, savoir *(..)* , qui rendent le premier membre divisible par C, il faut que chacune de ces valeurs rende P ou Q divisible par C. Parmi ces *(..)* valeurs, il ne peut y en avoir plus de M qui rendent P divisible par C, parce que P n' est que du degré M ; il ne peut non plus y en avoir moins de M, car alors il y aurait plus de *(..)* valeurs de X qui rendraient Q divisible par C ; ce qui est impossible, puisque Q n' est que du degré *(..)* . Donc le nombre de valeurs de X qui rendent P divisible par C, et qui sont comprises entre *(..)* , est précisément M. *remarque.* la même proposition aurait lieu, si P était diviseur de *(..)* , R étant un polynome d' un degré quelconque. (134) théorème. " si le nombre premier C est diviseur de *(..)* , N étant un nombre donné positif ou négatif, je dis que la quantité *(..)* doit être divisible par C ; et réciproquement si cette condition est remplie, il existera un nombre X (moindre que *(..)*) tel que *(..)* sera divisible par C. (on excepte le cas de *(..)* , et celui où N est divisible par C). "

p197

car 1 si C est diviseur de *(..)* , on aura, en omettant les multiples de *(..)* ; donc *(..)* . Le premier membre est divisible par C, donc le second doit l' être également. 2 si on suppose que soit divisible par C, je fais cette quantité *(..)* , ce qui donnera *(..)* . Mais si l' on fait pour un moment *(..)* , le second membre devient *(..)* , lequel est divisible par *(..)* . Donc *(..)* divise également le premier membre *(..)* . Donc (N 133) il y a nécessairement deux valeurs de X, moindres que *(..)* , qui rendent divisible par C ; ces deux valeurs n' en font proprement qu' une, parce qu' elles ne diffèrent que par leur signe. *remarque. nous avons démontré que N étant un nombre quelconque, et C un nombre premier qui ne divise pas N, la quantité (..) est toujours divisible par C ; cette quantité est le produit des deux facteurs (..) ; il faut donc que l' un ou l' autre de ces deux facteurs soit divisible par C ; d' où nous conclurons que la quantité (..) divisée par C, laissera toujours le reste (..) ou le reste (..) . (135)* comme les quantités analogues à *(..)* se *rencontreront fréquemment dans le cours de nos* recherches, nous emploîrons le caractère abrégé *(..) pour exprimer le reste que donne (..) divisée* par C ; reste qui, suivant ce qu' on vient de voir, *ne peut être que (..) .* lorsque *(..)* , on dit que N est un *résidu carré* de C, parce qu' alors *(..)* divisé par C, laisse le reste *(..)* , ce qui est la condition nécessaire pour que C soit diviseur de *(..)* ; au contraire, lorsque *(..)* , on dit que N est un *non-résidu carré* de C.

p213

(152) lemme. " le produit d' une somme de quatre carrés par une somme de quatre carrés, est semblablement la somme de quatre carrés. " il suffit, pour s' en assurer, de développer la formule suivante, qu' on trouvera être identique : *(..)* . Dans cette formule, on peut changer à volonté le signe de chacune des lettres qui y entrent, ce qui donnera plusieurs manières de décomposer en quatre carrés le produit dont il s' agit.

p214

remarque. ce beau théorème d' algèbre est encore dû à Euler ; il a été généralisé depuis par Lagrange dans les termes suivants : (mémoires de Berlin, année 1770). On voit par cette formule, que deux fonctions de la forme... *(..)* , B et C étant des coefficients constants, donnent pour leur produit une fonction semblable. Donc un nombre quelconque de semblables fonctions multipliées entre elles, donneraient pour leur produit une fonction semblable. (153) théorème. " tout nombre premier

A est de la forme *(..)* . " on a prouvé (N 151) qu' il existe toujours deux nombres T et U, tels que *(..)* est divisible par A . Mais si à la place de T et U on met *(..)* , le résultat *(..)* sera encore divisible par A ; on peut donc supposer que les premières valeurs de T et U sont moindres que *(..)* , ou qu' elles ont été rendues telles en en retranchant des multiples de A. Cela posé, si l' on fait *(..)* , on aura *(..)* . Considérons plus généralement l' équation *(..)* , dans laquelle chacun des nombres P, Q, R, S, sera supposé moindre que *(..)* , on aura *(..)* . Et d' abord si on avait *(..)* , il est clair que A serait égal à la somme de quatre carrés, et la proposition serait démontrée. Soit donc *(..)* , et parce que *(..)* est diviseur de *(..)* , il sera aussi diviseur de la quantité *(..)* étant pris à volonté. Supposons qu' on prenne

p215

ces indéterminées de manière qu' aucun des termes *(..)* , etc. N' excède *(..)* ; alors si l' on fait *(..)* , on aura *(..)* . Maintenant si au moyen de la formule du N 150 on multiplie la valeur de *(..)* par celle de *(..)* , on trouvera pour produit une somme de quatre carrés dont chacun est divisible par *(..)* ; de sorte qu' en divisant tout par *(..)* , on aura *(..)* . Cela posé, si on a *(..)* , la proposition sera démontrée ; mais si on a *(..)* , on procédera de la même manière pour obtenir un nouveau produit *(..)* exprimé par quatre carrés, et dans lequel on aura *(..)* . Continuant ainsi la suite des entiers décroissants A, *(..)* , etc., on parviendra nécessairement à un terme égal à l' unité ; donc alors le nombre premier A sera exprimé par la somme de quatre carrés. (154) théorème. " un nombre quelconque est la somme de quatre ou d' un moindre nombre de carrés. " c' est une conséquence immédiate de la proposition qu' on vient de démontrer, et du lemme qui la précède ; car un nombre quelconque étant le produit de plusieurs nombres premiers égaux ou inégaux, et chacun des facteurs étant de la forme *(..)* , si on multiplie deux facteurs entre eux, puis le produit des deux par un troisième, puis le produit des trois par un quatrième, etc. Jusqu' à ce que tous les facteurs soient employés, il est clair que les produits successifs seront toujours la somme de quatre carrés. Donc le produit final, qui est le nombre proposé, sera aussi la somme

p216

de quatre carrés, et pourra être représenté par *(..)* . Rien n' empêche d' ailleurs qu' un ou plusieurs des carrés *(..)* ne soient zéro ; donc un nombre quelconque est égal à la somme de quatre ou d' un moindre nombre de carrés. Nous remarquerons ici qu' une formule tirée de la théorie des fonctions elliptiques, fournirait un moyen très-simple et très-direct de démontrer la même proposition. On voit, en effet, dans le traité des fonctions

elliptiques, Tiii, P 133, que le développement de la puissance , donne la suite *(..)* . Il en résulte immédiatement que tout nombre *(..)* est la somme de quatre carrés impairs, d' où il est facile de conclure qu' un nombre quelconque est la somme de quatre carrés. L' identité dont il s' agit peut sans doute se démontrer par des considérations purement analytiques, et on obtiendrait ainsi la démonstration la plus simple qu' il soit possible de notre proposition. (155) il n' est point de nombre entier qui ne soit compris dans la formule *(..)* , mais ils peuvent, pour la plus grande partie, être représentés par la formule plus simple *(..)* . En général, on peut affirmer que " tout nombre impair est de la forme " *(..)* , excepté seulement les nombres *(..)* . " on excepte les nombres *(..)* , parce que si des trois termes P, Q, R , deux sont pairs et le troisième impair, la formule *(..)* sera de la forme *(..)* , et si les trois nombres P, Q, R sont impairs, la formule *(..)* sera de la forme *(..)* . Donc aucun nombre *(..)* ne peut être la somme de trois carrés. Si dans la formule *(..)* on suppose deux termes égaux, on aura une nouvelle formule *(..)* , laquelle est encore très-générale ; car on peut affirmer que " tout nombre impair, sans exception, est de la forme *(..)* . " ces propositions seront mises ci-après dans un plus grand jour : observons quant à présent, que les deux formes *(..)*

p217

dont il est question dans ces théorèmes, ont entre elles cette relation, que le double de l' une reproduit l' autre. C' est ce qu' on voit par les formules *(..)* . (156) la proposition que nous avons démontrée dans ce paragraphe, fait partie d' une propriété générale des nombres polygones découverte par Fermat, et dont nous ne pouvons nous dispenser de faire mention. Mais d' abord il faut, en faveur de quelques lecteurs, expliquer ce qu' on entend par nombres polygones. Si on considère différentes progressions arithmétiques qui commencent toutes par l' unité, et dont les raisons soient successivement 1, 2, 3, 4, etc. ; si ensuite, par l' addition des termes de chaque progression, on forme une suite correspondante, ces différentes suites composeront ce qu' on appelle *les nombres polygones* ; elles sont comprises dans le tableau suivant : *(..)* .

p299

suite des théorèmes contenus dans les tables précitées. *(228) théorème général. " soit (..) l' une des formes linéaires qui conviennent aux diviseurs de (..) , je dis que tout nombre premier compris dans la forme (..) sera nécessairement diviseur de la formule (..) , et sera par conséquent de l' une des formes quadratiques (..) qui répondent à la forme linéaire (..) . " ainsi en prenant dans la table Vii l' exemple de la formule (..) , et*

choisissant dans cet exemple les formes linéaires qui répondent au diviseur quadratique (..) , on peut affirmer que tout nombre premier de l' une des formes (..) , est diviseur de (..) , et conséquemment doit être de la forme (..) . Par un autre exemple pris dans la même table, on peut affirmer que tout nombre premier de l' une des formes (..) est diviseur de (..) , et par conséquent doit être de la forme (..) . La démonstration de ce théorème a été donnée ci-dessus, lorsque C est un nombre premier ou double d' un nombre premier ; elle peut être aussi établie sans difficulté pour toute valeur de C, si le nombre premier A de la forme (..) est en même temps de la forme (..) , car alors il est nécessaire que le nombre A divise la formule (..) , ou la formule (..) . Or si on cherche les formes linéaires des diviseurs de (..) , ces formes seront trouvées différentes de celles des diviseurs de (..) ; donc le nombre A, s' il est de l' une de ces dernières formes, ne peut diviser (..) ; donc il divisera nécessairement (..) , et sera par conséquent de l' une des formes quadratiques qui répondent à ces formes linéaires.

p300

Le même raisonnement n' aurait plus lieu si A était de la forme ; il est même incomplet dans le cas de (..) , parce qu' il suppose le développement effectif des diviseurs linéaires tant de la formule (..) que de la formule (..) ; c' est pourquoi il convient de suivre une autre route pour parvenir à la démonstration générale de la proposition.

p361

(283) théorème Ii. " si le nombre C est premier ou double d' un premier, la formule (..) aura autant de diviseurs quadratiques trinaires qu' il y a de formes trinaires du nombre C. " car chaque diviseur trinaire de la formule (..) répond à une forme trinaire de C qui s' en déduit immédiatement, et réciproquement chaque forme trinaire du nombre C conduit à un diviseur trinaire correspondant de la formule (..) . S' il n' y avait donc pas un égal nombre des uns et des autres, il faudrait ou que deux formes trinaires de C répondissent au même diviseur quadratique de la formule (..) , ou que deux diviseurs quadratiques différents répondissent à la même forme trinaire de C. La seconde hypothèse n' a lieu pour aucune valeur de C (N 274), et la première n' a pas lieu, en vertu du théorème précédent, puisque C est premier ou double d' un premier. Donc, etc. (284) théorème Iii. " si le nombre C est premier ou double d' un premier, chaque diviseur trinaire de la formule (..) ne pourra se décomposer que d' une seule manière en trois carrés, c' est-à-dire ne pourra avoir qu' une seule forme trinaire. " car si un même diviseur quadratique de la formule (..) avait plusieurs formes trinaires, il faudrait,

d' après le théorème précédent, que ces diverses formes répondissent à une même valeur trinaire

p362

de C. Mais on a prouvé (N 277) qu' une valeur trinaire donnée de C ne peut répondre à deux formes trinaires différentes d' un même diviseur quadratique, que lorsque celui-ci est de l' une des formes (..) , et qu' en même temps les coefficients extrêmes sont l' un et l' autre plus grands que 2. Or dans tous ces cas, il est facile de voir que le nombre C, représenté successivement par (..) , ne peut être ni premier, ni double d' un premier. Donc, etc. remarque. *cette proposition aurait également lieu si C ou (..) était une puissance d' un nombre premier ; elle contient ainsi une propriété qui convient exclusivement aux puissances des nombres premiers ou à leurs doubles, et qui peut servir à distinguer ces nombres de tous les autres.*

p371

(295) théorème Viii. " au contraire si un seul nombre (..) renfermé dans le diviseur quadratique (..) , est tel que C ne divise pas (..) , je dis que tout nombre N renfermé dans le même diviseur quadratique, est tel aussi que C ne peut diviser (..) , au moins en supposant N et C premiers entre eux. " car puisque C et N sont premiers entre eux, si C divisait (..) , il faudrait , suivant le théorème précédent, que C divisât aussi (..) , ce qui est contre la supposition. (296) nous appellerons, pour abréger , diviseur *réciproque* tout diviseur quadratique de la formule *(..)* , dont la propriété est telle que N étant un nombre quelconque compris dans ce diviseur, réciproquement C soit diviseur de *(..)* . Nous appellerons par opposition *diviseur* non -réciproque *tout diviseur quadratique qui ne jouit pas de cette propriété, ou qui n' en jouit que par rapport à quelques nombres particuliers N qui ont un commun diviseur avec C. Les conditions pour qu' un diviseur quadratique soit réciproque ou ne le soit pas, sont tellement précisées par les deux théorèmes précédents, qu' on pourra toujours décider promptement, et presqu' à la seule inspection, si un diviseur quadratique donné est réciproque ou non.*

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Administração
Baixar livros de Agronomia
Baixar livros de Arquitetura
Baixar livros de Artes
Baixar livros de Astronomia
Baixar livros de Biologia Geral
Baixar livros de Ciência da Computação
Baixar livros de Ciência da Informação
Baixar livros de Ciência Política
Baixar livros de Ciências da Saúde
Baixar livros de Comunicação
Baixar livros do Conselho Nacional de Educação - CNE
Baixar livros de Defesa civil
Baixar livros de Direito
Baixar livros de Direitos humanos
Baixar livros de Economia
Baixar livros de Economia Doméstica
Baixar livros de Educação
Baixar livros de Educação - Trânsito
Baixar livros de Educação Física
Baixar livros de Engenharia Aeroespacial
Baixar livros de Farmácia
Baixar livros de Filosofia
Baixar livros de Física
Baixar livros de Geociências
Baixar livros de Geografia
Baixar livros de História
Baixar livros de Línguas

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo