Jacques-Olivier Piednoir

Le pays des nombres premiers

Guide de voyage

"J'ai décidé de composer un livre concis pour ceux qui s'adonnent aux belles-lettres, afin de les aider à éclaircir ce qui était impénétrable et à faciliter ce qui était difficile. J'ai voulu qu'il enferme ce qui est subtil dans le calcul et ce qui en est le plus noble, ce dont les gens ont nécessairement besoin dans tout ce qu'ils traitent les uns avec les autres"

Muḥammad ibn Mūsā al-Khwārizmī, (780-850)

Notes de l'auteur :

Encore un livre sur les nombres premiers ! J'ai ressenti le besoin d'écrire celui-ci car je ne trouvais pas ce je recherchais dans les livres que j'avais lus :

- Des livres qui contenaient des anecdotes passionnantes mais peu de formules mathématiques.
- Des livres remplis de formules mathématiques qui s'adressent plus à des étudiants en bachelor ou master ou à des passionnés de mathématiques.

J'ai donc décidé d'écrire le livre que j'aurais voulu lire ! Un livre pour curieux ou nostalgiques des mathématiques apprises durant leurs années d'études. L'idée était de choisir un sujet passionnant dont les prérequis étaient du niveau terminale scientifique. L'arithmétique et ses nombres premiers se prêtent bien à ce défi. De plus, c'est un sujet passionnant. Les formules concernent le plus souvent les nombres entiers et les quatre opérations de base. C'est un livre à la carte. Si vous pratiquez toujours les mathématiques ou si vos souvenirs sont récents, certains chapitres de remise à niveau ne seront pas nécessaires. Lisez les en diagonale ! Pour d'autres lecteurs, certaines démonstrations nécessiteraient une étude approfondie dans laquelle ils ne souhaitent pas s'investir. Je leur suggère de les parcourir rapidement, juste pour apprécier l'élégance ou le caractère innovant du raisonnement. Les nombres premiers sont un prétexte. L'ambition de cet ouvrage est de vous donner envie de vous replonger dans le langage des mathématiques, dans le raisonnement logique et de vous donner envie de découvrir ou redécouvrir le monde merveilleux des mathématiques qui forment l'ossature de notre réalité.

Table des matières

Préambule

L’os d’Ishango

Les chasseurs sont partis à l’aube. Canongo, le sorcier de la tribu, est resté au campement. Assis en tailleur dans l’ombre du manguier, il contemple pour la centième fois les vingt cailloux aux reflets d’ambre polis par le ruisseau. Ils ont tous la même taille et presque la même forme. Canongo veut vérifier encore une fois. Il essaye de répartir des combinaisons de ses vingt pierres en tas égaux. Il commence par un tas de 10 pierres. Pas de problème, rapidement il constate que deux tas de cinq pierres remplissent ses conditions. D’ailleurs les chasseurs étaient dix ce matin, cinq sont partis à l’ouest et cinq à l’est. Il réessaye avec onze pierres et encore une fois son visage s’assombrit. Il ne trouve pas de répartition des pierres amenant à des tas égaux. Il passe vite à douze pierres. Son visage s’éclaircit. Comme il l’avait constaté hier, les solutions sont multiples : deux tas de six, quatre tas de trois et même trois tas de quatre. Il sait que le prochain essai sera difficile, treize pierres. Il essaye mais impossible de trouver une distribution équitable. Lassé, il sait que comme hier et avant-hier, quatorze, quinze, seize pierres seront faciles à répartir ainsi que dix-huit et vingt mais que dix-sept et

dix-neuf lui résisteront. Onze, treize, dix-sept, dix-neuf, il y a de la magie dans ces groupes de pierres. D'ailleurs, quelles que soient les pierres choisies, le résultat est le même. Ces nombres sont magiques. Ils semblent si forts que l'on ne peut les diviser. Il se saisit de son os venant d'un lion, celui avec un morceau de quartz au bout et grave quatre groupes d'incisions en forme de traits dans la longueur de l'os. Onze incisions, treize incisions, dix-sept incisions et finalement dix-neuf au bout de l'os.
C'est son troisième os, les deux premiers lui permettent de compter et d'additionner grâce à leurs groupes d'encoches. Mais celui-ci sera différent. Il est magique. C'est l'os indivisible, l'os premier qui veillera sur le groupe.
20 000 ans passent, nous sommes en 1950 après J-C. Canongo est mort depuis longtemps. La région s'appelle Ishango et fait partie du Congo. Le géologue belge Jean de Heinzelin de Braucourt (1920-1998) effectue des fouilles au bord du Lac Edouard. Il découvre les traces d'un campement et avec minutie ses équipes extraient au pinceau trois os gravés d'incisions. Ces os sont les premières preuves que les homo-sapiens de la région avaient des notions d'arithmétique et peut-être même avaient reconnu la spécificité des nombres premiers en notant sur un os les seuls nombres premiers entre dix et vingt.

Frank Nelson

Nous sommes maintenant en 1903, lors d'une séance de "l'American Mathematical Society". Personne ne se doute que cette séance deviendra mémorable. Frank Nelson Cole, né en 1861, se lève. C'est son tour de prendre la parole dans cette session dédiée à l'étude des nombres. Frank n'est pas un grand orateur. Ca tombe bien ; il ne va pas dire un mot. Pourtant il va résoudre devant les yeux ébahis de ses illustres collègues un problème vieux de vingt-cinq ans. Le mathématicien François Edouard Anatole Lucas (1842-1891) avait prouvé en 1876 que le soixantième nombre de Mersenne n'était pas premier. Un nombre de Mersenne est une puissance de deux, c'est-à-dire deux multiplié plusieurs fois par lui-même, auquel on retranche une unité. Par exemple $M_3 = 2^3 - 1 = 2 \times 2 \times 2 - 1$. Edouard Lucas avait donc prouvé que M_{60}, 2 multiplié soixante fois par lui même auquel on retranche 1 et qui peut s'écrire $2^{60} - 1$ ou bien 147 573 952 589 676 412 927 n'était pas premier. Beaucoup des nombres de Mersenne sont premiers. Certains mathématiciens pensaient même détenir ainsi une formule pour générer des nombres premiers. Mais rapidement on constata que

$M_{11} = 2^{11} - 1 =$ 211 − 1 = 2047 = 23 × 89

n'est pas premier car il est multiple de deux nombres. En effet à ce point de l'histoire il est temps de définir un

nombre premier, c'est un nombre qui n'est divisible que par 1 et lui-même. Donc les mathématiciens savaient depuis plus de 20 ans que M_{60} n'est pas premier mais ils étaient incapables de trouver les nombres qui multipliés entre eux donnerent M_{60}. On appelle ce calcul la factorisation. Revenons à Frank Nelson, sans dire un mot il se plante devant le tableau, tourne le dos à ses collègues et écrit
147 573 952 589 676 412 927 sur la partie gauche du tableau. Sur la partie droite, il commence à effectuer à la main la fastidieuse multiplication 93 707 721 × 761 838 257 287. Il ne dit pas un mot pendant une heure. A la fin de cette heure le nombre inscrit à gauche est égal au résultat de la multiplication :
147 573 952 589 676 412 927 = 93 707 721 × 761 838 257 287
C'est sous un tonnerre d'applaudissements que s'achève son intervention.
On créa le prix Frank Nelson en son honneur. Honneur bien mérité car Frank Nelson admit que ce calcul lui avait pris 3 années de dimanche !

Les jumeaux calculateurs

"L'homme qui prenait sa femme pour un chapeau" [1] est un livre publié en 1985 par Oliver Sacks, neurologue d'origine anglaise. Dans cet ouvrage l'auteur décrit les affections les plus bizarres qu'il a rencontrées dans sa carrière. Un chapître est consacré à deux jumeaux

autistes. Leurs communications se limitaient à des échanges de nombres de 6 chiffres. L'un disait "100019" et après quelques secondes l'autre affichait un visage réjoui. Oliver Sacks comprend que les nombres qu'ils échangent et qui semblent les plonger dans une sorte de jubilation, tel un oenologue dégustant un bon vin, sont des nombres premiers. Il leur soumet un nombre premier de 8 chiffres comme 12345713. Les jumeaux sont interloqués. Ils entrent dans une longue méditation, longue mais pas trop, moins de 1 heure et ensuite éclatent de rire. Pourquoi ces personnes autistes, avaient-ils choisi ce moyen de communication ? Comment pouvaient-ils reconnaître mentalement en quelques secondes un nombre premier de 6 chiffres, en moins de 1 heure un nombre premier de 8 chiffres alors que cela exige des dizaines de milliers de multiplications et de divisions ? Personne ne le sait. Leurs cerveaux étaient-ils câblés pour reconnaître ces nombres à l'aide d'un algorithme qui nous est inconnu ? C'est toujours un mystère. Pour ces jumeaux les nombres premiers "existaient" et étaient une source de joie inépuisable.

On pourrait écrire un livre entier sur les anecdotes liées au nombres premiers. Ce n'est pas l'objectif alors plongeons nous dans le vif du sujet en abordant une question :
Quel est le point commun entre ces nombres ?

2, 3, 5, 11, 643, 709, 947, 1001587,
170141183460469231731687303715884105 72.

Réponse : Ils sont premiers. Premier de quoi ? Premier de la classe ? Premier de cordée ?
“Nombre premier” dans ce contexte, comme nous l’avons vu plus haut, veut dire qu’ils n’ont pas de diviseurs autre que 1 et eux-mêmes. 5 et 11 c’est évident, 709, 947 pourquoi pas, mais :
170141183460469231731687303715884105 72 !
C’est un très très grand nombre, des milliards de milliards de milliards. Il est étonnant que parmi tous les nombres qui le précèdent, aucun ne le divise. Il y a même de plus grands nombres premiers. En fait si vous croyez avoir trouvé le plus grand, il y en aura toujours un plus grand. C’est Euclide, trois siècles, avant Jésus-Christ qui l’a démontré : “*les nombres premiers sont plus nombreux que n'importe quelle multitude de nombres premiers proposée*”.

Aujourd’hui avec tous nos ordinateurs, capables d’effectuer des milliards de divisions, le plus grand nombre premier connu est $2^{82\,589\,933} - 1$. Vous l’avez reconnu, c’est un nombre de Mersenne. S’il était écrit en système décimal comme nous en avons l’habitude, il comprendrait 25 millions de chiffres !

Pourquoi le qualificatif “*premier*”. Regardons la définition dans la neuvième édition du dictionnaire de l’Académie Française. Les académiciens ont choisi plusieurs sens au mot “premier” :

1. Qui est situé devant les autres dans l’espace.
Le premier de cordée, situé le plus haut, qui ouvre la voie. Ce n’est pas approprié pour les nombres premiers. Ils sont hors de l’espace ! De plus cela semble indiqué qu’il n’y a qu’un nombre premier, ce qui est loin d’être le cas !

2. Qui se présente avant les autres dans une série.
0, 1, 2, 3, 4 sont les premiers nombres dans la série des nombres entiers. Mais ce ne sont pas tous des nombres premiers. Le problème des nombres premiers, encore non résolu, est justement qu’il n’y a pas de série. Ils apparaissent au hasard dans un chaos apparent !

3. Qui l’emporte sur les autres en importance, en qualité, en dignité.
On se rapproche ! En effet les nombres premiers sont spéciaux. Il y en a à la fois peu et beaucoup. Leur absence de diviseur autre que 1 et eux-mêmes est une caractéristique unique. Si unique que depuis plus de 2000 ans, des grands génies comme Euclide, Gauss, Euler, Riemann leur ont dédié leur vie. Mais ce n’est pas

suffisant pour “l’emporter sur les autres en importance…”.
Il y a d’autres nombres aux caractéristiques uniques. Certains sont même appelés “*nombres parfaits*”. Un nombre parfait est un nombre égal à la somme de ses diviseurs : 28 est divisible par 1, 2, 4, 7 et 14, donc ses diviseurs sont 1, 2, 4, 7, 14. Si l’on fait la somme de ces nombres 1 + 2 + 4+ 7 + 14 on trouve 28. Donc 28 est un nombre parfait. Un nombre premier n’est pas parfait car il n’a comme diviseurs que 1 et lui même donc la somme de ses diviseurs donne le nombre qui le suit. Pas glorieux !

4. Qui précède tous les autres dans le temps.
Un peu comme les arts premiers. Evidemment ce n’est pas le cas des nombres premiers. La caractéristique des nombres premiers n’est pas temporelle. Les nombres sont et ont toujours été. C’est pourtant dans une sous catégorie de cette définition que les immortels de l’académie citent les nombres premiers : “*Qui date de l’origine, originel.”*
Si on ne tient pas compte de la notion temporelle, cette définition peut aider à caractériser les nombres premiers. En effet, Euclide a démontré que tout nombre entier naturel peut s’écrire sous la forme d’un produit de nombres premiers :
Par exemple :
- $24 = 2 \times 2 \times 2 \times 3$

- $100 = 2 \times 2 \times 5 \times 5$
- $3692 = 2 \times 2 \times 13 \times 71$

Ce sont un peu les pièces d'un lego qui permet de construire tout autre nombre à l'aide de la multiplication. Le seul ennui est qu'il y a une infinité de nombre premiers, alors il faudrait une grande boîte de Lego !
Nous verrons plus loin dans ce livre que cette décomposition est unique. Cela avait échappé à Euclide ! Ou bien il l'avait deviné mais n'avait pu le prouver.

Les anglophones ne disent pas "first number" mais "*prime number*". Le webster indique que la signification principale de "prime" est "*first in rank, authority, or significance* . On rejoint ici la troisième dé

finition de l'Académie Française : "*Qui l'emporte sur les autres en importance, en qualité, en dignité".*

Revenons aux grecs puisque c'est à Euclide que l'on doit la théorie des nombres. Ils utilisaient le terme **πρῶτος** qui a les mêmes définitions que "premier" en Français. Donc rien d'original de ce coté là.

Quittons la linguistique, qui ne nous apprend pas grand chose sur les nombres premiers et revenons à nos moutons car il n'y a pas qu'un mouton**s** comme disait Mr Tournadre, mon professeur de mathématiques au collège et au lycée, qui a été un des premiers à enseigner à titre expérimental les mathématiques dites modernes. C'est à

lui que je dédie ce livre car il m'a fait découvrir un univers fabuleux hors du temps et de l'espace. Je remercie aussi Jean-Claude Raimbault , spécialiste des mots et intransigeant sur l'orthographe et la grammaire, qui m'a fait l'honneur de relire et corriger ce livre. Ce **s** dans l'expression "car il n'y a pas qu'un mouton**s**" doit heurter son sens aigü de la grammaire. Mais il est justifié mathématiquement, en effet s'il n'y a pas qu'un mouton, c'est qu'il y en a plusieurs !

Revenons aux mathématiques et regardons la définition de wikipédia ?
*"Un **nombre premier** est un entier naturel qui admet seulement deux diviseurs distincts entiers et positifs : 1 et le nombre considéré lui-même."*

Cela réclame un peu d'explication, les termes *entiers naturels* et *diviseurs* apparaissent en bleu sur la page de l'encyclopédie. Cela veut dire que l'on peut trouver les définitions de ces termes en suivant les liens. Oublions Wikipedia, cela nous emmènerait trop loin et revenons à des définitions plus élémentaires :

Entier naturel :
Un *entier naturel* est un nombre entier positif, c'est à dire que l'on exclut tous les nombres à virgule et les nombres négatifs. Pour faire simple :

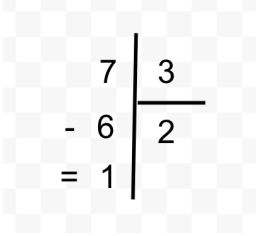
Ce sont les nombres que l'on utilise pour compter les choses. 0,1,2,3,....1000,....

Diviseur :

Un nombre entier est appelé *diviseur* d'un second nombre entier si la division du second par le premier donne un reste nul.

On a tous appris à l'école primaire à écrire la division sous la forme $7 \div 3 = 2 \times 3 + 1$. Savez vous comment on appelle ce signe " $\div$ " ?

Un obèle pontué ! Il tombe en désuétude et est maintenant remplacé par "/". On l'utilisera dans ce livre, pour bien différencier la division euclidienne qui à partir de deux nombres entiers : le dividende et le diviseur produit 2 nombres entiers : le quotient et le reste, de l'opération de division qui produit un seul nombre : une fraction ou nombre à virgule (voir plus loin). La méthode pour trouver le quotient et le reste consiste à "poser" la division comme disent les professeurs des écoles :



6 est un diviseur de 24 car $24 \div 6 = 4$. Le reste est nul, on ne l'écrit même pas. Mais il est là

$24 \div 6 = 4 + 0$. 6 n'est pas un diviseur de 25 car $25 = 4 \times 6 + 1$. Le reste est 1.

7 est premier. C'est un entier positif (entier naturel disent wikipédia et les mathématiciens) et il n'est divisible que par 1 et par 7. C'est à dire que si vous essayez de le diviser par tout autre nombre entier, le reste de la division ne sera jamais nul. Par exemple 7 divisé par 3 donne un quotient de 2 et un reste de 1, ainsi que pour 2, 4, 5, et 6 le reste ne sera jamais nul. Ce n'est pas la peine d'essayer les nombres supérieurs à 7, le quotient est 0 et le reste 7.

Comment prouver qu'un nombre est premier ?
La méthode la plus simple est d'essayer de trouver un diviseur. Si nous n'en trouvons pas alors le nombre est premier. On peut ainsi, à l'aide de divisions successives, observer que 31 est premier mais que 33 ne l'est pas. En effet le diviseur d'un nombre est toujours plus petit que ce nombre, il suffit donc d'essayer tous les nombres inférieurs au candidat à la *primalité* ! Ainsi pour montrer que 37 est premier, on effectue 35 divisions (pas besoin d'essayer 1 et 37) et on constate que le reste n'est jamais nul. Donc 37 est premier.

Si on utilise la même méthode fastidieuse pour 33, on s'arrête rapidement en essayant 3 car $33 = 3 \times 11$. Le reste est nul ! Donc 33 n'est pas un nombre premier, il est divisible par 3 et 11.

Il n'y a donc rien de compliqué dans la définition d'un nombre premier et dans la méthode utilisée pour décider si un nombre donné est premier ou pas. Le livre pourrait s'arrêter là. Vous savez tout ce qu'il faut savoir sur les nombres premiers !
Pourtant les nombres premiers ont fasciné les mathématiciens pendant plus de 3000 ans. La première preuve incontestable de l'intérêt des hommes pour ces nombres remonte à Euclide (300 avant J.-C.). Euclide définit les nombres premiers de manière formelle et démontre de nombreuses propriétés les concernant dans son œuvre : "Les Éléments". Une œuvre monumentale que les mathématiciens étudieront pendant des siècles. Elle comprend treize livres et fait le point sur les connaissances en arithmétique et en géométrie de cette époque. Euclide a été le premier à compiler et à formaliser les connaissances sur le domaine des nombres entiers. Mais ils ont été étudiés bien avant.
On trouve des résolutions de problèmes de calcul sur des tablettes Mésopotamiennes datant de plus de 2000 ans avant notre ère ou sur des papyrus égyptiens encore plus anciens. De tout temps, les humains ont eu besoin de compter et de diviser. Combien de flèches

avons-nous ? Comment les répartir entre les 5 chasseurs d'un groupe ? Comment diviser mon champ en 3 parcelles pour mes 3 enfants sans en léser un seul ?

Pourquoi cet intérêt et cette fascination ?
Les plus grands génies des mathématiques Euclide, Gauss (1777-1855), Riemann (1826-1866) ainsi que Alain Connes (né à Marseille en 1947 et professeur au collège de France) ont tous été passionnés par l'étude des propriétés de ces nombres. Sophie Germain (1776-1831) a même donné son nom à une catégorie de nombres premiers. Ils et elles ont passé des années à explorer l'univers des nombres dans lequel les nombres premiers semblent apparaître sans ordre apparent comme des sommets émergeant des nuages. Jakob Kulik (1793-1863), professeur à l'université de Prague, a passé 20 ans de sa vie à calculer à la main la liste des premiers 100 millions nombres premiers. Il a pour cela effectué des centaines de milliers de multiplications et de divisions à la main sans calculateur !
Les mathématiciens ont cherché des formules pour générer les nombres premiers, des méthodes pour vérifier rapidement si un nombre est premier ou pas. Des théorèmes potentiels émergeaient de leurs cerveaux créatifs. Parfois leurs efforts et leurs génies étaient récompensés. Ils ont pu développer des raisonnements logiques prouvant la véracité de leurs intuitions. Souvent les cheminements de leurs raisonnements logiques ne

les amenaient pas à la preuve tant espérée mais leur permettaient en chemin de développer d'autres branches des mathématiques ou de tomber par hasard sur des propriétés des nombres premiers qu'ils ne soupçonnaient pas.

Pourquoi depuis plus de 3000 ans, tant de mathématiciens brillants ont dévoué leur vie et parfois ruiné leur santé à étudier un domaine qui n'avait pas d'application pratique et n'était d'aucune utilité pour les physiciens ?

Il a fallu attendre la création de l'internet et de ses infrastructures de communications nécessitant des méthodes de chiffrages infaillibles pour que l'étude des nombres premiers trouve enfin une application pratique. Récemment l'invention des monnaies numériques comme le bitcoin est aussi due à une particularité des nombres premiers que Gauss avait déjà notée : Il est très facile de multiplier deux grands nombres premiers mais, partant du résultat de la multiplication, il est très difficile de retrouver ces deux nombres premiers. On appelle "*décomposition en produits de facteurs premiers*" ou *"factorisation entière en nombres premiers",* le calcul qui, partant d'un nombre donné, trouve les nombres premiers dont il est le produit. Par exemple la décomposition en nombres premiers de 21 donne 3 et 7 car $21 = 3 \times 7$. Prenez 2 nombres premiers de 100 chiffres. Vous

pourrez obtenir rapidement le résultat de leur produit sur un ordinateur de bureau ou même sur un smartphone. Mais si vous partez du résultat de la multiplication, un giga nombre de plus de 200 chiffres, tous les ordinateurs de la terre réunis ne pourront pas retrouver les deux nombres premiers du produit. Rappelez vous l'anecdote du début : Edouard Lucas avait prouvé qu'un nombre de Mersenne M_{60} de 21 chiffres n'était pas premier. Il a fallu 21 ans pour que Nelson Cole trouve sa factorisation. C'est à dire les deux nombres dont le produit donnait M_{60}.

Savez-vous d'ailleurs comment on appelle un nombre suivi de 100 zéros ?
Un gogol ! C'est cette appellation qui a été à l'origine du nom du célèbre moteur de recherche Google. Ses créateurs ont voulu ainsi montrer que leurs algorithmes de recherches sur internet pouvaient travailler rapidement sur une grande quantité de données. La sécurité des communications et les monnaies électroniques dépendent de la multiplication des gogols !

Revenons à la question posée précédemment : pourquoi Euclide, puis Eratosthène (-200 avant J-.C.) et ensuite beaucoup plus tard Mersenne (1588-1648) et plein d'autres grosses têtes illustres (Pascal, Euler, Gauss, Riemann,...) ont ils été fascinés par ces nombres ?

La réponse est simple : "Parce qu'ils sont là !".

En effet, les nombres premiers n'ont pas besoin des êtres humains qui les étudient pour conserver leur propriété de non divisibilité. Sur Mars, prenez un tas de 107 pierres, il n'y pas moyen de les répartir en plusieurs groupes de pierres constitués du même nombre de pierres, car 107 est premier. Si une tempête ou une collision avec un astéroïde dispersait ces pierres en plusieurs groupes, après le passage de la catastrophe, il y aurait toujours un groupe dont le nombre de pierres est différent des autres. En effet si on trouvait un nombre n de groupes contenant le même nombre de pierres p alors le nombre de pierres total serait $p \times n = 107$ et p et n seraient diviseurs de 107. Ce qui est impossible car 107 est premier et n'a pas de diviseur ! Pas besoin d'êtres humains pour les étudier, les nombres premiers sont là. On pourrait même considérer qu'ils n'ont pas besoin de pierres ou d'autres objets que l'on peut compter pour que leur caractéristique unique soit incontestable.

Dans le livre de Carl Sagan "Contact" [2]. Des extra-terrestres envoient un signal dans l'univers contenant des impulsions groupées. Chaque groupe contient un nombre d'impulsions différent. Ces nombres sont les nombres premiers de 1 à 1000. Le premier groupe d'impulsions contient 2 bips, le deuxième 3, le troisième 5 et ainsi de suite jusqu'aux derniers qui

contiennent 991 et 997 bips. Pourquoi choisir cette suite d'impulsions ?
La répartition des nombres premiers n'est pas régulière. Elle n'obéit à aucune formule. Donc seule une intelligence, comprenant ce qu'est un nombre premier, a pu générer ce message. Tout autre signal contenant une régularité dans le nombre d'impulsions de chaque groupe aurait pu être généré par un phénomène physique naturel comme un quasar. Ce type d'étoile qui émet un signal périodique. Ainsi, si un être intelligent reçoit ce signal, il peut soupçonner qu'il a été émis par un autre être intelligent.

Mallory est un alpiniste né dans le comté de Cheshire en 1886. Il a disparu sur la crête nord de l'Everest en 1924. Dans une conférence de presse à New-York, les journalistes le harcelaient en lui posant toujours la même question : "Mais pourquoi voulez-vous escalader l'Everest ?". Il a répondu sèchement "Parce qu'il est là !".

De même le mathématicien de Cambridge G.H Hardy (1877-1947), auteur de "Mathematicians apology" [3], décrit le processus de découverte mathématique ainsi : "*J'ai toujours pensé que le mathématicien était un observateur qui distinguait au loin,dans la brume, des montagnes et notait ses observations*". Une fois, ses observations notées comme le ferait un alpiniste

préparant son voyage, le mathématicien entreprend de gravir ces sommets. De retour de son expédition, il décrit comment s'y rendre.
Citons François Vannucci qui dans [4] propose une explication à la fascination que les mathématiques exercent sur les êtres humains depuis des siècles : "Le cerveau humain ressent un besoin toujours renouvelé de connaissances qu'il satisfait grâce à l'invention toute spéculative du langage mathématique justement adapté à comprendre l'univers "

Notons que Vanucci parle d'invention toute spéculative, même si il admet que ce langage est particulièrement adapté à comprendre l'univers. En 1960, le physicien Eugène Wigner avait publié un célèbre article au titre provocateur : "La déraisonnable efficacité des mathématiques dans les sciences naturelles". G.H Hardy parle de découvertes et d'observations. Les mathématiques et en particulier le sujet qui nous intéresse ici, l'arithmétique et ses nombres premiers sont un continent qui existe en dehors de notre réalité physique et que le mathématicien va découvrir. Ses choix d'observations, ses interprétations, son parcours viennent de son intuition. Le parcours de la voie choisie qui mène au sommet est du domaine de la déduction et obéit aux lois strictes de la preuve mathématique. Ces règles contraignent sa progression. De même que la gravité empêche l'alpiniste de voler pour atteindre

directement le sommet. Il devra planifier, trouver les bons outils et ensuite parcourir des chemins et des voies semés d'embûches.

Vous l'avez sans doute deviné, les nombres premiers sont un prétexte. Il y a de nombreux livres sur ces nombres hors du commun et d'excellents cours pour tous niveaux scolaires. J'ai choisi ce domaine car les énoncés sont accessibles à tout le monde. Les pré-requis sont simples. Il suffit de comprendre les opérations de base sur les nombres entiers apprises à l'école primaire : l'addition, la multiplication, la division. Les montagnes sont proches , pas besoin de télescope ou de prendre des avions pour rejoindre un camp de base et les contempler. Il suffit d'observer avec les bons outils et de noter ses observations avec le bon vocabulaire. Ensuite il faut comprendre les méthodes de déplacement dans cette chaîne de montagne que l'on appelle "Arithmétique". Ce sera fait dans ce livre sans compromis, sans analogie ou "comparaison qui semblent raison". Les chapitres suivants vont introduire le vocabulaire utilisé pour les observations que l'on appelle "énoncés", introduire les outils de base de la randonnée et de l'escalade (les crampons, les mousquetons,...) qui sont les objets élémentaires manipulés par les mathématiciens. Ils vont insister sur le raisonnement logique et la méthode de la preuve qui sont les techniques d'approche et d'escalade. L'objectif de ce

livre est de vous transformer en mathématicien avide de découvrir un nouveau monde.

Bien sûr l'observation et la connaissance des objets ainsi que les descriptions de paysages sont plus aisées que la randonnée et l'escalade. C'est pourquoi nous commencerons par là. Nous aborderons ensuite les notes prises par les mathématiciens depuis Euclide décrivant les théorèmes importants sur les nombres premiers. Et pour les plus courageux nous nous attaquerons à la randonnée vers le camp de base et l'escalade que sont les démonstrations de ces théorèmes. L'Everest de ce livre sera la démonstration du Postulat de Bertrand. Ne vous inquiétez pas, nous prendrons le temps d'y arriver tranquillement.
En parcours, nous reviendrons sur un point mentionné au début de ce préambule. A quoi servent les nombres premiers ? Alors nous étudierons comment ce domaine sans application pratique a trouvé une utilité révolutionnaire dans le domaine de la cryptologie sur laquelle reposent les infrastructures de l'internet et de nouveaux types de transactions financières comme les crypto-monnaies.

La chaîne des nombres premiers :

Devant ce paysage, le mathématicien décrit les théorèmes qu'il voit. Il énonce des conjectures qu'il devine dans la brume. Il planifie sa démonstration en passant par un plateau enneigé. Il doit bien sûr se munir de l'équipement nécessaire.

L'équipement :

Mathématicien bien préparé pour une démonstration difficile

Vous êtes prêts, intéressés, intrigués au moins ? Alors on y va !

Plan

La première partie est une introduction au langage des mathématiques. Elle peut être rapidement parourue par ceux qui ont une bonne connaissance de la syntaxe utilisée dans les énoncés mathématiques. Cette partie permet aussi de se familiariser avec les notions d'énoncés, d'axiomes et de démonstrations. A une époque où les "fake news" sont courantes. Il est réconfortant de voir que les mathématiques possèdent une *syntaxe* et une *grammaire* qui permettent de vérifier le *raisonnement logique*. A partir des *axiomes* (vérités premières) le raisonnement mathématique valide des *énoncés*. Il n'y pas de place pour l'ambiguïté ou les déductions fallacieuses.
Cela paraît évident aujourd'hui pour ceux qui ont "subi" les cours de mathématiques au collège et au lycée. Mais cela n'a pas toujours été le cas, l'arithmétique et l'étude des nombres premiers ont commencé il y a très longtemps. A une époque où certains grands mathématiciens comme Euclide ou même plus récemment Pierre de Fermat ($XVII^{ème}$siècle) n'avaient pas la même rigueur logique dans leurs raisonnements, ni la même volonté de partager leurs connaissances. Ils ont parfois présenté comme vrais certains énoncés en disant qu'ils en avaient la preuve. Ces énoncés ont donc reçu le

statut de théorèmes. Alors qu'aujourd'hui ils restent encore sans démonstration rigoureuse.
Ainsi Pierre de Fermat (XVII^{e} siècle) annonça dans la marge d'un livre de Diophante : "Il est impossible de partager soit un cube en deux cubes, soit u*n bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir*". Ce qui veut dire que l'on peut trouver un nombre dont le carré est la somme de 2 carrés comme par exemple : $5^2 = 3^2 + 4^2$; en effet $25 = 9 + 16$. mais il n'est pas possible de trouver 3 nombres x,y et z tel que $z^3 = x^3 + y^3$.
Il a fallu attendre 350 ans pour que Andrew Wyles (né à Cambridge en 1953) utilisant des outils mathématiques non découverts à l'époque de Fermat trouve une démonstration. Celle-ci fait plus de 180 pages ! Tous les mathématiciens s'accordent sur le fait que Pierre de Fermat n'avait pas trouvé de démonstration.

Le film "le théorème de Marguerite" réalisé en 2023 par Anna Novion met en scène une jeune doctorante, jouée par Ella Rumpf, qui s'attaque à la démonstration de la conjecture de Goldbach. Celle-ci a été formulée en 1742 par Christian Goldbach (1690-1764). Cet énoncé n'a toujours pas été démontré. C'est pourquoi on l'appelle

“conjecture” et non “ théorème”’. C’est l’un des plus vieux problèmes non résolus de la théorie des nombres. Son énoncé est d’une incroyable simplicité : “tout nombre pair supérieur à 2 peut s’écrire sous la forme de l’addition de 2 nombres premiers”. Par exemple :
$14 = 3 + 11, 50 = 3 + 47$,…
Des ordinateurs puisants ont cherché un nombre pair qui ne pouvait pas s’écrire sous la forme de l’addition de 2 nombres premiers ; Ils n’ont pas réussi. L’énoncé semble vrai, mais personne n’a pu en trouver une preuve rigoureuse.

Pendant longtemps, l’intuition suffisait à déclarer qu’un énoncé était vrai. C’était aux autres mathématiciens de prouver qu’il était faux. Depuis Gauss et ses contemporains, la charge de la preuve a été retournée. Un énoncé est considéré comme faux tant qu’il n’a pas été prouvé par une suite de déductions obéissant à des règles formelles et répertoriées. Il y a un code de la démonstration, comme il y a un code de la route. Ce code décrit les progressions autorisées pour passer d’un énoncé vrai à un autre énoncé que l’on pourra aussi considérer comme vrai. Gauss a été un des premiers mathématiciens extrêmement rigoureux dans la valeur de la preuve. Il a laissé après sa mort beaucoup de théorèmes qu’il n’avait pas publiés car il n’était pas totalement sûr de la validité de leurs démonstrations.

Une fois cette syntaxe et cette grammaire des mathématiques présentées, le livre introduit un concept clé des mathématiques découvert au XIXème siècle qui a permis d'immenses progrès dans la compréhension des nombres premiers : la théorie des ensembles et des groupes. Ainsi qu'une fonction importante dans l'étude des nombres premiers : le logarithme qui avec sa baguette magique transforme une multiplication en addition. Peu de gens savent ce qu'est une croissance logarithmique pourtant ils ont tous entendu parler de la croissance réciproque : la croissance exponentielle qui est aussi rapide que celle du logarithme est lente. Nous aborderons dans cette même partie la définition de ce qui constitue un raisonnement logique. Nous aurons donc appris la syntaxe, la grammaire et la méthode pour construire des démonstrations.

La deuxième partie présente directement, sans démonstration, les théorèmes fondamentaux de l'arithmétique concernant les nombres premiers. Cette partie est un peu comme une table d'orientation décrivant les sommets qui vous entourent dans le paysage des nombres premiers.
Pourquoi sans démonstration ? Elles viendront plus tard, pour ceux qui veulent approfondir le domaine et surtout contempler des joyaux du raisonnement de l'esprit humain. Rappelez vous les démonstrations sont les voies qui mènent du point de départ (les axiomes) aux

sommets des montagnes (les théorèmes). Certains voudront les parcourir, d'autres se contenteront de les survoler.

La troisième partie s'intéresse à la répartition des nombres premiers (Gauss $18^{ème}$ siècle, Riemann $19^{ème}$ siècle). En effet, il y a beaucoup de nombres premiers. Euclide a énoncé: *"les nombres premiers sont plus nombreux que n'importe quelle multitude de nombres premiers proposée"*.
Aujourd'hui on dirait qu'il y a une infinité de nombres premiers. Mais les grecs de l'antiquité comme de nombreuses générations suivantes avaient des problèmes avec la notion d'infini. Pour eux l'infini n'existait pas en mathématiques, on ne pouvait y faire référence, un peu comme Voldemort dans Harry Potter !

Mais comment, ces nombres si nombreux au point que l'on n'en voit jamais le bout, sont-ils répartis ?
Y a t'il une régularité, des règles cachées dans cet apparent chaos ?
Peut-on calculer le nombre de nombres premiers dans un intervalle donné ?
Connaissant un nombre premier peut-on calculer le suivant ?

Ces questions, toujours sans réponse, constituent l'essentiel des recherches sur les nombres premiers des 3 derniers siècles.

En effet le chaos est rare en mathématique, les mathématiciens sont là pour découvrir les règles qui sous-tendent un chaos apparent. Prenons par exemple les nombres pairs, il y en a aussi une infinité. Quel que soit le nombre pair que l'on choisit, on peut toujours en trouver un plus grand. Mais leur répartition est simple : un nombre sur deux est pair, les autres sont impairs. Connaissant un nombre pair par exemple 1244488, il suffit d'ajouter 2 pour trouver le nombre pair suivant 124500. Nous allons voir que ce n'est pas le cas des nombres premiers. Il y en a une infinité. Leur répartition semble obéir à certaines règles. Elles ont été confirmées par la puissance des ordinateurs modernes qui permet de générer une suite très longue des premiers nombres premiers. Mais on n'a jamais pu trouver une formule qui partant d'un nombre premier permet de trouver le suivant.
Gauss a émis une hypothèse concernant la densité des nombres premiers. Ceux-ci se raréfient au fur et à mesure que l'on progresse vers de plus grands nombres. Il a même proposé une formule permettant d'approximer la probabilité qu'un nombre soit premier mais elle n'a toujours pas été démontrée. Nous l'étudierons dans la partie dédiée à la répartition des nombres premiers.

Pour couronner le tout, il est extrêmement long et coûteux, voire impossible, de prouver qu'un très grand nombre (un nombre de plus de 300 chiffres par exemple) est premier. S'il n'est pas premier alors il a des diviseurs. Mais il est encore plus difficile de trouver les diviseurs. C'est sur la difficulté de trouver les diviseurs, la "factorisation en facteurs premiers", vue dans le préambule racontant la conférence muette de Nelson Cole , qu'est basée tout le mécanisme de la sécurité des échanges sur internet. Si demain, un mathématicien trouve une formule ou un algorithme qui permet de trouver facilement les facteurs d'un très grand nombre, alors c'est tout l'internet qui s'écroulera, plus aucune communication ne sera confidentielle. Des pirates du net pourront enregistrer et contrefaire les communications entre vous et votre banque.

Pendant longtemps la factorisation n'a pas intéressé les mathématiciens qui ne pouvaient espérer financer leurs travaux dans un domaine jugé inutile voire ludique. Gauss au $18^{ème}$ siècle s'y est intéressé avant que la factorisation ne tombe dans les oubliettes de la recherche. Cela a changé quand deux mathématiciens Whitfield Diffie et Martin Hellman ont présenté en 1976 à la "National Computer Conference" le concept de cryptographie à clé publique et que trois autres génies des mathématiques et de l'informatique ont développé un exemple de système de chiffrement utilisant les nombres premiers et la factorisation. C'est le codage RSA, nommé

ainsi car ses inventeurs s'appellent Rivest, Shamir et Adleman. Il est aujourd'hui utilisé pour toutes les communications sur internet et est basé sur l'impossibilité de factoriser un nombre de 300 chiffres dans un temps raisonnable avec les ordinateurs actuels.

La quatrième partie présentera les tests de primalité et les méthodes de factorisation. Cela permettra d'introduire quelques nombres premiers "intéressants" et des conjectures (théorèmes dont on ne sait toujours pas s'ils sont vrais ou faux). Ce sont les sommets non encore gravis du paysage des nombres premiers.

La cinquième partie présentera en détail l'algorithme de cryptologie RSA. En 2008, un mathématicien ou un groupe de mathématiciens a publié un article sous le pseudonyme de Satoshi Nakamoto. Cette publication scientifique présente un mécanisme de monnaie échappant à tout contrôle centralisé : le bitcoin. Les transactions dans cette monnaie sont validées par un mécanisme appelé "block chain' , basé sur la difficulté de factoriser les grands nombres premiers. La première plateforme d'échange de cette monnaie a été créée en 2008. Un bitcoin valait 0,003$ aujourd'hui il vaut plus de 50000$. Les nombres premiers ont pu générer des investissements très rémunérateurs, voire abusifs, pour ceux qui, travaillant dans ce domaine, ont découvert très tôt le potentiel des crypto-monnaies !

La sixième partie présentera des démonstrations. Des plus simples comme celles prouvant l'infinité des nombres premiers découverte par Euclide aux plus compliquées comme le postulat de Bertrand. Vous pourrez choisir de les étudier en profondeur au point de les reproduire sans modèle, de proposer des variations, ou simplement les survoler comme on admire un raisonnement brillant ou un tableau magnifique sans vraiment chercher à comprendre chaque détail.

Une annexe présentera des détails sur des domaines connexes. Leurs insertions dans le cœur de l'ouvrage auraient constitué trop de digressions. Mais il aurait été dommage de les omettre.

Arithmétique : Notions de base, notations et syntaxe

Ce livre concerne les nombres premiers. Nous allons donc étudier leur définition, leurs propriétés et leurs applications.
Mais ces nombres sont avant tout une bonne opportunité de découvrir le monde des mathématiques avec ses conventions, ses méthodes et son esthétisme. Esthétisme ? Oui c'est l'ambition de ce livre de vous faire découvrir la beauté et les émotions que peuvent générer un théorème ou une démonstration. Un raisonnement mathématique comme un texte littéraire est pourvu d'un style, une forme qui associée au fond rend la lecture d'un ouvrage passionnant.

Pour certains, leur intérêt pour les mathématiques ne s'arrête pas à l'étude d'ouvrages accumulant des connaissances acquises par l'homme pendant des milliers d'années, ils perçoivent dans ce domaine une transcendance qui va au-delà de leur propre existence et donne un sens à l'univers. Ce n'est pas nouveau, Pythagore vers 580 avant J.-C. liait la philosophie des nombres à l'harmonie céleste. Platon (-428 - 347) décrit dans l'allégorie de la caverne que le monde réel dans

lequel nous vivons n'est qu'une image projetée sur le fond d'une caverne du monde des idées. Alain Connes, médaille Fields, et titulaire de la chaire d'Analyse et Géométrie au Collège de France défend la thèse que les mathématiques sont les constituants d'une réalité plus stable que la réalité matérielle qui nous entoure alors que Jean-Pierre Changeux, neurobiologiste et membre de l'académie des sciences les décrit comme le simple produit de l'activité humaine. Ils débattent de ces deux visions des mathématiques dans un livre passionnant "Matière à pensée" [5].
Ce livre vous amènera t'il à vous poser ce type de questions ? J'en serais flatté.

Revenons à nos mouton**S !**

Les mathématiques sont utilisées dans la vie de tous les jours pour résoudre des problèmes et sont à la base de toutes les sciences appliquées comme la physique, la chimie ou la biologie.
Mais les mathématiques, que des mathématiciens Français regroupés sous le pseudonyme de Bourbaki ont unifié dans "*la Mathématique"*, est aussi une science qui est étudiée et développée en dehors de toute application. Les mathématiciens travaillent parfois à partir d'un problème posé par les physiciens : comment résoudre une équation particulière qui permet de prévoir le trajet d'une particule ? comment prévoir le temps du lendemain

à l'aide de modèles mathématiques complexes ? Mais ils travaillent souvent aussi sans objectif pratique, dans le but unique de mieux comprendre les structures et les mécanismes d'un monde abstrait : le monde des objets virtuels des mathématiques. Ils errent dans des paysages inconnus dans le but de découvrir de nouveaux sommets à gravir.

Ce qui est étonnant est que de nombreux domaines des mathématiques, développés sans but précis, ont produit des outils indispensables dans des théories physiques découvertes des années ou des siècles plus tard. Comme par exemple les géométries non euclidiennes, qui ont été introduites par Lobatchevski en 1829. Elles ont été étudiées en détail par Riemann, Klein ou Poincaré comme des bizarreries sans relation avec le monde réel. Pourtant deux siècles plus tard, Albert Einstein, dans sa théorie de la relativité générale, montrait que la géométrie de notre univers est non euclidienne.

Il en est de même pour les nombres premiers. Ils ont longtemps été considérés comme des objets exotiques, voire des manifestations divines pour les pythagoriciens. Leurs propriétés, démontrées aux cours des deux derniers millénaires, ont permis de développer les mécanismes de la cryptologie à la base des communications sur internet ou des crypto-monnaies.

Les mathématiques ou la mathématique ont leur langage qui permet à deux mathématiciens de langues et de cultures différentes de se comprendre et de travailler ensemble à la résolution d'un même problème.

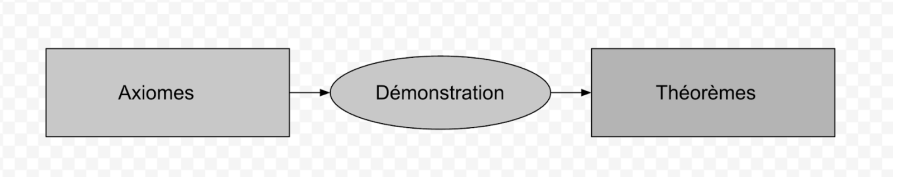
De même qu'un voyage à Milan est une bonne opportunité d'apprendre l'italien, ce voyage dans l'univers des nombres premiers va nous permettre de découvrir et de manipuler une partie de ce langage.

Les nombres premiers vont nous faire découvrir certains concepts mathématiques :

- Les ensembles. Tout débute avec eux. Un ensemble est une collection d'éléments distincts. Par exemple un troupeau de moutons ou bien une collection de nombres.
- Les nombres. En particulier les nombres entiers naturels. Ce sont ceux qui nous permettent de compter des entités comme les moutons dans un troupeau (1, 2, 3,...), ou leur absence avec le nombre zéro, noté 0. On verra que ces deux premiers concepts sont intimement liés. En effet Giuseppe Peano (1858-1932), mathématicien et linguiste italien, développa une axiomatique de l'arithmétique dans laquelle les nombres sont définis comme la cardinalité d'un ensemble. La cardinalité d'un ensemble est le nombre d'éléments d'un ensemble.

- Les relations et les fonctions qui permettent de relier des éléments en particulier les nombres entre eux.
- Les opérations : celles que nous apprenons à l'école primaire : l'addition, la soustraction, la multiplication et la division.
- Des structures simples comme les ensembles qui munies de certaines opérations peuvent acquérir des propriétés de structures plus complexes que l'on appelle groupes, anneaux ou corps. Les mathématiques ne sont pas avares de réutilisations de termes simples comme anneaux ou noyaux pour nommer une structure complexe. Reconnaissons aux mathématiciens la bonne idée de ne pas avoir été puiser dans le latin ou le grec ancien les noms des structures qu'ils découvraient. Les botanistes pourraient en prendre de la graine !

Ces objets ne sont que la partie émergée de l'iceberg des mathématiques. Les fondations sont les raisonnements logiques. Les bases de la démonstration qui permettent à partir des vérités admises par principe, appelées *axiomes,* de découvrir des énoncés vrais appelés *théorèmes*.



Nous allons ainsi apprendre dans ce chapître le vocabulaire et la grammaire de ce langage. Cela nous permettra de nommer les paysages que le raisonnement logique nous fera parcourir.

L'étude des nombres premiers fait partie de la branche des mathématiques que l'on nomme *Arithmétique*. L'arithmétique est liée à l'algèbre dont le but est de résoudre des équations et d'étudier les propriétés des opérations. Le mot « algèbre » est dérivé du titre d'un ouvrage rédigé vers 825 par le mathématicien d'origine *persane Al-Khwarizmi* :
,*Kitāb al-mukhtaṣar fī ḥisāb al-jabr wa-l-muqābala* (« *Abrégé du calcul par la restauration et la comparaison* »).

Euclide a étudié l'arithmétique au 3ème siècle avant JC. Son peuvre "Les éléments" n'utilise pas de langage mathématique avec des notations spécifiques mais est rédigé en grec ancien. Il contient des phrases du genre :

"*Si l'on a 3 grandeurs et d'autres grandeurs égales en nombres qui, prises deux par deux, sont dans le même rapport, mais que la proportion soit déréglée, di isou aussi elles seront dans le même rapport (Euclides 1970,33)"*

Ce qui en langage mathématique moderne s'exprime par $\forall a, b, c, d \in N,\ \frac{a}{b} = \frac{e}{f}\ et\ \frac{b}{c} = \frac{d}{e}\ \Rightarrow \frac{a}{c} = \frac{d}{f}$

Par exemple $\frac{3}{4} = \frac{9}{12}\ et\ \frac{4}{2} = \frac{18}{9} \Rightarrow \frac{3}{2} = \frac{18}{12}$

Le second énoncé peut paraître plus complexe mais il est sans ambiguïté et est compréhensible par tout mathématicien de tout pays. A la fin de ce chapître vous le comprendrez. Alors que la lecture des éléments d'Euclide dans le texte demande de comprendre le grec classique et une réflexion intense pour comprendre la signification de phrases alambiquées.

Sans recourir aux symboles, Euclide aurait pu écrire :
"Si 2 fractions sont égales, les produits du dénominateur de l'un par le numérateur de l'autre sont égaux".
En effet un raisonnement logique permet de passer de cet énoncé à la propriété précédente. Mais à l'époque le nombre, conçu comme une entité abstraite indépendante de ce qu'il comptait ou mesurait, n'existait pas. On ne pouvait donc donner un nom, numérateur ou dénominateur, à un concept inconnu. Pour Euclide les nombres sont des grandeurs géométriques. C'est-à-dire des longueurs de segments dont la base est l'unité. Ce qui rend ses énoncés complexes car les fractions ne sont pas des nombres mais des rapports de longueurs. Ceci explique aussi sa difficulté à accepter les nombres négatifs. En effet, il n'y a pas de segments de droite de longueur négative.

Jusqu'au XVI^{e} siècle, le raisonnement est exprimé par des phrases dans le style de celui d'Euclide, écrites en Français, en Allemand, ou souvent en latin. On se heurte rapidement à des ambiguïtés dûes à la nature de ces langages que les linguistes appellent langages naturels. C'est-à-dire les langues que les humains parlent, écrivent tous les jours, par opposition aux langages formels dont la syntaxe et le sens (on parle de sémantique) excluent toute ambiguïté dans leurs interprétations.

L'algèbre et donc l'arithmétique firent un bond prodigieux grâce aux mathématiciens français Francois Viète (1540-1603) et Albert Girard (1595-1632) qui ont promu le calcul littéral. Ils ont eu l'idée d'utiliser des lettres pour représenter les nombres et des symboles pour les opérations et les raisonnements. Cela parait évident mais comme bien des progrès en mathématiques, il a fallu des siècles pour que ces idées germent et se propagent.

Nous allons donc présenter dans les pages qui suivent les notations littérales et les objets mathématiques utilisés dans le cadre de l'étude des nombres premiers.

Les ensembles

Ce sont les fondations des mathématiques dites modernes. En partant du concept d'ensemble, on peut

découvrir toutes les autres structures du monde mathématique : les nombres, les fonctions, les formes géométriques….
Ils sont simples à comprendre. Un ensemble est une collection d'objets différents : les voitures sur un parking, les nombres de 1 à 10….
On peut les décrire par *extension* en citant tous leurs membres ou par *compréhension* en citant les propriétés requises pour faire partie du club. La notation en extension est simple. Les éléments sont énumérés dans n'importe quel ordre entre deux accolades. Par exemple : Ensemble P = {0,1,2,3,4,5,6,7,8,9}.
La définition en compréhension, en langage naturel serait P est l'ensemble des nombres entiers positifs compris entre 0 et 9, ou bien P est l'ensemble des nombres entiers composés d'un seul chiffre.
La description est longue, les mathématiciens comme les gendarmes tapent parfois sur leurs claviers avec deux doigts. Ils n'aiment pas les longues phrases. Et comme on l'a vu précédemment , le langage naturel peut être imprécis.
Qu'entend-on par "compris entre 0 et 9" ? Est-ce que 0 et 9 en font partie ?

C'est pourquoi, la définition en compréhension utilise une syntaxe particulière pour définir les propriétés qui définissent un ensemble. Un peu comme une sténo universelle. Un espéranto des mathématiciens qui leur

épargne les longues phrases, les imprécisions et l'apprentissage des langues étrangères.

Ces propriétés d'un ensemble sont décrites à l'aide de symboles. Ces symboles sont souvent des lettres grecs, ça fait plus chic. Mais cela ne doit pas vous effrayer !

1. $\in$ $(Epsilon)$: Cela veut dire "appartient". Par convention, on note N ou ℵ, l'ensemble des entiers positifs. $3 \in N$ indique que le nombre 3 appartient à l'ensemble N. On peut aussi dire que l'ensemble N inclut l'élément 3. Le symbole $\in$ a été introduit par Giuseppe Peano en 1889 dans "*Arithmetices principia".* A l'origine $3 \in N$ se lisait 3 est un N. Ce qui est resté dans l'expression 3 est un entier naturel. Mais $un\ mouton \in troupeau$, ne veut pas dire qu'un mouton est un troupeau !
2. $\subset$: veut dire "est inclus" . $A \subset B$ veut dire que l'ensemble A est inclus dans l'ensemble B. A est une partie de B. On en déduit que si $3 \in A$ alors $3 \in B$ car $A \subset B$. On devine ici la base d'un raisonnement logique basé sur la théorie des ensembles.
3. $\forall$: veut dire "pour tout" ou "quel que soit". Par exemple $\forall a \in N$ veut dire que la propriété qui va suivre est vraie pour tout élément a de N. Par exemple si on définit P en extension comme précédemment :

P = {0,1,2,3,4,5,6,7,8,9}. On peut écrire la propriété $\forall a \in P$, a est inférieur à 10. On aurait pu se passer de ce signe, mais les mathématiciens anglais auraient écrit “for all” et les français “pour tout". Pas pratique !

4. ∃: veut dire “il existe”. Ce symbole est souvent suivi dans la même phase du symbole “/” qui veut dire “tel que”. Par exemple : “ $\exists\, a \in P \,/\, a\ est\ inférieur$ à 5 " se lit « il existe un nombre a de l'ensemble P tel que a est inférieur à 5 ».

5. ∃! : qui se lit « il existe de manière unique ». "∃! $a \in B$ ” veut dire que dans l’ensemble B il existe un élément et un seul que l’on appelle a.

∃! $a \in P \,/\, a\ est\ strictement\ supérieur$ à 8 est une propriété vraie car le nombre 9 appartient à P et il est le seul à être strictement supérieur à 8.

On appelle cardinal de A le nombre d’éléments d’un ensemble A. On utilise la notation suivante : card(A).

Nous sommes maintenant en mesure de définir un ensemble par compréhension. Par exemple l’ensemble défini en compréhension par :

Q = { $a \in P / \ a\ est\ inférieur$ à 5}.

se défini en extension par : Q = {0,1,2,3,4}

On remarque que card(Q) = 5. Quel que soit le type de définition. SI ce n’est pas le cas, il y a erreur dans la propriété utilisée pour caractériser l’ensemble en compréhension. Erreur de “compréhension” !

Vous avez remarqué que nous avons utilisé plusieurs fois l'expression "est inférieur à". Nous verrons plus loin que cela s'appelle une relation. Et comme les matheux l'utilisent souvent, fidèles à leur goût pour la facilité et les symboles difficiles à trouver sur le clavier, ils ont utilisé un symbole pour cela : "<". Nous en verrons d'autres quand nous parlerons des relations. Tous ces symboles étaient bien pratiques quand les mathématiciens écrivaient leurs démonstrations à la main. Ils sont devenus un cauchemar pour les utilisateurs de clavier. En effet comment écrire $\in$ sur un clavier. Nous verrons en annexe comment les claviers et les polices de caractères ont évolué d'abord pour satisfaire les mathématiciens avides de symboles grecs et maintenant pour satisfaire les utilisateurs de whatsapp friands d'émoticônes !
Nous allons aussi souvent être confronté à un type d'ensemble particulier que l'on appelle intervalle : l'intervalle des nombres compris entre 2 et 6 inclus se note [2,6]. C'est l'ensemble {2,3,4,5,6}.

Entraînez vous sur quelques exemples en essayant d'écrire en compréhension à l'aide des symboles que nous venons d'introduire les ensembles suivants :

1. P = {2, 4, 6, 8, 10, 12}
2. P = {3, 6, 9, 12, 15}

3. P = {0}

Solutions :
Bien sûr, il y a plusieurs manières pour chaque ensemble de définir les propriétés qui le caractérise.
1. $P = \{a \in N / \, a \, est \, pair \, et \, 0 < a < 13\}$. D'ailleurs la propriété "a est pair" peut s'écrire aussi sous forme symbolique :
$\exists k \in N \, / \, a = 2 \times k$
En effet un nombre est pair s'il est le double d'un autre nombre et vice-versa.

2. $P = \{a \in N / \, a \, est \, multiple \, de \, 3 \; et \, 0 < a < 16\}$.
Bien sûr, vous avez deviné que l'on peut écrire "a est multiple de 3" sous la forme :
$\exists k \in N / a = 3 \times k$

3. $P = \{a \in N / \, a < 1\}$ car 0 est le seul nombre de N strictement inférieur à 1. On peut aussi utiliser la propriété unique du nombre 0, qui laisse un nombre inchangé après l'addition.
$P = \{a \in N / \, \forall k \in N, \, a + k = a\}$

Il est temps de parler d'un ensemble particulier : l'ensemble vide. On le note $\Phi \, ou \, \{\}$. Il est nécessaire pour introduire un nombre original, le nombre zéro : 0. C'est le cardinal de l'ensemble vide. $card(\Phi) = 0$.

Bien sur ce nombre était aussi un problème pour Euclide car on ne peux le définir comme un longueur. Ce sont les Babyloniens, un peu plus de deux cents ans avant J.C-., qui l'on introduit dans l'écriture positionnelle (le zéro de 306 indique qu'il y a 0 dizaine à ajouter aux 3 centaines) mais jamais seul ou à gauche, ni à droite d'un nombre. Les indiens ont formalisés son utilisation dans les opérations et dans l'introduction de la notation décimale. Il a ensuite été empruntés par les mathématiciens arabes qui l'ont transmis à l'Europe.

Les nombres

Pourquoi parler des nombres, après avoir introduit les ensembles ?

Car comme on l'a vu précédemment, on définit formellement un nombre entier naturel comme étant le cardinal d'un ensemble. Cette définition a été formalisée dans dans l'axiomatique de Peano (1858-1932), celle que l'arithmétique utilise de nos jours. Un nombre entier naturel, c'est-à-dire positif, est le cardinal d'un ensemble : le nombre d'éléments d'un ensemble. Les nombres sont définis par les ensembles et nous allons nous intéresser dans ce livre à un ensemble de nombres : les nombres premiers. C'est le pouvoir auto-générant du langage mathématique. Un concept amène toujours un nouveau

concept. Après avoir franchi un col, gravi un sommet, on découvre une nouvelle vallée bordée de sommets, séparés par des cols.

Dans l'ensemble des entiers naturels, nous allons nous intéresser à un sous-ensemble. C'est ainsi que l'on nomme une partie d'un ensemble. Le sous-ensemble des nombres premiers.
On a vu que les entiers naturels sont définis comme étant les cardinaux d'ensembles. Ce sont donc des nombres qui permettent de compter les éléments des ensembles. Les hommes les ont introduits pour compter des choses comme le nombre de sommets dans les Alpes ou les moutons d'un troupeau.
De nos jours, on utilise la base 10 pour les représenter à l'aide de symboles que l'on appelle "*chiffre"* : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.
La base 10 c'est facile, dès que l'on dépasse 9 éléments on ajoute un chiffre sur la gauche : 10, 11,.. De même pour 99 : 100,101,...et ainsi de suite. On appelle ce système de représentation des nombres, le *système positionnel*.
Cette notation semble évidente tant elle est maintenant répandue dans le monde entier mais il y eut d'autres systèmes comme le système quinaire des romains en base 5 (I,II,..., V,VI,...X,XI,..) ou le système sexagésimal (en base 60) des babyloniens (3200 avant J.-C) qui

perdure dans notre mesure du temps (1 heure = 60 minutes, 1 minute = 60 secondes).
Les opérations élémentaires comme l'addition et la multiplication sont difficiles dans le système romain. L'adoption de la base 10 (sans doute adoptée car nous avons 10 doigts et qu'il est tentant de compter sur ses doigts même si la maîtresse ne veut pas !) a facilité les calculs comme l'addition et la multiplication. Il suffit de mettre les nombres les uns en dessous des autres et de ne pas oublier les retenues.

$$\begin{array}{r} {}^{1}\\ 3\,3\,8\,2 \\ +\ 4\,5\,5\,3 \\ \hline 7\,9\,3\,5 \end{array}$$

Le système sexagésimal a perduré car 60 est loin d'être premier. Il est divisible par 2, 3, 4, 5, 6, 10, 12, 15, 20, 30. On peut ainsi utiliser un nombre entier pour représenter un quart d'heure, une demi-heure,... Si une heure comptait 10 minutes, il faudrait un nombre à virgule pour minimiser notre retard d'un quart d'heure en l'exprimant en minutes. Alors qu'avec la base 60, un quart d'heure vaut un nombre entier de minutes : "Un quart d'heure de retard, tu exagères, 15 mn au plus !".

Les ordinateurs fonctionnent à base de transistors. Ces derniers peuvent prendre 2 états, ouvert le courant passe, fermé il ne passe pas. Pour représenter l'état

interne des constituants d'un ordinateur et pour les programmer, les informaticiens ont donc utilisé la base 2 (0,1, 10, 11,100,...). Chaque chiffre 1 ou 0 est appelé un bit. On appelle registre un ensemble de bits. Les ordinateurs actuels utilisent des registres de 32 ou 64 bits. Autrefois ils étaient limités à 4 ou 8 bits. Pour représenter leur contenu, les programmeurs utilisent parfois la base 16, appelée notation hexadécimale utilisant 16 symboles de 0 à F : 0 1 2 3 4 5 6 7 8 9 A B C D E F 10 11… 1F 20 21… Il faut être Geek pour se sentir à l'aise en base 16 ! Pourtant avant l'invention des langages de programmation, les premiers calculateurs électroniques étaient programmés de cette façon. Les algorithmes, définissant les suites d'opérations à effectuer par l'ordinateur, étaient constitués de milliers de nombres hexadécimaux. Chaque nombre avait une signification particulière, interprétée par les transistors de l'ordinateur.

Quelques exemples :

- 15 en base sexagésimale va s'écrire 65 en base dix. En effet 15 est 1h (60 minutes) plus 5 minutes.
- 100 en base 2 va s'écrire 4 en base dix. Car il vient après 0,1,10,11 comme 4 vient après 0,1,2,3 en base 10.

Les propriétés des nombres sont indépendantes de la base utilisée. Un nombre premier en base 2 est aussi

premier en base 10 ou 60. Il n'a pas de diviseur quelle que soit la manière dont on l'écrit. Dans le reste de ce livre, on utilisera bien sur la base 10.

De manière littérale, quand on veut parler d'un nombre quelconque, on utilise des lettres de l'alphabet romain ou grec, souvent en minuscule : a, b, c, α, δ, … On réserve les majuscules aux ensembles :

- N : L'ensemble des entiers naturels
- P: L'ensemble des nombres premiers.
- ….

Quand on veut représenter un nombre inconnu dont on cherche la valeur, on utilise souvent les lettres x, y ou z. C'est le cas bien connu des équations : trouvez la valeur de x tel que x + 6 = 12 ?
Pourquoi utilise t'on x pour représenter l'inconnue d'une équation. Diophante d'Alexandrie, vivant autour du IIe siècle, est le premier à introduire un nombre indéterminé, qu'il nomme «arithmos», ce qui signifie simplement «nombre». Les musulmans qui jouèrent un rôle important en théorie des nombres jusqu'au XVème siècle utilisaient 'shay' qui veut dire "quelque chose". Les Andalous, sous occupation arabe, établirent une correspondance entre l'alphabet latin et arabe et utilisèrent "xay". Au XVIIe siècle René Descartes, fidèle à la recherche de la concision des mathématiciens remplaça xay par x. Le scénario du film x, deux millénaires en un paragraphe !

Rapidement les mathématiciens se sont heurtés au problème de la représentation de valeurs négatives pour mesurer des quantités en moins ou à venir : comme une dette. Les nombres négatifs étaient aussi nécessaires à la résolution de certaines équations comme : $x + 3 = 0$

Euclide pour qui tout était géométrique et les nombres des longueurs de segments ne reconnaissait pas les nombres négatifs comme des “vrais” nombres. Ils étaient pour lui des symboles intermédiaires, utiles pour résoudre certains problèmes mais n’avaient pas le même statut que les nombres positifs. La ségrégation au pays des nombres ! Aujourd’hui, ce sont des nombres de plein droit et on note les nombres négatifs en base 10 comme les nombres positifs en ajoutant un signe “-” sur leur gauche : -1 -2 -3

L'ensemble des nombres positifs et négatifs est appelé “*ensemble des nombres entiers relatifs”* ou simplement “*nombres entiers”* et est noté Z. Il interviendra souvent dans cet ouvrage. On peut noter que N, l’ensemble des entiers naturels, est une partie de Z, l’ensemble des entiers relatifs. On peut écrire $N \subset Z$.

Rapidement les mathématiciens grecs de l’antiquité se sont heurtés au rapport entre les valeurs entières quand ils voulaient comparer une longueur d’un segment avec

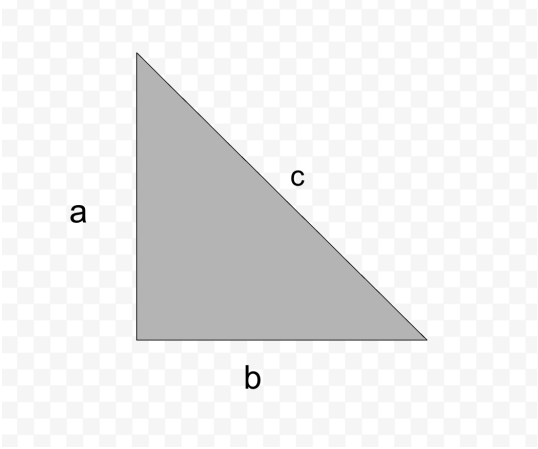
une autre. Ils ont introduit les nombres rationnels $\frac{p}{q}$ que l'on appelle à l'école primaire les fractions. De même que pour les nombres négatifs qui étaient nécessaires à la résolution de certaines équations, les nombres rationnels sont aussi les seules solutions d'équation du type : $6 \times x = 11$. Il n' y a pas de nombre entier qui soit la solution de cette équation. Il a fallu introduire le nombre rationnel $\frac{11}{6}$.

Ces nombres sont une extension des *nombres décimaux* appelés aussi "nombre à virgule". Les nombres décimaux sont des nombres avec un nombre fini de chiffres après la virgule (0 pour les nombres entiers car 2,0 = 2). Les nombres rationnels sont plus complexes et peuvent avoir un développement décimal infini.

Ah oui, désolé, c'est quoi le développement décimal ? Vous avez deviné peut être ? Ce sont les chiffres à droite de la virgule. Par exemple $\frac{10}{3}$= 3,33333….. est rationnel. Il contient un nombre infini de chiffres 3 à droite de la virgule. Alors que $\frac{10}{4}$= 2,5 est décimal.

On note D l'ensemble des nombres décimaux et Q l'ensemble des nombres rationnels (Q pour quotient sans doute). N est une partie de Z qui est une partie de D qui est une partie de Q. Ce qui s'écrit $N \subset Z \subset D \subset Q$.

Les nombres ne s'arrêtent pas là. Euclide pour qui tout nombre représentait une longueur ou un rapport de longueur a vite rencontré un problème avec le triangle suivant :



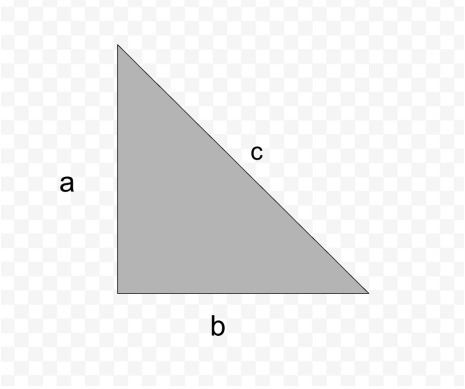
Rappelons quelques notions, évidentes pour certains, mais qui nécessitent, peut-être, pour d'autres une piqûre de rappel :

On appelle **"**carré**"** d'un nombre a, le nombre élevé à la puissance 2. C'est à dire le nombre a mutiplié par lui même : $a \times a$. On le note a^2. Le 2 est appelé l'exposant de a.

La réciproque du "carré" est la "racine carrée". On appelle racine carrée de a le nombre qui multiplié par lui même donne a. On note la racine carrée : $\sqrt{a}$ $\sqrt{a} \times \sqrt{a} = a$

Par exemple le carré de 3 est 3×3 . On peut le noter 3^2. Si vous vous souvenez de vos tables de multiplication, vous avez tout de suite vu que $3^2 = 3 \times 3 = 9$.
De même, la racine carrée de 9 est le nombre qui multiplié par lui-même donne 9. C'est donc 3. On note $\sqrt{9} = 3$.

Plusieurs siècle auparavant, Pythagore (580-495 avant J.C-.) et ses disciples; pour qui tout était nombre, furent effrayés par l'incommensurabilité de la diagonale d'un carré dont la longueur du coté valait 1 cm. En effet, le théorème de pythagore postule que la somme des carrés d'un triangle rectangle donne la valeur de son hypoténuse.



Dans le triangle de gauche, la longueur de l'hypoténuse vaut c cm, celle du côté inférieur b cm, et du côté de gauche a cm. L'angle entre a et b vaut 90°. Le triangle est donc un triangle rectangle.
On peut donc écrire

$$c^2 = a^2 + b^2$$

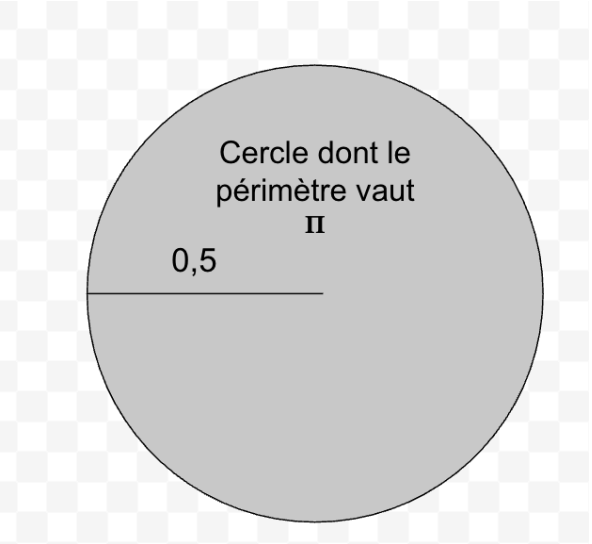
Considérons ce nouveau triangle de gauche dont les côtés valent 1 cm et l'hypoténuse d cm. On peut écrire $d^2 = 1^2 + 1^2 = 2$. Donc $d = \sqrt{2}$

Pythagore et ses disciples démontrèrent que $\sqrt{2}$, le nombre qui multiplié par lui-même donne 2, donc la longueur de la diagonale ne pouvait pas s'écrire sous la forme du rapport de 2 nombres entiers. Il n'existe pas de nombres entiers p et q tel que $\frac{p}{q} = \sqrt{2}$. La démonstration basée sur le principe de démonstration par l'absurde est assez élégante et se trouve facilement sur internet.
Cette simple énoncé "il n'existe pas de nombres entiers p et q tel que $\frac{p}{q} = \sqrt{2}$", bousculait la théorie philosophique, véritable religion, de la secte des pythagoriciens. Pour eux le monde était fait de nombres entiers ou de fractions de nombres entiers. Les nombres entiers ou leurs fractions pouvaient servir à mesurer n'importe quelle longueur. La simple diagonale du triangle rectangle, dont les mesures des 2 côtés sont égales à 1 cm, est donc "incommensurable". Pourtant elle était là devant leurs yeux et ils pouvaient facilement fabriquer un tel triangle. Une des bases de leurs croyances s'écroulaient. Leur réaction première tient plus du comportement d'un extrémiste religieux que d'un mathématicien, ils décidèrent de ne pas divulguer cette découverte contraire à leurs croyances fondamentales !

Quand les faits contredisent la théorie, changeons les faits. Les vérités alternatives ou “fake news” ne sont pas nées avec les réseaux sociaux !

La légende raconte que celui qui a divulgué cette information, Hippase de Métaponte, aurait, en représailles, été noyé en mer par les condisciples de Pythagore !

De même que des équations ont introduits les nombres négatifs et les nombres rationnels, ces mêmes équations du type : $x^2 - 2 = 0$, ne pouvaient trouver de solutions dans les nombres rationnels. Ils ont nécessité l’introduction de nouveaux nombres. Les racines de certains nombres entiers ne sont pas les seuls nombres qui ne peuvent s’exprimer sous forme de fractions. Il y a aussi des nombres appelés *transcendants* comme Π qui mesure le périmètre d'un cercle dont le rayon vaut $\frac{1}{2}$. Tous ces nombres sont appelés nombres réels car ils mesurent des quantités réelles dans notre univers.

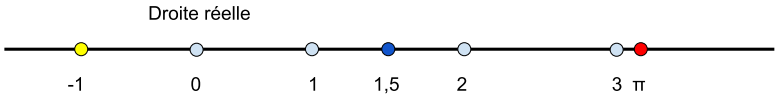


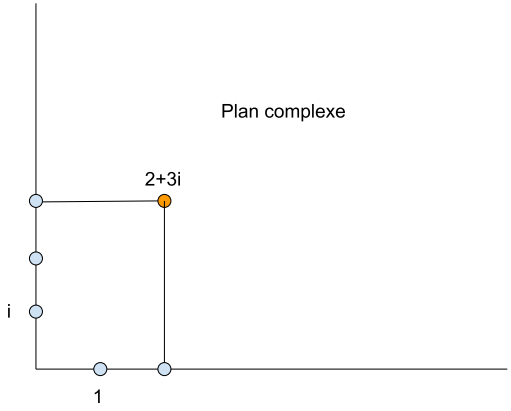
Bien sûr ces nombres réels bien que fort puissants pour les calculs ne suffirent pas aux mathématiciens toujours avides de découvrir de nouveaux territoires.

La résolution de l'équation $x^2 = 2$ a introduit les nombres réels car les nombres rationnels quotients de deux entiers n'offraient pas de solutions. Mais il y a d'autres équations qui n'ont pas de solution dans l'ensemble des nombres réels. Le carré d'un nombre est toujours positif car si ce nombre est négatif, en le multipliant par lui-même, le produit sera positif. Rappelez vous ce que l'on apprend au collège : "- par -" donne + et "+ par +" donne +.

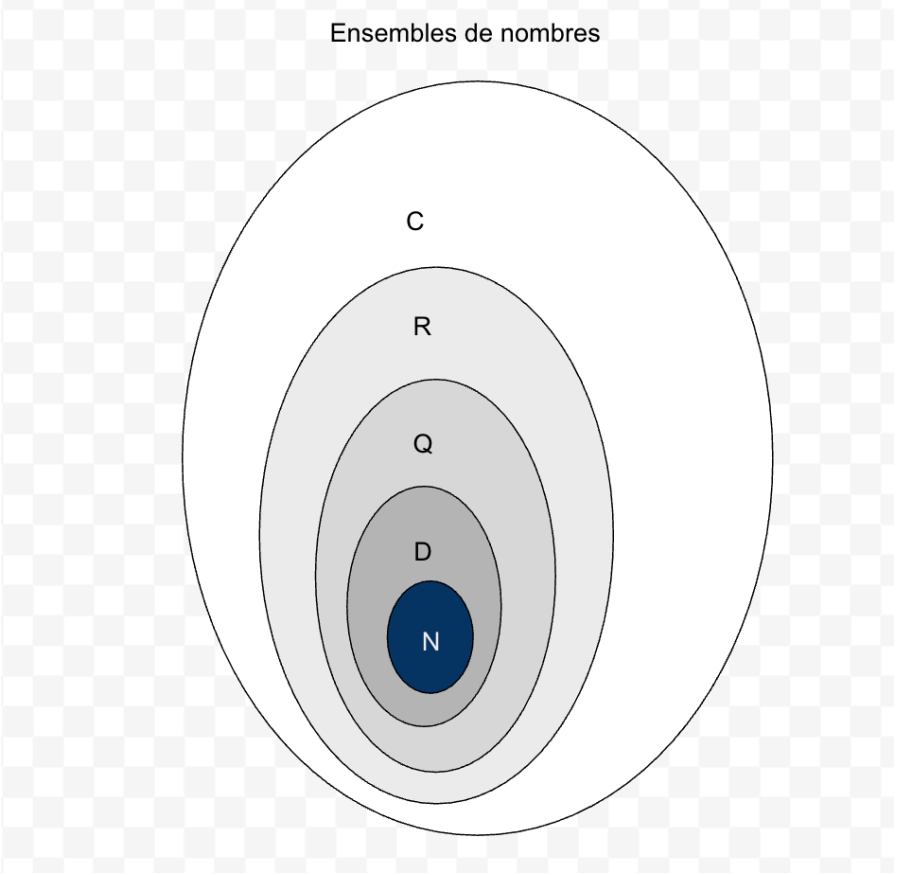
Alors comment résoudre l'équation $x^2 = -1$. On aurait pu ignorer cette équation et dire qu'elle n'a pas de solutions mais rapidement les mathématiciens ont été confrontés à des problèmes nécessitant des solutions à ce type de problème. Il a fallu alors s'aventurer dans le continent des nombres complexes en introduisant un nombre spécial que l'on note ***i*** qui par définition est la racine carrée de -1.
Les nombres complexes sont les nombres de la forme $a + bi$ ou a et b sont des nombres réels. Ainsi 1+2i est un nombre complexe..

Une représentation géométrique des nombres permet de représenter les nombres réels comme tous les points d'une droite alors que les nombres complexes sont les points du plan.





Assez sur les ensembles de nombres, leur histoire nécessiterait un livre entier. Il y a d'autres nombres encore plus étranges : les nombres ordinaux ou les quaternions mais il n'interviennent pas dans l'étude des nombres premiers. D'ailleurs jusqu'ici, ils ne servent pas beaucoup ! Dans les pages suivantes, nous allons nous concentrer sur le plus "petit" ensemble de nombres: N l'ensemble des entiers naturels.



Relation- Fonction

Les éléments d'un ensemble peuvent être reliés deux à deux par des ***relations***.

Par exemple, la relation “est le double de”. 6 “est le double de” 3. On dit que 6 est relié à 3 par la relation “est le double de”. On peut le noter sous la forme 6 D 3.

Une relation est donc une propriété qui relie deux éléments. Appelons ces deux éléments x et y. On note la relation entre eux sous la forme : $x\ R\ y$.

Certaines relations sont souvent utilisées alors on utilise des symboles spéciaux pour les noter, un peu comme la sténographie !

Quelques exemples de relations dont nous allons avoir besoin :
> : veut dire “est strictement supérieur à” : 4 > 3
< : veut dire “est strictement inférieur à” : 3 < 4
≤: veut dire “est inférieur ou égal”. $4 \leq (2 \times 2)$
≥: veut dire “est supérieur ou égal”. $6 \leq (2 \times 3)$
= : veut dire “est égal”. $6 = (2 \times 3)$

Une ***fonction*** est un cas spécial de relation dans laquelle chaque élément de l’ensemble est en relation avec au plus un élément : 0 ou un unique élément. On note les fonctions différemment par exemple “est le double” est une fonction car un nombre entier naturel est le double de au plus un nombre : pas de nombre si il est impair, un nombre, sa moitié, si il est pair.. On aurait pu écrire 6 D 3 mais pour bien montrer que c’est une fonction et qu’il y

a une “direction” dans la relation on utilise la notation fonctionnelle : d(6) = 3. On dit que 3 est l’image de 6 par la fonction d : d(6) = 3. 3 est le sujet de la fonction. Vous avez remarqué que l’on utilise de préférence les minuscules pour noter les fonctions. C’est simplement une convention de style de plus dans l’écriture du langage mathématique.

Notons que pour certains entiers naturels la fonction d n’est pas définie. En effet d(7) n’est pas un entier. Car 7 est le double de 3,5 qui n’est pas un entier naturel.

Ce qui précède est une version simplifiée des relations et des fonctions. En effet une relation peut relier un sujet dans un ensemble et une image dans un autre. Les fonctions peuvent avoir plusieurs variables. Par exemple la fonction “somme” associe un couple de 2 nombres à un nombre : somme(100, 28) = 128. Mais c’est tout ce dont nous aurons besoin pour ce livre. Une étude plus complète des ensembles, des relations et des fonctions nécessiterait aussi un livre entier.

La fonction somme est une bonne transition pour passer à un type particulier de fonction dans les ensembles de nombres qui va beaucoup nous intéresser dans ce livre : les opérations.

Les opérations

Nous connaissons tous les 4 opérations de base que l'on a apprises à l'école primaire : l'addition, la soustraction, la multiplication et la division.
Les mathématiciens qui aiment parfois compliquer les choses simples, appellent les opérations des ***"lois de composition".*** Elles permettent de composer deux éléments pour en engendrer un autre. En additionnant 2 nombres, on compose un nouveau nombre : le résultat de l'addition.
Ces lois de composition peuvent être "internes" ou "externes" à un ensemble. On dit qu'une loi de composition est interne à un ensemble quand, partant de deux éléments d'un ensemble, le résultat appartient toujours à ce même ensemble.

Par exemple, l'addition est une loi de composition interne dans l'ensemble des entiers naturels. L'addition de deux entiers naturels comme 100 et 320 donne un entier naturel : 420. Ceci est vrai quels que soient les entiers naturels considérés.

Par contre la soustraction n'est pas une loi de composition interne dans l'ensemble N. En effet, si on soustrait 8 à 5 : 5 - 8, on n'obtient pas un entier naturel, toujours positif, mais un entier relatif -3.

De même, la multiplication est interne dans N et Z. Quand on multiplie 2 nombres entiers, on obtient toujours un nombre entier : $12 \times 5 = 60\, et\, 3 \times (-4) = -12.$
On note la division de a par b soit sous la forme :
$\frac{a}{b}$ ou a/b.
La division n'est pas une loi de composition interne dans N et Z. En effet ¾ n'est pas un nombre entier mais un nombre décimal 0,75. La division d'un entier p par un autre entier q notée p/q ou $\frac{p}{q}$ donne un nombre rationnel.

Vous souvenez-vous quelle est la différence entre un nombre décimal et un nombre rationnel ?
Les nombres décimaux ont un nombre fini de chiffres après la virgule alors que les nombres rationnels peuvent en avoir un nombre infini comme dans le cas de 10/3 = 3,333333…..

Ce sont ces opérations qui ont amené les mathématiciens à explorer des régions (ensembles) de nombres de plus en plus vastes.

Dans les chapitres suivants, on s'intéressera à un cas particulier de division : la division euclidienne notée " ÷ ". A partir de 2 nombres entiers positifs, le dividende et le diviseur, on calcule un quotient et un reste :
$32 \div 6 = 5 \times 6 + 2$

32 est le dividende, 6 le diviseur, 5 est le quotient et 2 est le reste de la division. La division euclidienne est une relation qui relie un couple d'entiers naturels à un autre couple d'entiers naturels.

Nous l'avons déjà dit, on ne le répétera jamais assez, les mathématiciens sont économes en écriture. Cela ne date pas d'aujourd'hui, Evariste Galois (1811-1832) complétait rarement ses démonstrations qui finissaient souvent par "et donc etc… etc…". Ce qui ne plaisait pas à ses professeurs ! Certains de ses travaux incomplets ont été rédigés dans la nuit qui précéda le duel dans lequel il trouva la mort. La certitude de sa mort imminente, il avait eu "la bonne idée" de provoquer en duel un as de l'escrime pour une histoire d'amour, l'amena dans sa précipitation à laisser des pages de gribouillis décrivant des démonstrations incomplètes. Plus de 200 ans après sa mort, de nombreux chercheurs travaillent encore à déchiffrer ses manuscrits.

Une fonction intéressante le logarithme népérien

Le logarithme népérien, noté ln(p), est une fonction remarquable en mathématique. C'est une fonction, définie sur l'ensemble des réels strictement positifs donc aussi pour les entiers naturels, dont la particularité est de transformer un produit en somme :

$$\forall a, b \in \Re^{+*},\ ln(a \times b) = ln(a) + ln(b)$$

On en déduit facilement que la fonction transforme aussi une division en soustraction :

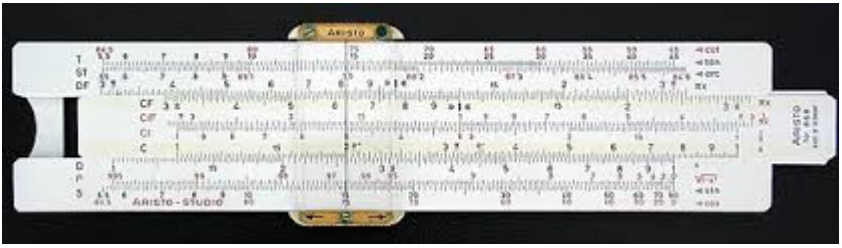
$$\forall a, b \in \Re^{+*},\ ln(\frac{a}{b}) = ln(a) - ln(b)$$

Le logarithme transformant une multiplication en addition, et il transforme une exponentiation en multiplication :

$$\forall a, b \in \Re^{+*},\ ln(a^{b}) = b \times ln(a)$$

Avant l'invention des calculatrices, les physiciens et les mathématiciens utilisaient des tables de logarithmes : des sortes d'annuaires qui donnaient le logarithme d'un nombre. Quand ils voulaient multiplier deux nombres, ils cherchaient leurs logarithmes et ensuite ils additionnaient ces logarithmes. L'addition est plus facile que la multiplication ! Dans une table de logarithme "inverse", ils trouvaient le nombre dont le logarithme est le résultat de l'addition et avait ainsi le résultat de la multiplication. En 1975 les lycéens utilisaient encore cette méthode pour résoudre les multiplications difficiles des applications numériques des problèmes de physique. La règle à calcul, encore en service à la même époque pour le bac,

est basée sur ce principe en ajoutant 2 longueurs, on trouve sur sa graduation le résultat d'une multiplication.



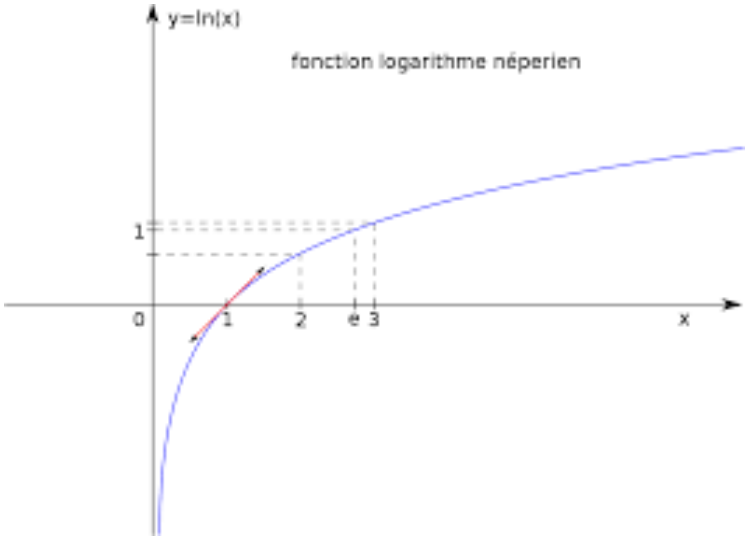
Les premières calculatrices (Texas Instrument, Rockwell, HP,...) sont devenues abordables pour les lycéens dès les années 80. Elles furent rapidement autorisées pour le bac et à l'université. Elles ont ainsi envoyé au musée les tables de logarithmes et les règles à calcul. Mais nous verrons plus loin dans les chapitres suivants que Gauss adorait lire son livre de tables de logarithme : "Vous n'avez pas idée de la poésie contenue dans une table de logarithme". C'est ainsi qu'il eut l'intuition qu'il y avait un lien entre la valeur du logarithme d'un nombre et le nombre de nombres premiers inférieurs à ce nombre ! Une calculatrice ne lui aurait sans doute pas permis cette formidable intuition qui a conduit à une conjecture sur laquelle les mathématiciens travaillent toujours.

Le logarithme ln(x) est une fonction qui croît lentement. Cette propriété est liée à une de ses définitions en effet la pente de la courbe de cette fonction est $f(x) = \frac{1}{x}$. Plus

x est grand, plus $\frac{1}{x}$ est petit et plus la fonction croît lentement.

Arrêtons-nous là pour cette fonction qui sera très utile quand on abordera la répartition des nombres premiers.

Courbe de ln(x):



Le raisonnement logique

Maintenant que nous maîtrisons l'écriture concise qui permet de décrire le paysage mathématique. Il nous faut regarder de plus près le moyen de locomotion dans ce

paysage qui va nous permettre de passer d'un énoncé à un autre : le raisonnement logique.
Dans un voyage, il y a un point de départ. Dans les mathématiques, ce sont les ***axiomes***.

Axiomes

Dans la théorie des nombres entiers, comme dans les autres théories, il y a des propositions que l'on considère comme vraies par définition : ***les axiomes***. Ce sont les points de départ des démonstrations. Elles ne peuvent être démontrées. Elles sont vraies par hypothèse..

Par la suite, dès qu'une proposition (ou *assertion*) est démontrée, on l'appelle "Théorème". Elle est vraie dans la théorie et peut être utilisée dans de futures démonstrations. On passe d'un axiome à un théorème ou d'un théorème démontré au suivant à l'aide du raisonnement logique. Ce raisonnement est contraint par des règles formelles comme le randonneur est contraint par les chemins praticables qui lui permettent de passer d'une montagne à l'autre.

Raisonnement

Le raisonnement logique, qui permet de passer d'un énoncé à un autre, en partant des axiomes utilise une

notation particulière. On les appelle des connecteurs logiques :

$\neg$: “Négation”, $\neg$A veut dire “le contraire de A”. C’est à dire si la proposition A est vraie alors la proposition $\neg$A est fausse et si A est fausse alors $\neg$A est vraie.

“et” ou $\wedge$: “Conjonction”, la proposition “A et B “ est vraie si la proposition A est vraie et la proposition B est vraie. “A et B” est fausse dans les autres cas.

“ou” ou $\vee$: “Disjonction”“, la proposition “A ou B“ est vraie si la proposition A est vraie ou la proposition B est vraie. “A ou B” est fausse si et seulement si A est fausse et B est fausse.

Attention le “ou” est inclusif en logique, alors que dans le langage courant, on l’utilise parfois de manière exclusive soit A est vraie, soit B est vraie mais pas les deux. On parle dans ce cas de “ou exclusif”.

$\Rightarrow$: “Inférence logique”, on écrit “A $\Rightarrow$ B”, qui se lit A implique B. Cela veut dire que si la proposition A est vraie alors la proposition B est vraie. Attention si A est faux on ne peut rien déduire de B.

⇔ : “Equivalence logique”, on écrit “A ⇔ B”, qui se lit A est équivalent à B. Cela veut dire que la proposition A et la proposition B ont toujours la même valeur de vérité. Si A est vraie, B est vraie, si A est fausse alors B est fausse. On peut utiliser l’équivalence pour introduire des définitions.

Voilà nous en savons assez pour lire les théorèmes fondamentaux concernant les nombres premiers. Avant de les aborder, pratiquons un peu. Une petite randonnée avant d'attaquer une expédition.

Par exemple comment définir l’ensemble des entiers naturels pairs. Donnons-lui un nom : “Pa”. Le définir en extension, c'est-à-dire en énumérant tous ses éléments, semble difficile vu qu’il y a une infinité de nombres pairs. Nous allons donc le définir en compréhension, en définissant la propriété des nombres pairs. En français on peut dire qu' un nombre est pair, si c’est un entier naturel multiple de 2. Nous pouvons donc écrire :

Définition :

“Un entier naturel a est pair” ⇔ "$\exists k \in N / \ a = \ 2 \times k$"

Le signe ⇔ indique bien que si on trouve un entier k de N tel que (le signe /) $a = 2 \times k$ alors a est pair et inversement.

On peut ainsi définir l"ensemble des nombres pairs.

Pa = $\{a \in N / \exists k \in N,\ a = 2 \times k\}$

Ce qui se lit l'ensemble Pa est l'ensemble des nombres a appartenant (le signe ∈) à l'ensemble N des entiers naturels, tel que, il existe (∃) un nombre k appartenant à N qui vérifie a = 2 x k.

Facile ?

Et pour les nombres impairs ?

Première méthode :

b est impair ⇔ $\exists k \in Pa \,/\, b = k + 1$

On définit un nombre impair comme le nombre qui suit un nombre pair ($a + 1$).

Deuxième méthode :

Un entier naturel b est impair ⇔ $\exists k \in N / \ b = 2 \times k$ +1

Laquelle préférez-vous ?

Maintenant une petite démonstration pour nous mettre en jambes. Démontrons que tout multiple de 6 est multiple de 3.

D'abord écrivons la définition générale d"un multiple d'un nombre a :

b est multiple de a $\Leftrightarrow \quad \exists k \in N/\ b = k \times a$

On a simplement écrit que b est multiple de a si il existe un nombre entier k qui multiplié par a donne b.

Donc b est multiple de 6 $\Leftrightarrow \exists k \in N/\ b = k \times 6$

Or $6 = 2 \times 3$ donc 6 est un multiple de 3 et on peut remplacer 6 par 2×3

Donc

$b = \ k \times 6 \Leftrightarrow b = k \times \ 2 \times 3 \Leftrightarrow b = k' \times 3 \Leftrightarrow b\ multiple\ de\ 3$

En prenant $k' = k \times 2$ on a trouvé un entier qui multiplié par 3 donne b. Donc b est multiple de 3.

Vous êtes maintenant prêt pour la suite. Les jeunes lecteurs, ou ceux qui ont continué à pratiquer les

mathématiques après des études scientifiques, ont sans doute trouvé cette partie un peu trop facile et verbeuse. Ce ne sera pas toujours le cas dans les pages qui suivent, mais accrochez vous, vous avez toutes les bases pour lire et assimiler ces fameux théorèmes fondamentaux.

Théorèmes Fondamentaux

Définition

Un entier naturel est premier s' il a deux diviseurs 1 et lui-même.

Par définition on considère donc que 1 n'est pas premier. 2 est premier. C'est le seul nombre pair premier.

Sous forme mathématique :

Soit $p \in N \quad , p > 1$,
$si\ (\forall\ k \in N,\ k \mid p \Rightarrow\ (k = 1 \vee k = p))\ alors\ p\ est\ premier.$

exemple : 2,3,5,...,107, 109,...
9564780647927552813573378126620390479441956306440 7
sont premiers.

La définition est simple. C'est pourquoi les nombres premiers sont connus depuis longtemps.

Crible d'Eratosthène

Le crible d'Ératosthène (276-194 avant J;-C.) est un procédé qui permet de trouver tous les nombres premiers inférieurs à un certain entier naturel donné n.

Graphiquement il consiste à construire un tableau de tous les nombres inférieurs à n. On élimine ensuite tous les multiples de 2, 3, 4,..., n . A la fin il ne reste que les nombres premiers.
exemple pour n = 100.

~~0~~	~~1~~	2	3	~~4~~	~~5~~	~~6~~	7	~~8~~	~~9~~
~~10~~	11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19
~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29
~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~
~~40~~	41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~
~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59
~~60~~	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~
~~70~~	71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79
~~80~~	~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89
~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~

Il ne reste que 2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97

Méthode :

- On raye 0 et 1, ils ne sont pas premiers.
- 2 est premier, on raye tous ses multiples.
- On passe au suivant non rayé, c'est 3. Il est premier, on ne le raye pas mais on raye tous ses multiples.
- On passe au suivant non rayé, c'est 5. Il est premier on ne le raye pas mais on raye tous ses multiples.
- Et ainsi de suite. On peut s'arréter au nombre entier qui suit $\sqrt{n}$, car comme $\sqrt{n} \times \sqrt{n} = n$, tous les nombres devant être rayés sont dèjà rayés. Ceux non rayés sont premiers.

Infinité des nombres premiers

L'ensemble des nombres premiers est infini.

Sous forme mathématique

Appelons P l'ensemble des nombres premiers, *card(P)* = ∞

La notion d'infini a longtemps soulevé de nombreux problèmes chez les mathématiciens qui ont préféré l'ignorer. En effet, les nombres sont définis comme étant la cardinalité d'un ensemble. Un nombre infini serait donc la cardinalité d'un ensemble infini. Mais cela pose des paradoxes comme celui illustré par l'hôtel de Hilbert : Un hôtel a un nombre de chambres infini. Un premier bus arrive avec un nombre infini de voyageurs. C'est un grand bus et ils sont bien tassés ! Chaque voyageur se voit attribuer sa chambre personnelle. Normal, le cardinal de l'ensemble des voyageurs est infini ainsi que celui de l'ensemble des chambres. On peut donc mettre en correspondance unique chaque voyageur et chaque chambre. Deux heures après, un autre bus chargé d'un nombre infini de voyageurs arrive. Ils n'ont pas réservé. L'employé leur répond que l'hôtel est plein. Mais il est assisté par un un stagiaire étudiant en mathématique qui lui dit : "Non pas de problème je vais trouver une chambre pour tout le monde". Il fait déplacer chaque arrivant du premier bus dans la chambre dont le numéro est le double de son numéro de chambre. Par exemple, l'occupant de la chambre 3 passe en chambre 6, celui de la chambre 4 en chambre 8,... Ainsi chaque arrivant du premier bus est logé dans une chambre dont le numéro est pair car c'est le double d'un numéro de chambre. Il ne reste plus qu'à loger les nouveaux arrivants dans les chambres aux numéros impairs. La cardinalité du premier bus est infinie. La cardinalité des chambres pairs

est infinie, en effet il y a une infinité de nombres pairs. On peut donc allouer une chambre à chaque occupant. De même pour le second bus avec les chambres impairs car la cardinalité de l'ensemble des nombres impairs est aussi infinie ! On a ainsi doublé la capacité de l'hôtel sans changer le nombre de chambres. Vous comprenez pourquoi les mathématiciens ont longtemps eu un problème à considérer l'infini comme un nombre. Il faudra attendre Georg Cantor (1845-1918), fondateur de la théorie des ensembles, pour formaliser la notion d'infini. Il a démontré d'ailleurs qu'il y a une infinité d'infinis de tailles différentes !

SI l'on veut éviter l'écueil de l'infini, on peut écrire qu'il n'y a pas de plus grand nombre premier ainsi :

$$\forall\, p \in P, \exists\, q \in P \,/\, q > p$$

Qui se lit, quel que soit p premier, il existe un nombre q premier tel que q est plus grand que p.

Donc on ne peut trouver de plus grand nombre premier. Euclide a démontré ce théorème au IIIème siècle avant J.-C. ! On étudiera la démonstration ainsi que d'autres dans le chapître dédié aux démonstrations.

Cette propriété est connue depuis plus de 2000 ans. Il n'y a pas de formule pour générer tous les nombres

premiers. Les ordinateurs ou autres machines à calculer rapides sont apparus dans la deuxième moitié du vingtième siècle. Alors vous avez sans doute deviné, les mathématiciens entrèrent en compétition pour trouver le plus grand nombre premier du jour.

Il n'y a pas de méthode pour trouver les nombres premiers *à coup sûr* mais il y a une formule qui donne souvent un nombre premier. On appelle les nombres générés par cette formule, les nombres de Mersenne. Marin Mersenne était un religieux mathématicien du XVIIe La formule est :

$2^n - 1$ avec n premier. On note ce nombre M_n.

Par exemple $M_3 = 2^3 - 1 = 7$. 7 et 3 sont premiers.

Si M_n est un nombre premier alors n est aussi premier mais malheureusement la réciproque n'est pas vraie. Il existe des nombres premiers n pour lesquels $M_n = 2^n - 1$ n'est pas premier.

C'est pourtant cette formule qui permit à Pietro Cataldi en 1588 d'affirmer que

$M_{17} = 2^{17} - 1 = 131071$ et

$M_{19} = 2^{19} - 1 = 524287$

sont premiers. Il le prouva en essayant toutes les divisions possibles !

Malheureusement il affirma aussi que M_{23}, M_{29}, M_{31}, M_{37} sont premiers. Il n'avait pas effectué tous les calculs et avait dû se contenter de preuves partielles ou de son intuition. C'est Pierre de Fermat en 1640 qui montra que M_{23} et M_{29} ne sont pas premiers et plus tard Euler montra que M_{31} et M_{37} ne le sont pas non plus. De plus leurs diviseurs ne sont pas très grands alors cela jeta un doute sur le fait que Pietro Cataldi ait vérifié M_{17} et M_{19}. Mais ils sont vraiment premiers, les ordinateurs modernes montrent qu'ils n'ont pas de diviseurs en quelques millisecondes.

Édouard Lucas (1842-1891), mathématicien Français, inventa un test de primalité pour les nombres de Mersenne qui lui permit de détenir le record du plus grand nombre premier en 1876 avec

M_{127} = 170 141 183 460 469 231 731 687 303 715 884 105.

Ce nombre resta le plus grand nombre premier connu jusqu'en 1951. Ensuite les ordinateurs et de nouveaux algorithmes pour tester la primalité entrèrent en jeu. En 2024 le record est :

$2^{136279841}$ - 1. Il contient 41 024 320 chiffres.

Un nombre plus grand que le nombre de tous les atomes et mêmes toutes les particules dans l'univers !

Ce nombre est premier. Il existe. Il a les propriétés d'un nombre premier. Pourtant aucun ensemble d'objets dans l'univers dit réel ne possède autant d'éléments. Si un nombre est simplement la cardinalité d'un ensemble, de

quel ensemble s'agit-il ? Ce nombre existe-il vraiment ? Dans quel univers ?

Unicité de la décomposition en nombres premiers

Si un entier naturel r n'est pas premier on dit qu'il est composé. Dans ce cas, r est un produit de nombres premiers. Cette décomposition est unique (à l'ordre près des facteurs).

Soyons explicite, que veut dire "à l'ordre près des facteurs". Il ne s'agit pas d'ignorer si les préposés à la distribution du courrier sont soigneux ou pas ! Mais simplement de ne pas tenir compte de l'ordre dans lequel apparaissent les facteurs premiers, car la multiplication est commutative dans N :

$105 = 3 \times 5 \times 7 = 7 \times 5 \times 3.$

Généralement on écrit les facteurs premiers par ordre croissants. De même on écrit généralement les facteurs apparaissant plusieurs fois sous forme de puissance :

$2 \times 3 \times 3 \times 5 \times 5 = 2 \times 3^2 \times 5^2$

Si on appelle P l'ensemble des nombres premiers

$\forall r \in N, \exists! \; p_1 \ldots p_k \in P \; et \; e_1 \ldots e_k \in N /$

$r = p_1^{e_1} \times \ldots \times p_k^{e_k}$

Donnons encore une fois, la traduction en français car cette formule est compliquée : Quel que soit l'entier naturel r, il existe une suite unique de nombres premiers notés p_i et d'exposants entiers naturels e_i tels que r est le produit de ces nombres premiers élevés à la puissance de ces exposants. Le mot important ici est "unique". Un entier naturel est la multiplication d'une suite unique de nombres premiers élevés à une puissance donnée.

ex : (3256 = 2^3 × 11 × 37)

Euclide dans son livre VI se rapproche de ce théorème en affirmant que tout nombre est divisible par un nombre premier. Il ne peut aller jusqu'à l'énoncé de la décomposition unique car à cette époque la notion d'élévation à la puissance d'un nombre n'était pas formalisée.

Si vous essayez de trouver, par vous même, la décomposition d'un nombre n en nombres premiers, vous constaterez tout de suite que cela peut-être très long et fastidieux. En effet il faut dans le cas général, connaître tous les nombres premiers inférieurs à ce nombre et essayer toutes les divisions les unes après les autres en ne gardant que celles dont le reste est nul. Dès que l'on trouve un nombre p qui divise n, vous

recommencez en essayant de trouver les diviseurs premiers de $\frac{n}{p}$.

Par exemple pour 987, on considérera la liste des nombres inférieurs à 987.

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983

On essaye 1 et 2, ça ne marche pas, les restes des divisions ne sont pas nuls. On essaye 3. Ça marche !

$987 \div 3 = 329$. On essaye ensuite de trouver les diviseurs de 329. Il faut essayer les 6 premiers nombres avant de trouver 7 qui donne un reste nul :

$329 \div 7 = 47$ et Bingo ! 47 est dans notre liste. On peut donc écrire :

$987 = 3 \times 7 \times 47$

Cette décomposition est unique. Quel que soit l'ordre dans lequel on essaye les diviseurs, on retombera toujours sur ce produit.

Il n'y a pas de formule donnant cette décomposition. On peut améliorer la méthode en tenant compte de certaines propriétés des nombres. Par exemple, les multiples de 5, 10 ou 3 sont facilement reconnaissables. Il n' y a donc pas besoin d'essayer avant de diviser. Mais dans le cas général pour de très grands nombres de plusieurs milliers de chiffres, il faudra essayer des millions de divisions. C'est ce qui fait l'intérêt pratique des nombres premiers dans les méthodes de cryptologie. Nous verrons cela plus tard.

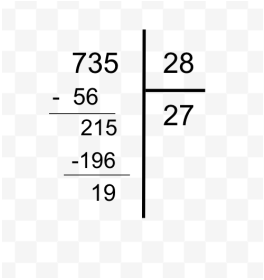
Division Euclidienne

La division Euclidienne, que l'on note ÷, associe à deux entier a et b avec $b < a$, une paire unique d'entiers naturels (q,r): le qotient q et le reste r, qui vérifient : $a = b \times q + r \, avec \, r < b$.

Exemple: 68 = 9 x 7 + 5. Le dividende est 68, le diviseur est 9. Le reste r = 5, le quotient q = 7

Savez -vous que nous ne posons pas tous les divisions de la même façon. Les Français utilisent la méthode de la potence que nous avons vu dans le préambule alors que les Anglais et les Américains utilisent la division longue.

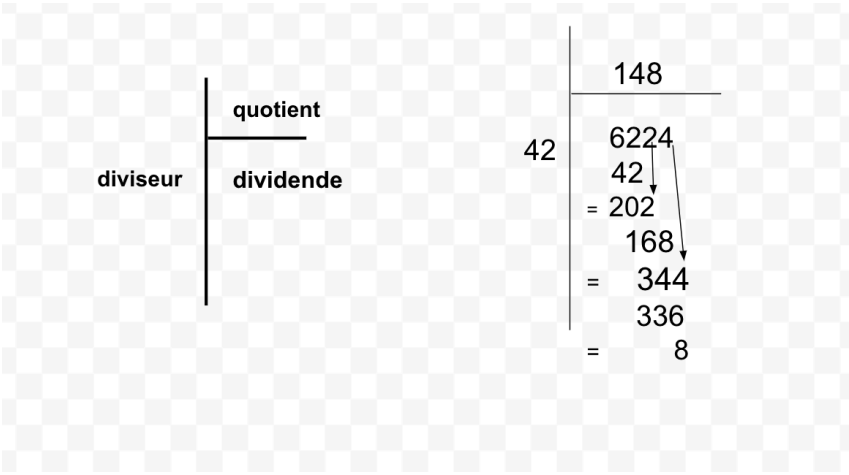
Méthode de la potence :
Le dividende est à gauche, le diviseur est à droite



Dans la division longue, le diviseur se place à gauche du dividende et le quotient au-dessus du dividende. Les différents restes et dividendes se placent sous le premier. Divisons à l'américaine 6224 par 42 :

On divise 62 par 42 il reste 20, le quotient est 1 on le monte en haut.
On fait descendre le chiffre du dividende suivant 2. On divise donc 202 par 42. Le quotient est 4, on le note en haut, on note le reste 34.
On fait descendre le 4. Cela donne 344, divisé par 42, le quotient est 8. On le monte. Le reste est 8, c'est inférieur à 42.

Voila c'est fini. Compliqué ? Et oui, beaucoup se demandent pourquoi les américains continuent à utiliser cette méthode.



PGCD de a et b

On note PGCD(a,b) le **Plus Grand Diviseur Commun** de 2 entiers naturels a et b.

On peut le noter : $a \wedge b$ (attention dans ce contexte " ∧ " n'est pas l'opérateur "et").
On peut dire que PGCD(a,b) est une fonction qui associe 2 entiers naturels à un autre entier naturel.

exemple: PGCD(32, 16) = 8

Si on considère que les nombres premiers sont les briques de base de chaque nombre, le PGCD est la plus grande brique commune. Comment trouver les PGCD de

deux nombres entiers. Euclide a trouvé une méthode toujours utilisée.

Algorithme d'Euclide

La méthode est basés sur le théorème suivant:

$Soit\ a, b\ \in\ N\ /\ a\ \geq$ b si r est le reste de $a\ \div\ b$, alors PGCD(a,b) = PGCD(b,r)

Ainsi pour calculer le PGCD, on effectue des divisions euclidiennes jusqu'à ce que l'on trouve un reste nul.

Exemple : On souhaite calculer le PGCD de 255 et 141. On effectue les divisions euclidiennes successives suivantes :

$$255=1\times 141+114$$

a= 255, b= 141 et r = 114

Donc le PGCD de 255 et 141 est le PGCD de 141 et 114. On continue.

$$141=1\times 114 + 27$$

Le PGCD de 141 et 114 est le PGCD de 114 et 27. On continue.

$$114=4\times 27+6$$

$\underline{27}=4\times\underline{6}+3$

$\underline{6}=2\times3+0$

Le PGCD de 255 et 141 est donc 3 car c'est le dernier reste non nul.

On dit que 2 nombres sont premiers entre eux s' ils n'ont pas de diviseur commun autre que 1.

Par exemple 24 et 35. $24 = 3 \times 8\, et\, 35 = 7 \times 5$

Ce sont des nombres qui ne partagent pas de brique de base.

Théorème de Bachet - Bézout

Ce théorème porte deux noms car il a été découvert par Bachet pour les nombres entiers et étendu à d'autres entités mathématiques comme les polynômes par Bézout, deux siècles plus tard.

Claude-Gaspard Bachet de Méziriac est né en 1581 à Bourg en Bresse. Il est poète, traducteur de poèmes en latin, grec et hébreu. A ses heures perdues, il est aussi mathématicien. Il a écrit un ouvrage : "*Problèmes plaisants et délectables qui se font par les nombres*." qui contient la

première démonstration de ce que l'on a appelé le théorème de Bachet-Bézout.
Étienne Bézout est né en 1730 en Seine et Marne. Il est mathématicien de la marine et est l'auteur du *"Cours de mathématiques à l'usage des gardes du pavillon et de la marine".*
SI on se limite aux entiers naturels, c'est-à-dire au théorème de Bachet. L'énoncé est le suivant :

Soient a et b deux entiers naturels non nuls. a et b sont premiers entre eux si et seulement si il existe deux entiers relatifs u et v tels que au + bv = 1.

En langage mathématique :

$$\forall a, b \in N,\ a\ premier\ avec\ b \Leftrightarrow \exists u, v \in Z / au + bv = 1$$

Notons que a et b ne sont pas uniques et peuvent être négatifs, ils appartiennent à Z.

On détermine les coefficients u et v en utilisant l'algorithme d'Euclide. Par exemple :

Les nombres a = 89 et b = 41 sont premiers entre eux.
En utilisant l'algorithme d'Euclide, on obtient :

(1) 89= 41 ×2 + **7** donc **7** = 89−41×2 = a−2b
(2) 41 = **7**×5 + *6* donc *6* = 41−7×5 = b−5(a−2b) = b−5a+10b = −5a+11b

(3) 7 = *6* × 1 + 1 donc 1 = 7 − 6 = a − 2b − (−5a + 11b) = a − 2b + 5a − 11b = 6a − 3b

On a donc montré que 6a + (−3) b = 1. Donc les coefficients u = 6 et b = −3 sont des coefficients de l'identité de Bachet.

PGCD et Théorème de Bachet

On peut généraliser le théorème de Bachet à tout couple d'entiers naturels :

Soient a et b deux entiers naturels non nuls.
d est le PGCD de a et b si et seulement si il existe deux entiers relatifs u et v tels que au + bv = d.

C'est une généralisation du théorème de Bachet vu précédemment. Car quand a et b sont premiers entre eux, leur PGCD vaut 1. En effet a et b étant premiers entre eux, ils n'ont pas de diviseur commun autre que 1 donc leur plus grand diviseur commun est 1.

On peut écrire

$$\forall a, b \in N,\ a\ premier\ avec\ b \Leftrightarrow PGCD(a,b) = 1$$

Comme précédemment, on utilise l'algorithme d'Euclide pour calculer u et v

exemple avec 190 et 75

190 = 75 x 2 + 40

75 = 40 x 1 + 35

40 = 35 x 1 + 5

35 = 5 x 7 + 0

Le PGCD est 5. On veut donc trouver u et v tel que

u x 190 + v x 75 = 5

On effectue ensuite le calcul en marche arrière en ne gardant que les valeurs 190 et 75 pour trouver les coefficients u et v.

De 40 = 35 x 1 + 5 on déduit 5 = 40 - 35 x 1 = 40 - 35

De 75 = 40 x 1 + 35 on déduit 35 = 75 - 40 x 1 = 75 - 40

De 190 = 75 x 2 + 40 on déduit 40 = 190 - 75 x 2

En effectuant chaque substitution

Donc 5 = 40 - (75 - 40) = 40 - 75 + 40 = 2 x 40 - 75

Le 40 nous ennuie. Or 40 = 190 - 75 x 2. On le substitue. Donc

5 = 2 x (190 - 75 x 2) - 75 = 2 x 190 - 2 x 75 x 2 - 75

= 2 x 190 - 5 x 75 = 2 x 190 +(-5) x 75

2 et -5 sont donc des entiers tels que 190 x + 75 y = 5

Ces calculs ne sont pas faciles. Ils nécessitent de ne pas perdre de vue ce que l'on cherche et parfois un peu d'astuce. C'est pourquoi on les retrouve souvent dans les examens d'arithmétiques de tout niveau. En particulier dans les problèmes de mathématiques, pour ceux qui ont choisi la spécialisation mathématique

Théorème de Gauss

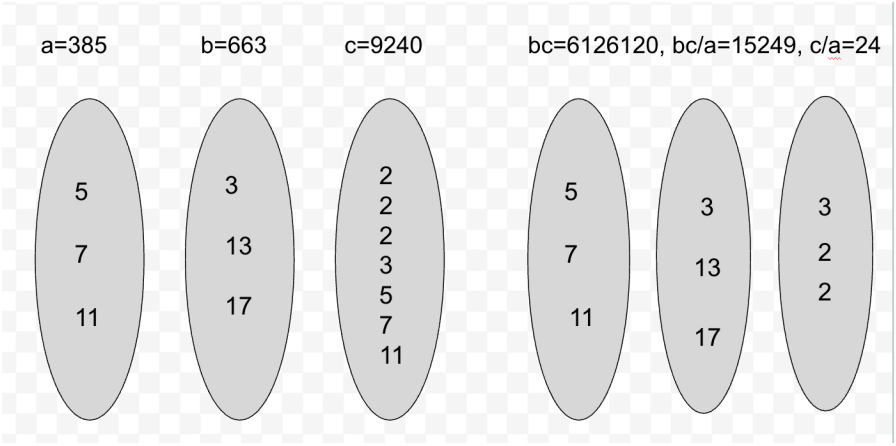
Soient a, b et c trois entiers naturels non nuls. Si a divise le produit bc et si a est premier avec b alors a divise c.

En langage methématique :
$\forall\, a, b, c \in N,\ pgcd(a, b) = 1\ et\ a \mid bc \Rightarrow a|c$

Exemple : 37 et 62 sont premiers entre eux. En effet 37 est premier, il n'a pas de diviseur autre que 1 et 37 et comme 37 ne divise pas 62 on en conclut que 37 et 62 n'ont pas de diviseur commun. Ils sont donc premiers entre eux.

Prenons $4588 = 62 \times 74$. Or 37 divise 4588 : $4588 \div 37 = 124$ donc 37 divise 74. En effet $74 \div 37 = 2$.

Une manière simple de comprendre ce théorème important est de visualiser les nombres comme des ensembles constitués de leurs briques de base : leur décomposition en nombres premiers.



Nous comprenons que comme a et b sont premiers entre eux, ils n'ont pas de brique commune. bc va contenir les briques de b et les briques de c donc aussi les briques de a car a divise bc. Donc les briques de a vont être contenues dans la partie de bc qui ne contient pas les briques de b donc dans c. Ce qui explique pourquoi a divise c.

Corollaire important:

C'est quoi ce nouveau terme "***corollaire***"? On appelle corollaire une conséquence directe d'un théorème.

Soient a, b et n trois entiers naturels non nuls, avec a et b premiers entre eux. Si n est divisible par a et b alors n est divisible par le produit ab.

$\forall\, a, b, n \in N,\ PGCD(a, b) = 1\ et\ a \mid n\ et\ b \mid n \Rightarrow ab \mid n$

Exemple: 8 et 9 premiers entre eux. 144 est divisible par 8 et 9 donc 144 est divisible par 72

(72 = 9 x 8 et 144 = 72 x 2)

Application

Ainsi, par exemple, pour montrer qu'un nombre et divisible par 6, il suffit de montrer qu'il est divisible par 2 et par 3.

Attention il faut que a et b soit premiers entre eux. 2 et 3 le sont.

Résolution des Équations Diophantiennes

Diophante est un mathématicien d'origine grecque. On ne sait pas grand-chose sur lui. Il est né entre le 1er et le 4ème siècle. Ce n'est pas très précis pour un mathématicien. Il est connu pour son ouvrage le plus important *"Les Arithmétiques".* Un ouvrage dont on a perdu la plus grande partie. Il reste donc célèbre pour

ses équations à deux inconnues entières du style : $a \times x + b \times y = c$ que l'on écrit en abrégé, en supprimant le signe multiplication comme souvent entre des valeurs littérales :

ax + by = c

où a, b et c sont des entiers relatifs et où les inconnues x et y sont aussi des entiers relatifs. Diophante précise que les solutions x et y peuvent être des entiers négatifs. Entiers qu'il qualifie d'absurdes. C'est à Diophante que l'on doit cette fameuse formule apprise au collège "- par - égal +, - par + égal -".

Par exemple $-5 \times 3 = -15$ alors $-5 \times -3 = 15$

Essayons de résoudre une équation Diophantienne. Par exemple $5 \times x - 3 \times y = 7$. Des équations de ce type sont étudiées en terminale spécialité mathématiques !

1. On cherche une solution particulière de l'équation. Par exemple : x = 2 et y = 1
2. On écrit le système d'équations composés de l'équation initiale et l'égalité résultant de la solution trouvée :
$5 \times x - 3 \times y = 7$ et $5 \times 2 - 3 \times 1 = 7$
3. En soustrayant les 2 égalités on obtient:
$5(x - 2) - 3(y - 1) = 0\ cad\ 5(x - 2) = 3(y - 1)$
4. On trouve la forme générale des solutions en appliquant le théorème de Gauss : 3 divise $5(x - 2)$. Comme 3 et 5 sont premiers entre eux, 3 divise $(x - 2)$. Donc
$\exists\, k \in Z / (x - 2) = 3 \times k \Rightarrow \exists\, k \in Z / x = 3 \times k + 2$

5. En remplaçant x dans l'égalité précédente on obtient :
$5(3k + 2 - 2) = 3(y - 1) = 15\,k \Rightarrow y = 1 + 5k$
6. Les solutions sont donc de la forme $x = 3k + 2$ et
$y = 1 + 5k\ avec\ k \in Z$
7. Réciproquement on vérifie que les x et y de cette forme vérifient toujours l'équation
$5 \times (3k + 2) - 3 \times (1 + 5k) = 15k - 15k + 10 - 3 = 7$

Pas évident, les équations Diophantienne ne sont pas populaires parmi les étudiants des classes préparatoires. Il n'y a pas de formules ou de méthodes qui donnent facilement la solution. Il faut trouver une astuce, en utilisant les théorèmes de Bachet-Bézout et le théorème de Gauss. Soit l'étudiant trouve l'astuce dans le temps imparti pour l'examen, soit il rame. Et cela dure depuis 2000 ans !

De nouvelles notions de base

Il est nécessaire d'introduire de nouvelles syntaxes et de nouvelles notions pour pouvoir continuer dans la découverte des théorèmes fondamentaux.
Dans nos contemplations sur les sommets de la chaîne de montagne du pays des nombres premiers, de nouveaux outils sont nécessaires. Il nous faut des paires de jumelles plus puissantes, des méthodes de mesures plus complètes afin de mieux noter nos observations.
Revenons donc aux notations. Vous vous souvenez que ce sont les symboles grecs qui permettent aux

mathématiciens d'être fainéants du stylo et de remplacer de longues phrases ambigües par des signes cabalistiques denses et précis. Mais souvent ces signes, ces lettres grecques en effraient plus d'un. Donc pas de panique, on va introduire doucement avec force exemples ces nouveaux symboles :

Comment écrire une longue suite de multiplication du style : $(1-2) \times (1-3) \times (1-4) \times \ldots \times (1-8)$
On introduit un nouveau symbole le Π majuscule muni de 2 indices qui indiquent le début et la fin de la séquence qui suit :

$\prod_{i=1}^{8}$: Ce signe sur 3 étages indique le produit pour tous les entiers i de 1 à 8 de l'expression qui suit.

Par exemple :

$$\prod_{i=1}^{8}(1-i) = (1-1) \times (1-2) \times \ldots (1-8).$$

On a remplacé la valeur de i, dans l'expression $(1-i))$ par les valeurs entre la borne inférieure en bas du signe et la borne supérieure en haut du signe:

$\prod_{i=1}^{8}$

Dans ce cas, il s'agit de 1 et 8.

La factorielle de a est le produit de tous les nombres entiers inférieurs à a. Donc on peut l'écrire :

$a! = \prod_{i=1}^{a} i = 1 \times 2 \times \ldots \times a$

Exemple : $4! = \prod_{i=1}^{4} i = 1 \times 2 \times 3 \times 4 = 24$

De même on peut écrire une longue suite d'additions avec le signe sigma majuscule muni de 2 indices de début et de fin :

$\sum_{i=1}^{a}$: indique la somme pour tous des entiers de 1 à a de l'expression qui suit.

Exemple :

$\sum_{i=1}^{12} i = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12.$

Le mathématicien Gauss, génie précoce mais parfois agité en classe, a trouvé une formule pour cette somme de n nombres consécutifs. Son professeur, afin de le calmer, lui demanda de calculer la somme de tous les nombres de 1 à 100. Il espérait avoir la paix dans sa classe pendant au moins 10 minutes. Mais Gauss répondit quelques secondes plus tard : "5550". En effet il avait trouvé par lui même la formule :

$$\sum_{i=1}^{a} i = \frac{a \times (a+1)}{2}$$

Donc la somme de tous les entiers de 1 à 100 vaut
$\frac{100 \times 101}{2} = \frac{10100}{2} = 5550$

La démonstration de cette formule est élégante, et vous pourrez la trouver au début de la partie démonstration.
Je profite de l'introduction de ces signes cabalistiques pour ouvrir un débat. Pourquoi les mathématiciens ont-ils besoin d'introduire de tels symboles souvent basés sur des lettres grecques ?

Nous l'avons déjà dit et répété, les mathématiciens sont avares d'écriture et aiment la concision. Les idées, les intuitions, pour certains les révélations, naissent dans leur tête. Alain Connes mentionne que ses meilleures idées naissent lors de ses marches. De retour à la maison, ils doivent noter et surtout prouver. Pour certains c'est une perte de temps, tant leur intuition les a convaincu de la véracité des conclusions. Gauss et Riemann étaient les Ayatollahs de la preuve. Ils ne voulaient rien publier tant qu'ils n'avaient pas de preuve irréfutable de leurs théorèmes. De nombreux théorèmes ou idées de Riemann sont restés au niveau de conjectures. Il est mort rapidement d'une pleurésie et sa

femme de ménage a détruit une grande partie de ses écrits qui contenaient des démonstrations qu'il ne jugeait pas assez abouties pour les publier !

Pendant longtemps, les mathématiciens écrivaient à la main sans ordinateur. Il n'y avait pas de clavier donc l'utilisation de lettres grecs, absentes des claviers modernes, n'était pas un problème. Aujourd'hui il faut un logiciel spécial et un langage dédié que l'on appelle LaTex pour écrire ces formules remplies de symboles grecs qui souvent nécessitent des empilements de lettres (exposants, indices). Les langages de programmation inventés pour les informaticiens à l'époque des ordinateurs et des claviers ont choisi de se passer de ces signes qui modifient l'espace entre les lignes et nécessitent des caractères absent de la plupart des claviers. Par exemple dans le langage C, l'expression

$t = \sum_{i=1}^{5} (3 + i)$ s'écrira :

```
for( i=1, i <= 5 ; i++) t = t + (3+i);
```

Pas d'exposant, pas d'indice, tout est sur le clavier.

x_3^4, c'est à dire le troisième élément d'une suite de nombre x_1, x_2, x_3 élevé à la puissance 4 pourra s'écrire en

language C : pow(x[3] ,4). La fonction pow(a,b) vient de l'anglais "power" qui veut dire puissance donc pow(x[3],4) veut dire $x[3]^4$ et $x[3]$ représente le troisième élément d"une suite de nombres.

Ces notations à base de lettres grecques, d'exposants et d'indices ont survécu à la révolution informatique. Est ce que ce sera toujours le cas ?

Kenneth E. Iverson (1920-2004) avait créé un langage informatique avec des caractères spéciaux nécessitant un clavier dédié (voir ci-dessous) pour les applications mathématiques (publications, programmes), en particulier celles utilisant des matrices (tableaux de nombres). IBM a commercialisé un clavier spécial et même une machine à écrire mécanique utilisant ces symboles.

Ce langage APL pour lequel Lenneth E. Iverson a reçu le prix Alan Turing (Nobel des informaticiens) en 1970 n'a pas survécu à l'émergence des ordinateurs personnels.

La diaclarisation (accents) des langages naturels comme le français ou l'espagnol avec ses é, è, à,... nécessitent aussi des claviers différents pour écrire en anglais ou en français. Résistera-t-elle ?

Nous en savons maintenant assez pour aborder un nouveau théorème.

Théorème de la caractérisation par la décomposition

Un produit de facteurs premiers divise un autre produit de facteurs premiers si et seulement si pour chacun des facteurs premiers la multiplicité dans le premier produit est inférieure à la multiplicité dans le second.

$$\prod_{i=1}^{k} p_i^{a_i} \mid \prod_{i=1}^{k} p_i^{b_i} \Leftrightarrow a_i \leq b_i \text{ pour tout i}$$

On appelle Plus Petit Commun Multiplicateur de a et b, le plus petit entier naturel multiple de a et b. On le note PPCM(a,b). On appelle Plus Grand Diviseur Commun de a et b, le grand entier naturel qui divise a et b. On le note PGCD(a,b).
On peut calculer les PPCM et les PGCD de 2 nombres à l'aide de leurs décompositions en nombres premiers.
Prenons 2 nombres n et m tels que leurs décompositions sont :

$n = \prod_{i=1}^{k} p_i^{a_i}$ et $m = \prod_{i=1}^{l} p_i^{b_i}$

On montre que :

PGCD(n,m) = PGCD($\prod_{i=1}^{k} p_i^{a_i}$, $\prod_{i=1}^{l} p_i^{b_i}$) = $\prod_{i=1}^{min(k,l)} p_i^{min(a_i,b_i)}$

PPCM(n,m) = PPCM($\prod_{i=1}^{k} p_i^{a_i}$, $\prod_{i=1}^{l} p_i^{b_i}$) = $\prod_{i=1}^{max(k,l)} p_i^{max(a_i,b_i)}$

PGCD(n,m) x PPCM(n,m) = n x m

Vous avez sans doute atteint avec ces formules une indigestion de produits et d'indices. Ce n'est pas facile à lire. Le concept est pourtant bien simple. On note la décomposition en facteurs premiers de 2 nombres. On regarde ensuite les facteurs premiers en commun et la valeur de leurs exposants que l'on appelle multiplicité. Il est normal que l'un divise l'autre si tous les facteurs premiers de l'un sont compris dans l'autre.

exemple : $72 = 2^3 \times 3^2$, $63 = 3^2 \times 7$

Pour appliquer la formule on utilise l'astuce consistant à faire apparaître les mêmes facteurs premiers p_i dans chaque expression. Il suffit de constater que tout nombre entier naturel élevé à la puissance 0 vaut 1. Par exemple : $6^0 = 1$ et que on ne change pas un nombre en l'élevant à la puissance 1 : $6^1 = 6$

On peut donc écrire :

$72 = 2^3 \times 3^2 \times 7^0$ et $63 = 2^0 \times 3^2 \times 7^1$

En prenant les maximums et les minimums de chaque exposant, on obtient

$PGCD(72, 63) = 2^0 \times 3^2 \times 7^0 = 3^2 = 9$

$PPCM(72, 63) = 2^3 \times 3^2 \times 7^1 = 8 \times 9 \times 7 = 504$

On dit d'un nombre p qu'il est une puissance $q^{ème}$ si il existe un nombre entier naturel n tel que n^q = p.

On montre que :

Si la décomposition de p est $p = \prod_{i=1}^{k} p_i^{a_i}$ alors p est une puissance $q^{ème}$ si tout a_i est un multiple de q.

Quittons ces indices indigestes. Nous les retrouverons rapidement.

Anneaux, Groupes, Idéaux et Corps.

De même qu"il nous a fallu introduire de nouveaux symboles pour comprendre les théorèmes précédents, nous allons introduire de nouveaux objets mathématiques pour les énoncés suivants. Ces objets sont des ensembles munis d'opérations. Ils ont des propriétés si intéressantes que les mathématiciens leur ont donné des noms spécifiques tirés du langage commun : les anneaux, les groupes, les idéaux et les corps.

Abandonnons donc pour une page ou deux les nombres entiers et généralisons nos définitions à tout ensemble d'éléments que nous appellerons A et B.
Et pour continuer notre abstraction, parlons d'une opération quelconque que l'on notera * (lire étoile) au lieu de nous limiter à l'addition et la multiplication.

Une opération * est appelé ***loi de composition* de A vers B** quand elle relie tout couple d'éléments de A à un élément de B.

$\forall a, b \in A,\ a * b \in B$

On parle de ***loi de composition interne*** quand les ensembles A et B sont les mêmes. On prend un élément de A et un autre élément de A et on obtient un élément de A.

Un ***groupe*** (A,*) est un ensemble A muni d'une loi de composition * si les propriétés suivantes sont réunies :

1) * est une loi de composition interne.
$\forall a, b \in A,\ a * b \in A$

2) L'ensemble possède un élément neutre.
$\forall a \in A,\ a * e = a$.

3) Chaque élément de A possède un élément symétrique.
$\forall a \in A,\ \exists\, b \in A \,/\, a * b = e$

4) La loi est associative.
$\forall a, b, c \in A \,/\, a * (b * c) = (a * b) * c$

4 propriétés sont donc requises pour qu'un couple ensemble et loi de composition forme un groupe.

On parle de groupe commutatif quand
$\forall a, b \in A \,/\, a * b = b * a$

Illustrons ces notions avec un ensemble et une loi connue, les entiers relatifs Z et l'addition "+". On remarque et on démontre que l'addition est une loi de composition interne dans Z.
Si je prends 2 nombres entiers comme 3 et 6 et si je les additionne, le résultat 9 est toujours un nombre entier. L'addition est donc bien dans ce cas une loi de composition interne dans Z. Notons que c'est un exemple, cela ne constitue pas une démonstration !
Il faut un élément neutre, c'est-à-dire un nombre que l'on peut ajouter à tout nombre sans changer ce dernier. Vous avez deviné ? Ce nombre c'est le 0.
Ce nombre est apparu assez tard dans l'histoire des mathématiques. Euclide voyait les nombres comme des longueurs ou des rapports de longueurs, donc peu de place pour le zéro. Pour compter des objets, ce n'était pas très utile non plus. Il a fallu attendre l'an 628 pour que Brahmagupta (598-660) définisse le zéro dans un traité d'astronomie. Il le définit comme la soustraction d'un nombre par lui-même (a - a = 0).

Chaque nombre doit posséder un symétrique. C'est-à-dire un compagnon qui produira 0 après addition. Nous sommes dans l'ensemble des entiers relatifs. Les nombres négatifs sont les compagnons rêvés des nombres positifs. $3 + (-3) = 0$, -3 est donc le symétrique de 3, chaque nombre à son symétrique.

La loi doit être associative. Qu'est ce que cela veut dire ? Simplement que l'addition de 3 nombres ne dépend pas de l'ordre dans lequel vous effectuez les additions :
$3 + (4 + 5) = 3 + 9 = 12 = (3 + 4) + 5.$
Je peux commencer par les deux premières additions ou les deux dernières, le résultat est le même.
Z muni de l'addition, noté (Z,+) est donc un groupe. Et de plus ? Il est commutatif. C'est à dire que l'on peut commuter les opérandes : $9 + 5 = 5 + 9 = 14.$

Tous les ensembles de nombres munis de l'addition ne sont pas des groupes. En effet (N,+) n'est pas un groupe car les éléments n'ont pas de symétrique. Prenons 3, il appartient bien à N, mais il n'y a pas de nombre dans N qui ajouté à 3 donne 0. En effet -3 n'est pas dans N.

De même on peut facilement remarquer et même démontrer que l'ensemble des entiers relatifs munis de la multiplication, noté (Z,×) n'est pas un groupe car seul 1 a un symétrique :
1 est l'élément neutre de (Z,x). En effet quand on multiplie un nombre par 1, on ne le change pas : $3 \times 1 = 3$
mais il n'y a pas de nombre entier qui multiplié par 3 donne 1. 3 n'a pas de symétrique.
$\frac{1}{3}$ est le symétrique de 3 car $3 \times \frac{1}{3} = 1$

Mais $\frac{1}{3} \notin Z, \frac{1}{3} \in Q$

L'ensemble des nombres rationnels (des fractions).

Regardons maintenant la notion d'**Anneau**. Il nous faut introduire une deuxième loi, notons la ○ (prononcer "rond").

On dit que l'ensemble A muni des lois de composition interne * et ○ est un ***Anneau*** si et seulement si $(A, *)$ est un groupe et la loi ○ est distributive par rapport à la loi *
Ce qui peut s'écrire :
$\forall a, b, c \in A,\ c \circ (a * b) = (c * a) \circ (c * b)$

La distributivité est un nom bien choisi pour cette propriété d'une opération sur une autre. En effet on distribue l'opération ○ sur les deux opérandes de la première opération *

Cela va mieux avec un exemple. La multiplication peut être distribuée sur les 2 opérandes de l'addition :
$3 \times (4 + 7) = (3 \times 4) + (3 \times 7) = 33$
Cette propriété est vraie, quels que soient les entiers relatifs choisis, donc (Z,+,x) est un anneau.

On peut constater que (Z,+,-) n'est pas un anneau car
$3 - (4 + 7) = 3 - 11 = -8$

Alors que
$(3 - 4) + (3 - 7) = -1 + (-4) = -5$

Les anneaux nous permettent d'atteindre l'Idéal ! On appelle ***idéal*** *I* de l'anneau (A,*,○) un sous ensemble I de A si :

- (I,*) est un groupe
- ○ est une loi de composition interne dans I :

$\forall a, b \in I,\ a \circ b \in I$

Par exemple on pourra vérifier que l'ensemble des multiples de m que l'on note mZ est un Idéal de Z. On montre aussi la réciproque, plus surprenante que tout idéal de Z est de la forme mZ.

Illustrons avec un exemple. Soit l'ensemble des multiples de 5 que l'on note 5Z :
5Z = {...-20,-15,-10,0,5,10,15,20,....}

(5Z,+,x) est un Idéal de Z, en effet : (5Z,+) est bien un groupe car :

1. + est une loi de composition interne. Quand on additionne 2 multiple de 5 on obtient un multiple de 5. $15 + 30 = 45$
2. 0 est l'élément neutre de l'addition et c'est bien un multiple de 5 car 0 = 5 x 0.
3. Chaque élément a un symétrique. $15 + -15 = 0$

4. L'addition est associative. Peu importe dans quel ordre on additionne les nombres, on trouve le même résultat :
$5 + (10 + 20) = (5 + 10) + 20 = 35$
5. La multiplication est une loi de composition interne
Par exemple : $15 \times 10 = 150 = 5 \times 30$

On montre aussi que l'ensemble aZ + bZ de toutes les combinaisons linéaires du type ax+by avec $a, b, x, y \in Z$ est un Idéal de Z. Par exemple, l'ensemble 5Z + 3Z est un idéal de Z. Il suffit de démontrer que (5Z + 3Z, +) est un groupe et que la multiplication est distributive sur l'addition dans ce groupe.

Illustrons cette propriété par un exemple :
Choisissons 3 éléments de 5Z+3Z que l'on nommera a,b et c. C'est à dire des nombres résultant de l'addition d'un multiple de 5 et d'un multiple de 3 :

- $a = 5 \times 2 + 3 \times 8 = 34$
- $b = 5 \times (-1) + 3 \times 4 = 7$
- $c = 5 \times 4 + 3 \times (-2) = 14$

Constatons à l'aide de ces 3 nombres que (5Z + 3Z, +) est un groupe :

- L'addition est une loi de composition interne si on additionne 2 nombres de (5Z+3Z) on trouve un autre nombre 5Z+3Z. Dans notre exemple :

$a + b = 34 + 7 = 41 = 5 \times 7 + 3 \times 2$

- L'élément neutre 0 appartient bien à 5Z+3Z en effet : $0 = 5 \times 0 + 3 \times 0$
- Chaque élément a un symétrique : Le symétrique de 34 est -34 car $34 + (-34) = 0$ et -34 appartient bien à 5Z + 3Z : $-34 = 5 \times (-2) + 3 \times (-8)$
- L'addition est associative dans (5Z+3Z) car elle l'est pour tout élément de Z.

Il ne nous reste plus qu'à observer sur notre exemple que la multiplication est une loi de composition interne et distributive sur l'addition.

- $a \times b = 34 \times 7 = 238 = 5 \times 14 + 3 \times 56$
- $a \times (b + c) = 34 \times (7 + 14) = 714$ et

$a \times b + a \times c = 34 \times 7 + 34 \times 14 = 714$

Attention le paragraphe qui précède n'est pas une démonstration, c'est un exemple du théorème.

Introduisons maintenant le Graal des ensembles munis de lois : **Le Corps.**

On dit que l'ensemble A muni des lois de composition internes ° et ○(A,*,○) est et un corps si et seulement si :
(A,*) est un groupe.
(A^*,○) est un groupe
La loi ○ est distributive sur la loi *.

Que signifie A^*, dans ce contexte c'est l'ensemble A, privé de l'élément neutre de l'opération *. On peut aussi le noter :
A/{0} si 0 est l'élément neutre de *.
Par exemple Z^* est l'ensemble de tous les entiers relatifs privés de 0.

Le corps est le top du top dans la hiérarchie des ensembles munis de lois de composition interne. Pour la vie de tous les jours, c'est la normalité car depuis notre enfance nous manipulons les opérations de base que sont l'addition "+" et la multiplication "x" dans l'ensemble des nombres rééls et (R,+) est un groupe, $(R^*,\times)$ est aussi un groupe et la multiplication est distributive sur l'addition.

Petit rappel :
- (R,+) est un groupe :
- L'élément neutre est 0. Par exemple $5 + 0 = 5$
- Le symétrique de 5,812 est -5,812, de π est $-\pi$.

Le symétrique pour l'addition est souvent nommé **l'opposé**.
- $(R^*$,x) est un groupe :
- L'élément neutre est 1. Par exemple $5 \times 1 = 5$
- Le symétrique de 5,812 est $\frac{1}{5{,}812}$ de π est $\frac{1}{\pi}$. Le symétrique pour la multiplication est appelé " l'inverse".

Si un élément possède un inverse, on dit qu'il est inversible. Seul 0 n'est pas inversible mais 0 n'appartient pas à R^* !

- La multiplication est distributive sur l'addition :
- $3 \times (2 + 6) = 3 \times 2 + 6 \times 2$

Donc (R,+,X) est un corps. Respect pour l'ensemble des réels !

Peut-être avez-vous remarqué que l'on met des parenthèses quand on veut indiquer qu'il faut effectuer les additions avant les multiplications mais pas pour les multiplications. C'est une facilité d'écriture, on dit que la multiplication est prioritaire sur l'addition. Ainsi il n'y a pas de besoin d'écrire :
$(3 \times 2) + (6 \times 2)$ pour indiquer que l'on effectue les deux multiplications avant l'addition pour obtenir $6 + 12$.
On peut écrire simplement $3 \times 2 + 6 \times 2$
Dans leur flemme pour l'écriture, les mathématiciens se dispensent même d'écrire explicitement le signe de la multiplication $\times$ quand les opérandes sont des valeurs littérales (des lettres). Ainsi $8 = abc$
est un raccourci pour $8 = a \times b \times c$

C'est Evariste Galois qui a introduit la notion de groupe en 1830. Cette notion fut formalisée vers 1870. Elle est aujourd'hui étendue à de nombreux domaines des mathématiques dans lesquels la notion de symétrie est

importante. Par exemple un Rubik's cube et ses manipulations muni d'une loi de composition interne forment un groupe. Un groupe qui tient dans la main !

Il y a beaucoup de littérature sur le sujet sur internet [6]. Ce type d'article requiert des connaissances sur la théorie des groupes plus importantes que celles dont nous aurons besoin dans ce livre.

Il nous suffit ici de noter que si on appelle une "manipulation", l'action qui consiste à faire passer le cube d'un état à un autre (sans le démonter !) et que l'on note M l'ensemble de toutes les manipulations possibles et ∂ l'opération "suivie de", on peut facilement constater que (M,∂) est un groupe.
En effet :
1. ∂ est une loi de composition interne, une manipulation suivie d'une autre manipulation donne une manipulation.
2. L'élément neutre est la manipulation qui consiste à ne rien faire. Notons la O

3. Le symétrique d'une manipulation est la manipulation en "sens inverse". En effet si on nomme S^{-1}, la manipulation inversé de S,

$S \partial S^{-1}$ = O. On peut toujours faire une manipulation en sens inverse, donc chaque manipulation a un symétrique.

4. ∂ est associatif si on effectue à la suite S_1et S_2, on pause et ensuite S_3, on obtient le même résultat que si on effectue S_1, une pause et ensuite S_2et S_3.

$(S_1 \partial S_2) \partial S_3 = S_1 \partial (S_2 \partial S_3)$

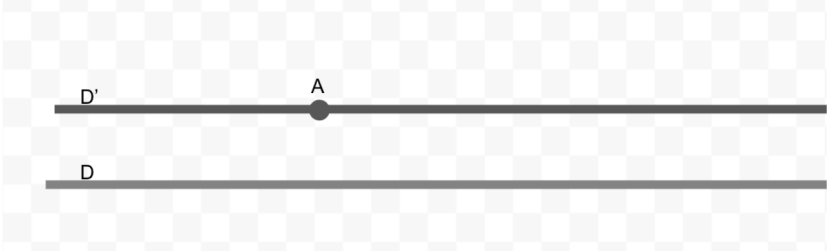
On peut bien sûr essayer d'être plus précis et de classifier les manipulations possibles et les états du cube correspondants. Vous trouverez cela dans la référence [24] ou d'autres sites sur internet. Ce sont souvent des sites de cours de licence de mathématiques.

Nous en savons maintenant assez sur les principes de base des mathématiques et en particulier sur les nombres entiers, l'addition et la multiplication pour aborder la suite des théorèmes fondamentaux. Il nous suffit de garder en tête que (Z,+,x) est un anneau.

Permettons-nous une nouvelle digression, avant d'aborder un sujet plus ardu. Alain Connes mentionne dans une interview à France Inter en 2023 que les

mathématiques sont avant tout un langage. Mais que ce langage à la différence des autres est auto-génératif. En effet, un dictionnaire de Français, contient des mots et des verbes utilisés à une époque donnée pour décrire le monde réel. Chaque définition est décrite avec d'autres mots du dictionnaire. Les mathématiques sont différentes, elles génèrent elles même de nouveaux objets. On pourrait arguer que ces nouveaux objets ne sont que des abréviations de concepts inventés mais cette vue se heurte à l'incroyable efficacité des mathématiques pour expliquer le monde réel. Euclide a défini la géométrie par 5 axiomes. Le cinquième précise que par un point il ne passe qu' une seule droite parallèle à une autre droite. De nombreux mathématiciens ont essayé pendant des siècles de démontrer que ce cinquième axiome était redondant et qu'il était une conséquence des 4 premiers. Ce n'était pas le cas et Hilbert a été le premier à formaliser des géométries non Euclidiennes. Dans ces géométries, par un point il pouvait passer une infinité de droite parallèles à une autre droite ou bien aucune droite. Ces géométries étaient cohérentes. On ne pouvait en déduire des théorèmes à la fois vrais et faux. Les cinquièmes axiomes alternatifs (une infinité de droite ou aucune) n'étaient pas en contradiction avec les quatre premiers. Ces géométries étaient considérées comme des bizarreries. Cela ne servait à rien, le monde était

Euclidien, par un point on ne peut faire passer qu' une seule droite parallèle à une autre.
Dans le dessin suivant, il est évident que D’ est l’unique droite passant par A et parallèle à la droite D.



Car ce dessin est tracé sur un plan non courbé. Si on trace les droites sur une sphère ou une forme en selle de cheval. Il peut par un point ne pas passer de droite du tout ou alors une infinité parallèles à une autre droite. Hilbert ne se doutait pas, que plus d’un siècle plus tard, Einstein montrera que notre univers suit les lois d’une géométrie non Euclidienne. De cette nouvelle géométrie découlent les lois de la relativité générale. Des lois dont la véracité est prouvée chaque jour par votre GPS. Si votre GPS ne tient pas compte de la courbure de l’espace caractéristique d”une géométrie non Euclidienne, il se trompera de plusieurs centaines de mètres. Les mathématiques auto-engendrent des concepts, des objets parfois sans objectifs pratiques. Pour reprendre l’analogie avec notre alpiniste, l’explorateur chemine, il découvre de nouveaux sommets, de nouveaux paysages d’un pays préexistant

à son voyage, sans savoir ce qu'il va découvrir. Il nomme les sommets au cours de son périple.

Congruence et arithmétique modulaire

Nous en avons fini avec les théorèmes les plus simples. Les théorèmes suivants vont introduire une notion importante dans la théorie des nombres premiers : l'arithmétique modulaire.

Afin de comprendre l'arithmétique modulaire, il faut utiliser des notions clés dans la théorie des ensembles : les notions de Groupe, Anneaux et Idéaux vus aux chapitres précédents.

Nous avons vu que l'ensemble des multiples d'un entier m muni de l'addition et de la multiplication est un anneau de Z.

Soit $a \in Z$ on note aZ *ou* $Z_a = \{a \times m, m \in Z\}$

Nous avons vu au chapître précédent que Z_a est un idéal de Z. Et même que tout idéal de Z est de la forme Z_a.

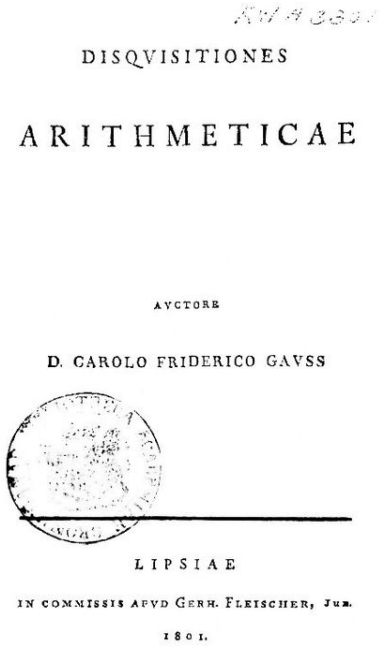
On dit que *b est* ***congru*** *à a modulo m,* que l'on note $a \equiv b$ *(mod m) , ou* $a \equiv b\,[m]$ ou plus simplement $a = b$ *(mod m)* si (*a - b) est un multiple de m.*

Exemple : 24 est congru à 3 modulo 7 car 24 - 3 = 21 = 3 x 7
57 est congru à 1 modulo 8 car 57 - 1 = 56 = 8 x 7.

On peut voir la congruence modulo m comme une horloge avec m heures. Prenons par exemple le cadran d'une montre avec les heures numérotées de 1 à 12. Si il est 17h, on peut aussi dire qu'il est 5h de l'après-midi car 17 est congru à 5 modulo 12 : 17 - 12 = 5.
Quand on parle d'un nombre n modulo m, il faut imaginer une horloge à m chiffres. On tourne l'aiguille de n positions, parfois il faut faire plusieurs tours et on regarde le chiffre indiqué par l'aiguille. L'arithmétique modulaire consiste à travailler sur les restes de la division euclidienne d'un nombre par un autre, plutôt que sur le nombre lui-même. Cette approche qui peut paraître déconcertante permet de travailler sur de très grands nombres. On en attribue la naissance à la publication du livre : "*Disquisitiones arithmeticae*" par Carl Friedrich Gauss en 1801. Toujours le même Carl Friedrich Gauss, le prince des mathématiciens !

Il y a de nombreuses approches du système modulaire dans l'antiquité. On a déjà cité le système sexagésimal

des Babyloniens qui a perduré dans les cadrans de nos montres. Aussi nous le verrons plus loin, dans le théorème des restes chinois, illustré par une question de Sun Zi écrit vers l'an 300 qui s'énonce ainsi « Soient des objets dont on ignore le nombre. En les comptant 3 par 3 il en reste 2, en les comptant 5 par 5, il en reste 3 et en les comptant 7 par 7, il en reste 2. Combien y a-t-il d'objets ? »


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

Revenons aux théorèmes.

On note $\overline{a}$ l'ensemble des entiers congrus à a modulo m. Chaque ensemble est représentée par un entier unique de {0…m-1}. On note $\frac{Z}{mZ}$ cet ensemble. par exemple $\frac{Z}{60Z}$ représente les 60 graduations d'une montre.

Si m et b sont des entiers naturels positifs tels que b > m et a ≡ b (mod m) alors a est le reste de la division euclidienne de b par m.

b est l'inverse de a modulo m si et seulement si ab $\equiv 1\ (mod\ m)$

SI p est premier, (pZ, +, x) est un corps commutatif: tout entier b a un inverse b' tel que b x b' $\equiv 1\ (mod\ p)$

Si p n'est pas premier; il existe des éléments de {2…p-1} qui n'ont pas d'inverse modulo p

On note parfois Z_m^* l'ensemble des entiers inversibles modulo m.

Cela fait beaucoup de nouveaux concepts et d'énoncés. En mathématique, il est parfois utile de faire une pause dans la théorie et d'illustrer les théorèmes et les concepts par des exemples simples.

Prenons le nombre premier 7. L'ensemble des entiers modulo 7 est

$\frac{Z}{7Z} = \{0, 1, 2, 3, 4, 5, 6\}$

Comme 7 est un nombre premier, montrons que $\frac{Z}{7Z}$ est un corps. Nous allons utiliser la méthode de la force brute en additionnant et en multipliant toutes les paires possibles de nombres dans cet ensemble. Le résultat tient dans deux tableaux avec les nombres de 0 à 6 en colonnes et en rangées.
La somme et le produit de i par j sont dans la rangée i et la colonne j.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Nous constatons que :

- l'addition est une loi de composition interne, chaque somme est dans $\frac{Z}{7Z}$
- L'élément neutre de l'addition est 0
- Chaque élément à un symétrique pour l'addition (les cases grisées)

L'addition est associative car elle est associative dans Z.

Donc($\frac{Z}{7Z}$,+) est un groupe.

Nous constations aussi que :

- la multiplication est une loi de composition interne, chaque produit est dans $\frac{Z}{7Z}$
- L'élément neutre est 1 pour la multiplication
- Chaque élément à un symétrique pour la multiplication

La multiplication est associative car elle est associative dans Z.

Donc($\frac{Z}{7Z}$,x) est un groupe.

Il suffit de constater que la multiplication est distributive sur l'addition car c'est le cas dans Z.

Et nous avons prouvé que ($\frac{Z}{7Z}$,+,x) est un corps !

Répétons le même exercice avec 12, comme les 12 heures de la journée. Nous constaterons que $(\frac{Z}{12Z}, +)$ est bien un groupe mais pas $(\frac{Z}{12Z}, \times)$. En effet dans le tableau de la multiplication il y a beaucoup de rangées donc de nombre qui n'ont pas de symétrique. Par exemple pour $x = 3$ on ne peut trouver y tel que $3 \times y = 1$.

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

x	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

Vous pouvez le constater avec votre montre si vous avez encore une montre à aiguille. Positionnez la grande aiguille sur le 3 (15 minutes), vous pourrez décaler l’aiguille de 3 graduations (ajouter 15 minutes) autant de fois que vous voulez, vous ne tomberez jamais sur la graduation 1 (5 minutes).

Fonction indicatrice d'Euler

$\varphi(m) = card(Z_m^*)$ que l'on peut noter $|(Z/mZ)^*|$.

On l'appelle l'ordre du groupe multiplicatif ,
C'est -à -dire le nombre d'entiers x entre 0 et m-1 compris inversibles modulo m.
Ce sont les entiers x, $0 \leq x < m$, qui sont premiers avec m.

Dans le tableau précédent pour n = 12, on voit que $\varphi(n) = 4$
En effet il n'y a que 4 nombres inversibles. 4 nombres dont la rangée contient 1 : 1, 5, 7, 11.
Ce sont les nombres qui sont premiers avec 12. C'est-a-dire les nombres qui n'ont pas de diviseurs communs avec 12 autre que 1.

Si n est premier alors $\varphi(n) = n-1$.

Ce qui est évident car si n est premier tous les nombres inférieurs à n sont premiers avec lui : ils n'ont pas de diviseurs communs car n n' a pas de divierseurs ! Donc $\varphi(n) = n-1$.
Par exemple $\varphi(13) = 12$

En général pour tout n

$$\varphi(n) = n \prod_{p|n}(1 - \frac{1}{p})$$

Illustrons cette formule barbare avec n = 14.

$\prod_{p|n}(1 - \frac{1}{p})$ indique que que l'on fait le produit $(1 - \frac{1}{p})$ pour tous les nombres p qui divisent 14. Quels sont-ils ? Il n'y a que 2 et 7

La formule devient donc :

$\varphi(14) = 14(1 - \frac{1}{2})(1 - \frac{1}{7})$

$\varphi(14) = 14(\frac{1}{2})(\frac{6}{7}) = 14 \times \frac{6}{14} = 6$

Ces nombres sont donc inversibles dans $\frac{Z}{14Z}$. Trouvons leurs inverses ou symétriques. Il faut donc trouver, par quel nombre il faut les multiplier, pour que le reste de la division par 14 donne 1 qui est l'élément neutre $\frac{Z}{14Z}$. Le théorème nous dit que seuls les nombres premiers avec 14 sont inversibles. Il faut donc considérer 1, 3, 5, 9, 11, 13. Car 2, 4, 6, 7, 8, 9, 10, 12 ont tous des diviseurs communs avec 14.

1 est l'inverse de 1 *car* $1 \times 1 = 1$

3 est l'inverse de 5 *car*
$5 \times 3 = 15\, et\, 15 \div 14 = 1 \times 14 + 1$
On en déduit que l'inverse de 5 est 3 car la multiplication est commutative *:* 5×3 **=** 3×5
9 est l'inverse de 11 *car*
$11 \times 9 = 99\, et\, 99 \div 14 = 7 \times 14 + 1$
On en déduit que 11 est l'inverse de 9.
13 est l'inverse de *13 car*
$13 \times 13 = 169\, et\, 169 \div 14 = 12 \times 14 + 1$
On a donc bien 6 nombres inversibles.

Théorèmes de la fonction d'Euler

$\forall n, m \in Z, n > 0, m > 0,$
- Si n et m sont premiers entre eux alors
$\varphi(nm) = \varphi(n)\varphi(m)$
$-\ \forall n \in N\ si\ \exists k \in N\ /\ n = p^k avec\ p\ premier$
$alors\ \varphi(n) = p^k(1 - \frac{1}{p})$

Le premier théorème permet de calculer les indicateurs de nouveaux nombres quand on connait leurs décompositions en facteurs premiers :

Par exemple :
$30 = 2 \times 3 \times 5$ donc
$\varphi(30) = \varphi(2) \times \varphi(3) \times \varphi(5) = 8$

Le deuxième théorème permet de calculer $\varphi(n)$ facilement pour les puissances de nombres premiers. Prenons par exemple

$81 = 3^4$ alors

$\varphi(81) = 3^4(1 - \frac{1}{3}) = 3^4 \times \frac{2}{3} = 3^3 \times 2 = 54$

Il y a donc 54 nombres inversibles modulo 81.

En général le calcul de la fonction indicatrice d'Euler est complexe et requiert une grande puissance de calcul informatique car elle nécessite de connaître la décomposition en facteurs premiers d'un nombre. Cette difficulté est utilisée en cryptologie.

Pour les lecteurs qui visent la médaille Fields, citons la conjecture de Derrick Henry Lehmer (1905-1991)

n est premier si et seulement si n ≡ 1 mod(φ(n))

Vous pouvez essayer de le démontrer ou de trouver un contre-exemple. Bon courage, personne n'a encore réussi !

Petit théorème de Fermat

Soit p un nombre premier

Forme 1 : $\forall n \in Z,\ n^p \equiv n\ (mod\ p)$

Forme 2 :

$\forall n \in Z,\ n\ non\ multiple\ de\ p,\ n^{p-1} \equiv 1\ (mod\ p)$

Forme 3 :

$\forall n \in Z,\ n\ non\ multiple\ de\ p,\ \exists k > 0\ /\ n^k \equiv 1\ (mod\ p)$

En outre le plus petit k vérifiant cette équation divise (p-1)

Pierre de Fermat a énoncé ce théorème pour la première fois dans une lettre à Bernard Frénicle de Bessy en 1640. Le texte de cette lettre permet d'apprécier la simplicité introduite par la notation littérale moderne des mathématiques. La lettre décrivait le théorème sous cette forme :

"Tout nombre premier mesure infailliblement une des puissances – 1 de quelque progression que ce soit, et l'exposant de ladite puissance est sous-multiple du nombre premier donné – 1 ; et, après qu'on a trouvé la première puissance qui satisfait à la question, toutes celles dont les exposants sont multiples de l'exposant de la première satisfont tout de même à la question."

L'écriture moderne est la forme 3 du théorème bien que le rapport entre les deux ne soit pas évident. Remercions encore une fois François Viète (1540-1603) et Albert Girard (1595-1632) pour l'introduction de la notation littérale. Même si cette dernière nécessite un certain apprentissage.

Bien sûr, Pierre de Fermat ne donne pas de démonstration ! Il faudra attendre 1683 pour que Leibniz en développe une, mais il ne la publie pas ! C'est finalement en 1750 soit un siècle plus tard que Euler publie une démonstration. Les mathématiciens étaient très cachotiers à l'époque !

Comme pour les autres théorèmes, on les comprend mieux en pratiquant. Etudions la première forme avec p = 7

7 est premier

Forme 1 : $\forall n \in Z,\ n^7 \equiv n\ (mod\ 7)$

Prenons n = 5

$5^7 = 78125$ et $78125 \div 7 = 11160 \times 7 + 5$

On retrouve bien 5 comme le reste de la division.

Forme 2 : $5^6 \equiv 1\ (mod\ 7)$

$5^6 = 15625$ et $15625 = 2232 \times 7 + 1$; on retrouve bien 1 comme le reste de la division.

Forme 3 : Cherchons le plus petit nombre k tel que
$5^k \equiv 1\ (mod\ 7)$
$5^6 = 15625, 5^5 = 3125,\ 5^4 = 625$
$5^3 = 125,\ 5^2 = 25,\ 5^1 = 5$
Calculons les restes de division par 7 pour obtenir les congruences modulo 7
$15625 \equiv 1,\ 3125 \equiv 3, 625 \equiv 2$
$125 \equiv 6,\ 25 \equiv 4, 2 \equiv 2$
Le plus petit nombre k tel que $5^k \equiv 1\ (mod\ 7)$ est 6 et 6 divise $7 - 1 = 6$. C'est magique !

Théorème d'Euler

$$\forall\, n \in N,\ \forall\, a \in N\ /\ a\ premier\ avec\ n,\ a^{\varphi(n)} \equiv 1\ (mod\ n)$$

Il permet la réduction modulo n de puissances. Par exemple, si l'on veut trouver le chiffre des unités de 7^{222}, c'est-à-dire trouver à quel nombre entre 0 et 9 est congru 7^{222} modulo 10, il suffit de voir que 7 et 10 sont premiers entre eux, et que $\varphi(10) = 4$. Le théorème d'Euler nous indique donc que

$7^4 \equiv 1\ (mod\ 10)$

On en déduit que

$7^{222} \equiv 7^{4x55+2} \equiv 7^{4^{55}} \times 7^2 \equiv 1^{55} \times 49 \equiv 9\ (mod\ 10)$

Le chiffre recherché est donc 9.

Théorème de Wilson

p est premier $\Leftrightarrow$ $(p-1)! + 1\ est\ un\ multiple\ de\ p.$

Exemples:

- Si *p* est égal à 5, alors (*p* – 1)! + 1 est égal à 25, un multiple de 5.
- Si *p* est égal à 6, alors (*p* – 1)! + 1 est égal à 121 qui n'est pas multiple de 6.
- Si *p* est égal à 17, alors (*p* – 1)! + 1 est égal à

20 922 789 888 001,

un multiple de 17 car

17 × 1 230 752 346 353 = 20 922 789 888 001.

Cette formule $a^{\varphi(n)} \equiv 1\ (mod\ n)$ est la seule formule connue qui permet, à coup sûr, d'identifier un nombre premier. Pas besoin d'essayer des tonnes de divisions ! Il "suffit" de calculer $(p-1)! + 1$ et de le diviser par p. Si le reste est 0 alors p est premier. Malheureusement cette méthode

présente peu d'intérêt car pour un grand nombre, (p-1)! devient vite incalculable. La méthode des divisions par tous les nombres qui le précédent est plus efficace, retour à la case départ !

Par exemple pour 37, nous obtenons 36!+1 =
371993326789901217467999448150835200000001
Il faut ensuite le diviser par 37 pour constater que le reste est nul et que c'est donc un multiple de 37. Un bien long calcul avec un grand nombre de chiffres alors que la méthode de base du crible d'Eratosthène nous renseignera beaucoup plus vite, avec moins de puissance de calcul, que 37 est premier. Dommage !

Formule de Legendre

On appelle valuation p-adique d'un nombre n étant donné un nombre premier p, le plus grand nombre x tel que p^x divise n.
C'est aussi l'exposant de p dans la décomposition en facteurs premiers de n.

Par exemple

$v_{11}(2662) = 3$ car $2662 = 11^3 \times 2$

$v_5(2000) = 3\ car\ 2000 = 2^4 \times 5^3$, $v_7(30) = 0$

Si vous cherchez “Formule de Legendre” sur Wikipédia, vous verrez une définition assez cryptique :

“*En théorie des nombres, la formule de Legendre donne une expression, pour tout nombre premier p et tout entier naturel n, de la valuation p-adique de la factorielle de n qui se note* $v_p(n!)$.”

Dans notre vocabulaire, c’est l’exposant de p dans la décomposition en facteurs premiers de la factorielle de n : n!, ou encore le plus grand entier v tel que p^v divise n!

Legendre (1752-1833) montre que

$$v_p(n!) = E(\frac{n}{p}) + E(\frac{n}{p^2}) + E(\frac{n}{p^3}) + \ldots = \sum_{k=1}^{\infty} E(\frac{n}{p^k})$$

E(x) désigne la partie entière (les chiffres avant la virgule dans le développement décimal) d’un nombre x.
Par exemple :

$E(4,672) = 4,\ E(\frac{10}{3}) = E(3,333.....) = 3,\ E(\pi) = 3$

Ce qui permet de définir par récurrence $v_p(n!)$

$$v_p(n!) = E(\frac{n}{p}) + v_p(E(\frac{n}{p})!)$$

On peut étendre la définition de la valuation p-adique au cas où p n'est pas premier et sans introduire de factorielle.

$v_p(n) = x \Leftrightarrow (si\ \exists y \in N / p^y$ divise n alors $y \leq x)$

C'est toujours le plus grand nombre x tel que p^x divise n

Théorème des restes Chinois

Soient $m_1 \ldots m_r$ des nombres premiers entre eux deux à deux et soit m leur produit. Pour toute suite $x_1 \ldots . x_r$ d'entiers donnés,
$\exists!\ x,\ 0 < x < m - 1\ /\ \forall i \in \{1..r\},\ x \equiv x_i (mod\ m_i)$

En utilisant les congruences, le théorème donne la solution x:

Solution :

$Soient\ m_1, \ldots, m_n \in N\ /\ \forall i \in [1,n],\ \forall j \in [1,n],$
$m_i > 2\ et\ m_j > 2\ et\ m_i, m_j\ premiers\ entre\ eux$
$Soient\ a_1, \ldots a_n \in N$
Le système d'équations :

$x \equiv a_1[m_1]$

…..

$x \equiv a_n[m_n]$

admet une solution unique x modulo $M = m_1 \times \ldots \times m_n$

$x = a_1 M_1 y_1 + \ldots + a_n M_n y_n$ avec $M_i = \frac{M}{m_i}$ et $y_i \equiv M_i^{-1}[m_i]$

pour i entre 1 et n.

Exemple :

Prenons les nombres 17,11 et 6. Ils sont premiers entre eux deux à deux car 17 et 11 sont premiers.

Prenons la suite d'entiers 3, 4 et 5.

Le théorème nous dit qu'il existe un nombre entier x unique tel que

$x \equiv 3\,[17],\ x \equiv 4\,[11], x \equiv 5\,[6]$

Comment calculer x en appliquant la solution détaillée précedemment :

On calcule

$M = 17 \times 11 \times 6 = 1122$

$M_1 = 1122/17 = 66, M_2 = 1122/11 = 102, M_3 = 1122/6 = 187$

On calcule l'inverse de chaque M_i modulo m_i par l'algorithme d'Euclide, ce qui nous donne :

$y_1 = 8, y_2 = 4,\ y_3 = 1$

On peut maintenant calculer x

$3 \times 66 \times 8 + 4 \times 102 \times 4 + 5 \times 187 \times 1 = 1584 + 1632 + 935 = 4151 = 785\, mod(1122)$

Donc x= 785

A quoi sert ce théorème ?

Si on regarde sur google :
"*Le théorème des restes Chinois permet de résoudre explicitement tout système de congruences dans l'anneau euclidien R = K[X] des polynômes sur un corps K, c'est-à-dire tout système de la forme. où les données sont des polynômes Ri deux à deux premiers entre eux et des polynômes Ai, et l'inconnue est le polynôme P.*"

Nous voila bien avancés ! Plus pratiquement il permet de répondre aux questions du type :

"Il y a certaines choses dont le nombre est inconnu. Si on les compte par 3, il en reste 2; par 5, il en reste 3; par 7, il en reste 2. Combien y-a-t-il de ces choses?"

Plus clair mais pas toujours plus utile dans la vie de tous les jours. C'est la beauté de l'arithmétique, cela ne sert souvent à rien dans la vie quotidienne ou même pour les physiciens, mais les mathématiciens se sont intéressés à ces problèmes pendant des siècles. En effet la question a été posée par le mathématicien chinois Sun-Zi entre le IIIème siècle et le IVème siècle après J.-C. Il a donné la réponse : 23. Mais sans bien sûr divulguer sa méthode. Il a fallu attendre Gauss pour généraliser le problème et expliquer la solution dans son ouvrage de 1801 que vous

connaissez bien maintenant : “Disquisitiones Arithmeticae”.

Nous connaissons maintenant les théorèmes principaux, nous pouvons aborder une question qui interroge toujours les mathématiciens : la répartition des nombres premiers. Que savons nous sur ce sujet :

1. Il y en a une infinité.
2. Il n’y a pas de formule permettant de connaître le nombre premier qui suit un nombre premier donné.
3. Mais il semble qu’ils ne sont pas répartis de manière totalement aléatoire.

Y'a t’il un ordre derrière ce chaos apparent ? Une musique dont les nombres premiers formeraient la mélodie ? C’est ce que nous allons voir dans le chapitre suivant.

Répartition des nombres premiers

On a vu qu'il y a une infinité de nombres premiers. On se doute qu'ils se raréfient au fur et à mesure que l'on progresse vers de plus grands nombres. Mais à quelle vitesse ? Comment savoir si il y a un nombre premier entre 2 nombres ? Y a t'il une formule qui génère des nombres premiers ?...
Ce sont encore des sujets de beaucoup de recherches.

Densité des nombres premiers

Soit D un sous ensemble de N. La densité des éléments de D inférieurs à m est

$$d_{D(m)} = \frac{|\{x \in D / x < m\}|}{m}$$

Ainsi si D est l'ensemble des nombres pairs : {0, 2, 4, …..}

$$d_{D(10)} = \frac{|\{0,2,4,6,8\}|}{10} = \frac{5}{10} = \frac{1}{2}$$

La densité est liée à la probabilité de choisir au hasard un nombre de l'ensemble D parmi les nombres inférieurs à m. Si vous citez au hasard un nombre entre 0 et 9, il y a une chance sur deux qu'il soit pair.

Si D est la face correspondant à un nombre impair d'un dé.
D = {1,3,5} alors
$d_{D(4)} = \frac{|\{1,3\}|}{6} = \frac{2}{6} = \frac{1}{3}$

Lorsque l'on lance un dé, il y a une chance sur trois de tomber sur un nombre impair inférieur à 4 : 1 et 3.
Nous reviendrons sur cette notion de probabilité que Gauss a exploitée quand il a voulu estimer la densité des nombres premiers inférieurs à un nombre donné.

Gauss, par souci de concision pour un concept qu'il a beaucoup manipulé, a choisi un symbole pour noter le nombre de nombres premiers inférieurs à un nombre donné. Malencontreusement il a choisi π . Ce qui introduit parfois une confusion avec le nombre π utilisé pour calculer le périmètre d'un cercle. On peut s'appeler Gauss et faire de mauvais choix !

On note $\pi(m) = |\{x \in P / x < m\}|$, le nombre de nombres premiers inférieurs à m.

Théorème de raréfaction de Legendre

La densité limite de P ensemble des nombres premiers tend vers 0.

$$d_{P(m)} = \frac{\pi(m)}{m} \to 0 \; quand \; m \to \infty$$

Que veut dire ce théorème ?

Il énonce une vérité qui peut nous sembler évidente. Bien qu'il existe une infinité de nombres premiers, ceux-ci deviennent de plus en plus rares au fur et à mesure que l'on progresse vers l'infini. Pourquoi cela semble t'il évident ? En effet, plus un nombre est grand, plus il existe de diviseurs potentiels ! C'est un bon exemple d'intuition. La démonstration n'est pas si simple.

Notons que cela ne nous renseigne pas sur leur répartition. La densité tend vers 0, mais les nombres peuvent apparaître en groupes, comme par exemple les nombres premiers jumeaux (2 nombres premiers impairs qui se suivent comme 1667 et 1669) et ensuite disparaître pendant une longue série d'entiers qui se suivent mais ne sont pas premiers. C'est cet aspect

chaotique et aléatoire qui intrigue les mathématiciens cherchant de l'ordre dans un désordre apparent.

Théorème de raréfaction d'Euler

Beaucoup d'ensembles infinis ont une densité limite nulle mais certains sont plus "grands" que d'autres.

On parle de "grand infini" quand la somme des inverses des éléments de l'ensemble tend vers l'infini.

La somme des inverses des nombres premiers tend vers l'infini

$$\sum_{p\ premier} \frac{1}{p} = +\infty$$

L'ensemble des nombres premiers est non seulement infini mais c'est un grand infini !

Pour étudier la répartition des nombres premiers, il nous faut introduire une nouvelle fonction : la fonction zêta qui se note ς.

Théorème d'Euler, Produit Eulérien

On note

zêta(k) = ς(k) =

$$1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \frac{1}{5^k} + \frac{1}{6^k} + etc$$

La somme de tous les inverses des nombres entiers élevés à la puissance k.

Exemple :

$$\varsigma(2) = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \ldots.$$

Etrangement cette série converge vers $\frac{\pi^2}{6}$. Etrangement car que vient faire π (le π du cercle, pas celui de la densité) dans cette galère. En effet nous additionnons des inverses de carrés de nombres entiers et nous finissons pas converger vers un nombre réel. De plus, c'est un nombre réel transcendant : un nombre qui n'est pas la solution d'un polynôme à coefficients rationnels . Euler a été le premier à trouver cette égalité pourtant la série converge lentement. Il faut 15000 additions pour trouver 4 décimales exactes de $\frac{\pi^2}{6}$. La première démonstration d'Euler en 1735 manque de rigueur, il

applique des règles de factorisation à une somme infinie, ce qui à l'époque n'était pas admis. En 1741, il apporte une démonstration plus rigoureuse basée sur une innovation mathématique importante due au mathématicien Français Taylor (1685-1731) qui permet d'approximer une fonction en un point à l'aide d'une somme infinie. La fonction en question est la fonction **sinus** qui intervient en géométrie et dans les mesures d'angles. On comprend mieux ainsi comment $\frac{\pi^2}{6}$ se glisse dans une somme infinie ne faisant intervenir que des nombres entiers.

Donc $\varsigma(2) = \frac{\pi^2}{6}$

Alors que $\varsigma(1)$ ne converge pas, la somme des inverses des nombres entiers tend vers l'infini.

$\varsigma(1) = 1 + \frac{1}{2} + \frac{1}{3} + \ldots. = + \infty,$

Au delà de 2 la somme converge. Par exemple

$\varsigma(4) = \frac{\pi^4}{90}$

Euler va établir un lien entre la somme des inverses des puissances des nombres entiers élevés à une puissance supérieure ou égale à 2 et les nombres premiers en utilisant le crible d'Eratosthène. Il montre que

$$\sum_{n=1}^{\infty} \frac{1}{n^k} = \prod_{p \in P} \left(\frac{p^k}{p^k - 1}\right) = \varsigma(k)$$

Alors la ! Chapeau, respect ! Regardez de plus près cette formule. Elle est étonnante, stupéfiante ! La somme des inverses de tous les nombres entiers élevés à la puissance k, converge vers un produit incluant tous les nombres premiers élevés à la puissance k. On ne connaît pas tous les nombres premiers mais on est capable d'énoncer une formule incluant la somme de leurs puissances !

Cette formule, qui n'est valable que pour k > 1, quand la suite $\sum_{n=1}^{\infty} \frac{1}{n^k}$ converge, va être utilisée pour approximer $\pi(m)$. C'est la clé de la boîte de Pandore qui consiste à estimer le nombre de nombres premiers inférieurs à un nombre donné. Cette boite n'est toujours pas refermée. Elle donnera naissance au fameux problème des "zéros non triviaux de la fonction zêta de Riemann". Une conjecture toujours non démontrée. Nous allons l'aborder dans les pages qui suivent.

Théorème de raréfaction de Hadamard et de la Vallée Poussin

Introduisons un nouveau signe qui veut dire “peu différent” : ≃

Par exemple : 10258672459 ≃ 10258672458.

En 1792 après un examen de la liste des nombres premiers et de la table des logarithmes qu’il chérissait, Gauss, alors âgé de 16 ans, conjecture que la densité des nombres premiers inférieurs à m est environ $\frac{1}{ln(m)}$. Adrien-Marie Legendre (1752-1833) fait la même hypothèse. Voyons ce que cela implique pour le nombre de nombres premiers inférieurs à m.

$d(m) = \pi(m)/m$. On en déduit que $\pi(m) = m \times d(m)$. En remplaçant $d(m)$ par $\frac{1}{ln(m)}$ et en introduisant la notion de “peu différent”. On obtient :

$$\pi(m) \simeq \frac{m}{ln(m)}.$$

La densité des nombres premiers inférieurs à un nombre m est peu différente de m divisé par le logarithme

népérien de m. Gauss montre que non seulement $\pi(m)$ est peu différent de $\frac{m}{ln(m)}$ mais qu'il est toujours inférieur. Gauss propose ensuite d'utiliser le logarithme intégrale (voir en annexe une définition simplifiée de la notion d'intégrale).

$li(m) = \int_0^m \frac{dt}{ln(t)}$ qui donne une meilleure approximation

On constate que la fonction d'écart Li(x) donne encore une meilleurs approximation.

$Li(x) = li(x) - li(2) = \int_2^m \frac{dt}{ln(t)}$

En 1896 Hadamard et de la Vallée Poussin démontrent que

$\pi(m)$ tend asymptotiquement vers $\frac{m}{ln(m)}$.

Que veut dire l'expression "tend asymptotiquement" ? Simplement que la différence devient de plus en plus faible au fur et à mesure que le nombre m devient plus grand.

$$\frac{\pi(m)}{m/ln(m)} \to 1 \; quand \; m \to \infty$$

Dans le domaine de la physique, cette approximation aurait sans doute suffi à énoncer une loi physique, tirée de l'expérience, montrant que le nombre de nombres premiers inférieurs à m est Li(m). La différence aurait pu être attribuée à l'imprécision des mesures. On aurait ensuite cherché une explication. En l'absence de celle-ci, on aurait sans doute conclu que c'est une constante de l'univers mathématique, comme la vitesse de la lumière est une constante de l'univers physique. L'approche mathématique est différente. On se demande "pourquoi ?" alors que les physiciens se concentrent sur "comment ?". Les mathématiciens veulent trouver un raisonnement logique partant des axiomes de l'arithmétique et ayant pour conclusion une formule donnant l'écart entre la valeur de la densité des nombres premiers et Li(m). La seule démonstration est celle de Hadamard et de la Vallée Poussin qui ont démontré que cet écart tend vers 0 quand le nombre m tend vers l'infini.

Les physiciens sont intéressés par des lois qui permettent d'approcher le résultat de leurs prochaines expériences. Savoir que deux masses s'attirent et connaître une bonne approximation de la force d'attraction suffit. C'est le "comment". Le "pourquoi" serait de savoir "Pourquoi deux masses s'attirent ?". Einstein y répond en montrant que les masses courbent l'univers. Cela permet simplement d'affiner la précision de la formule mais on ne sait pas "Pourquoi une masse déforme l'univers ?". Le pourquoi en physique amène à

des questions philosophiques ou religieuses. En Mathématique, il est le début de la quête d'une démonstration.

Gauss a souhaité se concentrer sur le pourquoi ainsi que Legendre mais malheureusement leurs recherches ont été interrompues par manque de financement.. Les deux mathématiciens ont dû réorienter leurs travaux vers des problèmes moins théoriques et plus pratiques. Gauss vers l'astronomie en acceptant le poste de Directeur du nouvel observatoire de Gottingen en 1807 après l'assassinat par Napoléon du Duc Ferdinand, qui était son mécène, et Legendre vers des sujets plus applicables à la guerre et l'industrie sur la demande du même Napoléon qui avait créé l'Ecole Polytechnique et l'Ecole Normale Supérieure dans ce but. Il faudra attendre Riemann qui prit la succession de Gauss pour voir les travaux sur l'estimation de $\pi(m)$ progresser de nouveau.

Depuis les mathématiciens cherchent toujours à affiner l'estimation de $\pi(m)$.
Par exemple le Russe Pafnouti Tchebychev (1821-1894) a établi en 1851 : π(x) est compris entre $0,92129 \times \frac{x}{ln(x)}$ et $1,10556 \times \frac{x}{ln(x)}$. Il est étrange de voir des constantes apparaître ainsi dans des théorèmes mathématiques.

Cet encadrement a été amélioré avec la fonction de Riemann R(m)

$$R(m) = \sum_{n=1}^{m} \frac{\mu(n)}{n} li(m^{\frac{1}{n}})$$

avec $\mu(1) = 1$, $\mu(n) = (-1)^k tincts$

$\mu(n) = (-1)^k$ quand n est le produit de k nombres premiers distincts et $\mu(n) = 0$ quand n est divisible par un carré.

Voyons sur quelques exemples, le degré de précision donné par ces différentes approximation :

Prenons $m = 10^8$. C'est à dire 100 millions. Il y a 5761455 nombres premiers inférieurs à 100 millions. La formule $\frac{m}{log(m)}$ estime qu'il y a en a 332744 de moins. La formule $li(m)$ en estime 754 de plus et la formule $R(m)$ 97 de plus. $R(m)$ est donc précis à 0,029 % près.

Faisons un grand bond dans l'ensemble des entiers naturels et considérons $m = 10^{12}$, ce qui représente 100 milliards. Il y a 4 118 054 813, un peu plus de 4 milliards, de nombres premiers, inférieurs à m. $\frac{m}{log(m)}$ estime qu'il y en a 189 923 160 (presque 200 millions) de moins, la formule $li(m)$, 3104 en plus et $R(m)$ 79 en plus. $R(m)$ est donc précis à 0,000002 % près ! Pas mal, mais pas parfait, on ne connait pas de formule exacte. Si on avait

une formule exacte, elle nous donnerait aussi une méthode pour déterminer si un nombre est premier. En effet connaissant exactement le nombre de nombres premiers inférieurs à un nombre m : $\pi(m)$, il suffirait d'appliquer la formule pour savoir si $m + 2$ est premier. Si $\pi(m) = \pi(m + 2)$ alors $m + 2$ n'est pas premier, il l'est dans le cas contraire !

Avec l'apparition des ordinateurs et la possibilité de calculer tous les nombres premiers jusqu'à des milliards de milliards, les mathématiciens avaient hâtivement conclu en observant les résultats que li(m) était une bonne approximation de $\pi(m)$ et que $li(m) < \pi(m)$.

Le mathématicien anglais John Littlewood (1885-1977) a démontré, dès 1914, qu'il y a des nombres pour lesquels cette inégalité est inversée $li(m) > \pi(m)$. En 2024 même les ordinateurs les plus puissants n'ont pu trouver un seul nombre satisfaisant à cette condition. On sait que ces nombres existent mais ils sont supérieurs aux nombres que l'on peut manipuler avec les ordinateurs actuels ! Cela montre que la méthode expérimentale ne permet pas d'établir des théorèmes, les mathématiciens ont besoin de preuves suivant un raisonnement logique !

Nous verrons dans le chapître suivant, une hypothèse conjecturée par Riemann qui affine cette approximation. Cette hypothèse, bien sûr appelée "hypothèse de Riemann" n'a toujours pas été démontrée. Les meilleurs mathématiciens du monde ont essayé pendant plus de deux siècles. Un prix de un million de dollars à été

financé pour celui qui la démontre. Helge von Koch (1870-1924) en 1901 a montré que si cette hypothèse est vraie, c'est à dire si on trouve une démonstration, l'estimation la plus proche sera alors de

$$\pi(x) = li(x) + E \; avec \; E = O(xln(x))$$

Dans cette formule E est l'écart entre $\pi(x)$ et $li(x)$.
$O(xln(x))$ veut dire que plus x est grand plus la valeur de $xln(x)$ devient prépondérante devant l'écart.

Parlons donc maintenant de cette fameuse hypothèse de Riemann, tellement vitale pour les mathématiciens travaillant dans le domaine des nombres premiers que Hilbert (1862-1943) inclut cette hypothèse en 1900 dans la liste des 23 problèmes non résolus et les plus importants à résoudre avant la fin du siècle. C'est le 8ème problème, groupé avec la conjecture de Goldbach et l'infinité des nombres premiers jumeaux. Hilbert aurait dit « *Si je devais me réveiller après avoir dormi pendant mille ans, ma première question serait : l'hypothèse de Riemann a-t-elle été prouvée* ? »
L'institut Clay, fondé par un milliardaire de Boston en 1998, a financé un prix de un million de dollars pour chaque mathématicien qui résout un des problèmes de Hilbert encore non résolu. Seule la moitié de ces problèmes a été résolue. Ils sont cités dans un article de wikipédia [7].

Lors d'une traversée agitée en bateau de Scandinavie au Royaume-Uni, Hardy, mathématicien anglais, dont nous avons déjà parlé, expédia une carte postale à un

collègue pour lui annoncer qu'il avait démontré l'hypothèse de Riemann. Il pensait ainsi que Dieu, qu'il tenait pour son ennemi intime (bien qu'il soit athé, Hardy pas Dieu !), n'allait pas le laisser mourir et ainsi faire croire à la communauté mathématique qu'il avait démontré une importante conjecture de la théorie des nombres premiers. [8]

Fonction Zêta de Riemann

La fonction zêta d'un nombre k que nous avons pu précédemment a été définie par Riemann..

$$\text{zeta(k)} = \varsigma(k) = 1 + \frac{1}{2^k} + \frac{1}{3^k} + \frac{1}{4^k} + \frac{1}{5^k} + \frac{1}{6^k} + \ldots$$

On a vu que Euler a démontré que

$$\sum_{n=1}^{\infty} \frac{1}{n^k} = \prod_{p \in P} \left(\frac{p^k}{p^k - 1}\right) = \varsigma(k)$$

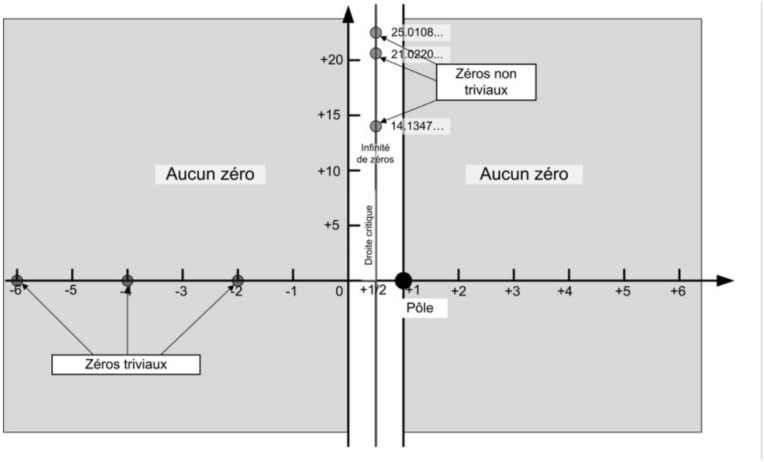
La fonction Zêta n'est définie que pour k > 1 pour k = 1 elle diverge.

L'idée géniale de Riemann a été d'étendre la fonction aux nombres complexes :

$$\varsigma(s) = \frac{1}{1-2^{1-s}} \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n^s}$$

Dans ce contexte “étendre” veut dire que si s est un nombre entier naturel, on retrouve bien la fonction zêta(s) définie plus haut mais que cette fonction garde un sens pour toute valeur de s < 1 et même pour s complexe avec une partie réelle positive : $a + ib$ avec $a > 0$.

La fonction ainsi écrite possède des zéros triviaux -2, -4, -6,...
On appelle zéro d’une fonction f(x) les valeurs de x qui annulent la fonction : $x\ tel\ que\ f(x) = 0$
Ils sont appelés zéros triviaux car une démonstration trop complexe pour cet ouvrage montre que la fonction s'annule pour tous les entiers de la forme -2n.
Cette fonction a aussi des zéros non triviaux pour lesquels on n’a pas trouvé de formule. Ces zéros ont été découverts empiriquement et jusqu’ici on constate qu’ils ont tous pour valeur réelle $a = \frac{1}{2}$. Ils sont de la forme $\frac{1}{2} + yi$. Si on les représente sur un plan muni d’un repère (0,1),(0,i), ils sont sur la droite verticale d’abscisse $x = \frac{1}{2}$.



Riemann conjectura que tous les zéros non triviaux sont sur la droite $x = \frac{1}{2}$

Cette conjecture n'a jamais été démontrée.

La distribution des zéros non triviaux joue un rôle important dans la répartition des nombres premiers. En effet on définit la fonction Gamma par

$$\Gamma(s) = \int_0^\infty e^{-u} u^{s-1} du$$

La fonction Gamma étend la fonction factorielle aux nombres complexes : $\Gamma(n) = n!$ quand $n \in \aleph$

Elle est liée avec la fonction Zêta aux nombres d'entiers premiers inférieurs à m : $\Pi(m)$ par l'identité fondamentale:

$$\Pi(m) = R(m) - \sum R(m^{\theta})$$

ou les valeurs de θ sont les zéros non triviaux de la fonction Zêta.

Cette identité montre que $\Pi(m)$ est bien approché par

$R(m)$ avec la fonction correctrice $\sum R(m^{\theta})$.

Il est donc important de connaître les zéros de la fonction Zêta pour mieux approcher la valeur de $\Pi(m)$. Malheureusement on ne peut connaître ces zéros que de manière empirique. Les valeurs de ces zéros trouvées jusqu'à nos jours (2025) sont toutes sur la droite x=½ en accord avec la conjecture de Riemann.
Les mathématiciens ont démontré qu'ils sont tous situés dans la bande 0 < x < 1 et sont symétriques par rapport à la droite x=½, mais pas qu'ils étaient situés exactement sur cette droite.

En fait on a transformé un problème non résolu : trouver une formule donnant le nombre de nombres premiers inférieurs à un nombre m par un problème encore plus complexe : prouver que toutes les valeurs non triviales qui annulent la fonction zêta(x) sont situées sur l'axe

$x = \frac{1}{2}$. Ce problème n'a pas été résolu non plus, mais les mathématiciens ont pu développer des théories basées sur le fait que l'hypothèse de Riemann était vraie. Mais tant que cela n'a pas été démontré, on n'est pas beaucoup plus avancé !

Cette approche ne satisfait pas au principe du rasoir d'Occam. Le principe du rasoir d'Occam est un principe philosophique qui prêche la simplicité. C'est au raisonnement ce que la sobriété est au bonheur selon Pierre Rabhi [9]. Pour ceux qui se demandent : "Quel est le rapport avec le rasoir du barbier", il n'y en a pas ! En philosophie, le terme « rasoir » désigne un principe ou une règle générale qui permet de réduire (de « raser ») le nombre d'explications d'un phénomène.
Pierre Occam ou Ockham était un philosophe, théologien et logicien anglais, né en 1285 et mort en 1347. Il prônait que « L'explication la plus simple est généralement la bonne ». Il fût jugé hérétique par l'Église car il prétendait qu'il était impossible de prouver l'existence de Dieu. Les mathématiciens ont donc remplacé un problème difficile par un problème qui semble encore plus complexe. Est ce que le 21eme siècle à défaut de voir prouver l'existence de Dieu, verra la preuve de l'hypothèse de Riemann !

De la densité des nombres premiers on peut passer à l'écart entre les nombres premiers.

L’écart entre les nombres premiers

Postulat de Bertrand

En 1845 Joseph Bertrand (1822-1900) énonce la conjecture suivante :

Pour tout entier n supérieur à 2, il existe un nombre premier entre n et 2n.
$\forall n \in N / n \geq 2, \exists\, p\, premier / \, n < \ p \ < \ 2 \times n$

Par exemple, entre 15 et 30, il y a le nombre 23 ainsi que d’autres (17,...)..
Entre 1500000 et 3000000, il y a 1502323 (et des milliers d’autres).

La conjecture fut complètement démontrée en 1850 par Pafnouti Tchebychev. On étudiera dans ce livre la démonstration “plus simple” donnée par Paul Erdos en 1932. Ce sera l’Everest de cette exploration dans le continent des nombres premiers !

Nombres premiers jumeaux

Parfois l'écart entre 2 nombres premiers vaut 2 : 3 et 5, 5 et 7, 11 et 13 ….De tels nombres premiers sont qualifiés de **jumeaux.**

En 2025 il n'existe pas de preuve qu'il existe une infinité de nombres premiers jumeaux. La plus grande paire connue est

$361700055\ x\ 2^{39020} - 1\ et\ 361700055\ x\ 2^{39020} + 1$

Des nombres de 11755 chiffres!

Anecdote: Brun a prouvé que la somme des inverses des nombres premiers jumeaux est convergente

$B = (\frac{1}{3} + \frac{1}{5}) + (\frac{1}{5} + \frac{1}{7}) + \ldots = 1,902160577783278\ldots.$

C'est en voulant calculer les nombres premiers jumeaux inférieurs à 10^{15} en 1994 que Thomas Nicely, professeur à l"université de Lynchburg, a trouvé un bug dans le processeur Pentium d'Intel. Ce bug était situé dans l'algorithme de division implémenté dans le circuit. Après avoir nié l'importance du bug, Intel a corrigé les nouvelles versions du Pentium. Une application inattendue des recherches sur les nombres premiers !

Écart Maximum ?

On peut trouver des écarts aussi grands que l'on veut entre 2 nombres premiers.

En effet, tous les nombres entre (n! + 2) et (n! + n) sont composés : pour 1 < k < n+1, on peut écrire

$n! + k = k \times (\frac{n!}{k} + 1)$

$\frac{n!}{k}$ est un nombre entier car k est inférieur à n+1 donc compris dans les facteurs de n!.

Rappelez vous :

$n! = 1 \times 2 \times 3 \times \ldots k \times \ldots n$. En choisissant n, aussi grand que l'on veut, des milliards de milliards, on peut ainsi définir un intervalle de nombres dans lequel il n'y a pas de nombre premier.

Par contre, il est difficile de savoir pour quelle valeur un écart donné apparaît pour la première fois ! Quel est le premier nombre premier p pour lequel le nombre premier suivant est situé entre p et p + 7251952 ?

On peut s'intéresser à des "formes" spécifiant l'écart possible entre des nombres premiers.

Par exemple : 3 nombres premiers consécutifs ne peuvent être de la forme p+2, p+4 et p+6 car il y a toujours un multiple de 3 dans une telle suite (voir chapître démonstration).

Par contre :

p, p+2 et p+6 ou p, p+4 et p+6 sont possibles.
On appelle des constellations des suites de nombres premiers correspondant à une forme donnée.

Anecdote : On a démontré que les 2 conjectures de Hardy et Littlewood sont incompatibles :
1. Quelque soit la forme possible, il y a une infinité de constellations.
2. Conjecture de décroissance des densités : Pour toute longueur d'intervalle L et pour tout entier k : le nombre de nombres premiers entre 2 et L est supérieur au nombre de nombres premiers entre k+2 et k + L.

On ne sait pas démontrer ces conjectures mais on sait que si l'une est vraie, l'autre est fausse !

Primalité, Factorisation

Test de primalité

Démontrer qu'un grand nombre est premier peut demander beaucoup de temps de calcul, énormément de temps de calcul, plus de temps de calcul que celui disponible sur terre en 2025 ! En effet il n'y a pas d'algorithme simple, permettant de tester la primalité d'un nombre. Il existe des astuces et des moyens d'accélérer l'algorithme de base mais on en revient toujours, plus ou moins, à essayer de diviser ce nombre par tous les nombres qui le précèdent..

Par contre on peut démontrer avec moins d'efforts de calculs que certains nombres ne sont pas premiers. On peut utiliser pour cela la forme 2 du théorème de Fermat.

$$p\ est\ premier\ \Rightarrow \forall\ n\ non\ multiple\ de\ p,\ \ n^{p-1} \equiv 1\ (mod\ p)$$

Par conséquent si pour un entier n on trouve un entier a tel que 2 < a < n et que $a^{n-1} \neq 1(mod\ n)$ alors on peut en déduire que n n'est pas premier. Il est composé. Ce test est appelé test de primalité de Fermat.

Prenons par exemple p = 15 et n = 2,

$2^{15-1} = 2^8 \times 2^4 \times 2^2 = 16^2 \times 16 \times 4$

$= 16^3 \times 4 = 1\ (mod\ 15) \times 4 = 4\ (mod\ 15)$

Donc 15 n'est pas premier.

Ce test est très utile pour les grands nombres en utilisant l'exponentiation modulaire (voir en annexe).

Par exemple on montre que

$2^{111111111111} = 1015669396877\ (mod\ 1111111111111)$

donc que 111111111111 n'est pas premier.

Si il est facile avec le théorème de Fermat de prouver qu'un nombre est composé, on pourrait penser qu'il suffit d'utiliser la même méthode pour prouver qu'il n'est pas composé donc premier.

Malheureusement la condition de la forme 2 du théorème de Fermat est nécessaire mais pas suffisante.

$\forall\ n\ non\ multiple\ de\ p,\ n^{p-1} \equiv 1\ (mod\ p)$ n'implique pas que n est premier.

On peut donc trouver des nombres n pour lesquels :

$n\ non\ multiple\ de\ p\ \ et\ \ n^{p-1} \equiv 1\ (mod\ p)$ sans que p soit premier. On appelle ces nombres des nombres 2-pseudo-premiers.

On a vu que la principale application pratique des nombres premiers est la cryptologie. Ces nombres 2-pseudo-premiers ne sont-ils pas suffisamment “bons” pour cette application ?

Les nombres 2-pseudo-premiers sont-ils fréquents ?

Il y a 1091987405 nombres premiers inférieurs à 25 milliards mais seulement 21853 nombres 2-pseudo-premiers. On peut donc calculer la probabilité qu’un nombre inférieur à 25 milliards tiré au hasard soit premier ou 2-pseudo-premiers.
La probabilité qu’il soit premier est de 4,36794962% donc la probabilité qu’il ne soit pas premier est de 95,63205038%.

Donc si on choisit n au hasard tel que n soit inférieur à 25 milliards et que l’on calcule 2^{n-1} (mod n). Il y a 2 possibilités :

1. Le résultat est différent de 1 dans 95,63205038% des cas et on a prouvé qu’il est composé.
2. Le résultat a égale à 1 dans $\frac{1091987405+21853}{25000000000} = 4,36\%$ des cas.
   Mais on n'a pas prouvé qu’il est premier. Il peut être pseudo-premier dans 21853 cas et premier dans 1091987405 cas. Il est donc premier dans $\frac{21853}{1091987405} = 99,998\%$ des cas.

Donc si dans un excès d'enthousiasme, on déclare qu'un nombre 2-pseudo-premier est premier, il y a peu de chance que l'on se trompe : 0,002%.

Plus n est grand, plus le risque d'erreur diminue. On l'a vu plus haut, une erreur peut aussi être due à un bug du programme ou à un défaut du circuit (cf Pentium).
De plus, les mathématiciens ont démontré que si n est 2-pseudo-premier alors 2n-1 l'est aussi. Il y a donc une infinité de nombres 2-pseudo-premiers.

On définit donc ainsi le test **probabiliste** de primalité de Fermat:

Choisir des nombre a au hasard 2 < a < n-1, si $a^{n-1} = 1\ (mod\ n)$ déclarer que n est premier.

On itère ce test avec différentes valeurs de a pour réduire le risque que n ne soit pas premier. A la fin de ces tests on peut conclure que n est premier si on obtient pour toutes les valeurs de a essayées $a^{n-1} \equiv 1\ (mod\ n)$ et il y a très peu de chance que l'on se trompe. C'est pourquoi on parle de test probabiliste de primalité, le test ne garantit pas à 100% qu'un nombre est premier mais pas loin.

Donc les nombres 2-pseudo-premiers ne sont pas aussi “composés” que cela pour les applications pratiques. Et oui car il y a des applications pratiques des nombres premiers, nous le verrons dans le prochain chapître. Mais pendant plus de 2000 ans, il n’y en avait pas. Ces nombres étaient étudiés par pur plaisir de faire avancer la connaissance de voyager dans le mays des nombres premiers. Maintenant ce pays produit quelque-chose d’utile : la cryptologie. Cette production n’est pas anecdotique. Elle est à la base de toutes les transactions sur internet. Le pays des nombres premiers devient un territoire clé, comme le Groëland ignoré pendant des années et maintenant convoité pour ses minerais et sa position géographique. Il ne faut jamais désespérer de l’incroyable efficacité des mathématiques mais ne pas compter dessus non plus. C’est parfois plus beau, quand c’est inutile.

Nombres de Carmichael

Robert Daniel Carmichael (1879 -1967) est un mathématicien américain. On appelle nombre de Carmichael les nombres qui vérifient la condition suivante :

n est un nombre Carmichael si et seulement sii

$\forall\, a/\, 1 < a < n \, et \, a \, premier \, avec \, n \, alors \, a^{n-1} = 1 \, (mod \, n)$

Ils sont ennuyeux pour les tests probabilistes de primalité de Fermat. Dans ce test, on fait varier la valeur du nombre a et on en déduit que si après un grand nombre de valeurs de a on obtient toujours $a^{n-1} = 1\ (mod\ n)$ alors n a une grande probabilité d'être premier. Les nombres de Carmichael sont embêtants car quels que soient le a choisi premier avec n, on a toujours $a^{n-1} = 1\ (mod\ n)$ alors que n n'est pas premier.

Le premier nombre de Carmichael est 561 = 3 x 11 x 17, ensuite viennent 1105, 1729, 2465,...

En 1994, Alford, Granville et Pomerance démontrent qu'il existe une infinité de nombres de Carmichael.

L'astéroïde 101101 s'appelle astéroïde de Carmichael. Il est nommé en l'honneur de Carmichael car le nombre 101101 est le plus petit nombre de Carmichael palindrome (qui peut se lire dans les deux sens). Si vous voulez briller dans les dîners en ville, vous pouvez poser la question : Quel est le point commun entre l'astéroïde dit de Carmichael et la préfecture de la Mayenne ?
Réponse: ce sont tous les deux des palindromes. Il vous faudra ensuite expliquer, avant le dessert, ce qu'est un nombre de Carmichael. Il vous faudra aussi, peut-être, expliquer que la préfecture de la Mayenne est Laval, tout le monde ne connait pas les préfectures. Bonne chance !

Nombre de Mersenne

Un nombre de Mersenne est un nombre de la forme $2^n - 1$ souvent noté M_n.

Théorème :

Si un nombre de Mersenne M_n est premier alors n est premier

Cette condition est suffisante mais pas nécessaire.

Par exemple $2^3 - 1 = 7$ est premier et 3 est premier. La condition est suffisante.

Mais 11 est premier et $2^{11} - 1 = 2\,047 = 23 \times 89$ n'est pas premier. La condition n'est pas nécessaire.

Il existe un test de primalité efficace pour les nombres de Mersenne, le test de primalité de Lucas-Lehmer. Wikipedia donne une très bonne définition de ce test.

C'est pourquoi les plus grands nombres premiers connus sont souvent des nombres de Mersenne. On ne sait pas s'il existe une infinité de nombres de Mersenne premiers. Si cela vous tente, vous pouvez vous attaquez à ce problème. Il existe un lien entre les nombres de Mersenne et les nombres parfaits.

Nombres parfaits

n est un nombre parfait si la somme de tous ses diviseurs, n exclu, est égal à n.

Par exemple:

$$496 = 2^4 \times 31 = 1 \times 2 \times 2 \times 2 \times 2 \times 31$$
$$= 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$$

Au 3^{eme} siècle avant JC, Euclide a démontré que :

Si $M = 2^p - 1$ est premier, alors $M(M + 1)/2 = 2^{p-1}(2^p - 1)$ est parfait.

Euler a ensuite démontré que tout nombre parfait pair est de la forme proposée par Euclide.

$A = 2^{p-1}(2^p - 1)$ (avec $2^p - 1$ premier) $\Leftrightarrow$ A est un nombre parfait pair.

Les 4 premiers nombres parfaits sont :

$6 = 2^1(2^2 - 1) = (1 + 2) + 3$

$28 = 2^2(2^3 - 1) = (1 + 2 + 4) + (7 + 14)$

$496 = 2^4(2^5 - 1) = (1 + 2 + 4 + 8 + 16) + (31 + 62 + 124 + 248)$

$8\,128 = 2^6(2^7 - 1) = (1 + 2 + 4 + 8 + 16 + 32 + 64) + (127 + 254 + 508 + 1\,016 + 2\,032 + 4\,064)$

En 2018 on ne connaissait que 51 nombres parfaits et donc 51 nombres de Mersenne premiers.

On ignore s' il existe des nombres parfaits impairs.
Pourquoi les appelle t'on des nombres parfaits ?
Il faut sans doute remonter à la numérologie grecque. Si la sommes des diviseurs est plus petite on dit que le nombre est déficient. Si elle est plus grande il est abondant. Donc si elle est égale, on l'appelle parfait, ni déficient, ni abondant !

Factorisation

S'il faut beaucoup de puissance de calcul pour montrer qu'un nombre est premier, il en faut encore plus pour le factoriser dans le cas où il n'est pas premier.

Par exemple on a pu prouver que le nombre de Fermat :
$F_{24} = 2^{2^{24}} + 1$
n'est pas premier. Il s'écrie avec 5 millions de chiffres. On ne sait pas calculer ses facteurs premiers. On ne le saura sans doute jamais, mais ils existent.
Pour un nombre "pas trop grand", il est facile de trouver ses diviseurs en essayant de le diviser par tous les nombres premiers qui lui sont inférieurs. Pour un très grand nombre A, cette méthode ne fonctionne pas car on ne connaît pas tous les nombres premiers inférieurs à A.

Fermat a proposé une méthode basée sur la recherche de R et S tel que $A = R^2 - S^2$.
Carl Pomerance, dans les années 70 propose un algorithme appelé "*crible quadratique"*, basé sur la recherche de R et S tels que N divise $R^2 - S^2$.
Cet algorithme a produit, en 1994, grâce à plusieurs centaines d'ordinateurs et des mois d'efforts, la factorisation du nombre RSA-129, un nombre à cent vingt-neuf chiffres produit de deux grands nombres premiers [11].

La difficulté de factoriser de très grands nombres a permis à 3 chercheurs Ronald Rivest, Adi Shamir et Leonard Adleman de développer une méthode de chiffrement à clé publique appelée RSA (initiales des chercheurs). Nous allons voir dans le chapitre suivant ce qu'est une méthode de chiffrement à clé publique.

Cryptologie

La cryptologie, science du secret, englobe :

- La cryptographie, le codage secret d'un message.
- La cryptanalyse, le décodage d'un message codé.

Il existe 2 grandes classes de méthodes de cryptographie:

- Les algorithmes symétriques à clés secrètes ou privées. La clé par un mécanisme de substitution permet de coder un message. Par exemple, une clé basée sur le nombre 3 permet de coder un message en décalant chaque lettre de 3 dans l'ordre alphabétique (a devient d). La machine Enigma utilisée par les allemands pendant la guerre utilisait un tel mécanisme mais beaucoup plus sophistiqué.
- Les algorithmes asymétriques à clés publiques. Dans ces algorithmes il existe 2 clés : une clé publique et une clé privée. Par exemple, Pierre veut recevoir un message en toute sécurité. Il émet 2 clés, il envoie la clé publique à Paul. Paul code son message avec la clé publique mais seul Pierre qui connaît la clé privée peut le décoder.

L'algorithme RSA est le plus utilisé des algorithmes à clés publiques. Il sert au codage et décodage des messages sur internet et des transactions financières. Il

est basé sur les propriétés des nombres premiers et sur le fait qu'il est facile de trouver des grands nombres premiers mais très difficile de factoriser des grands nombres qui sont le produit de ces nombres premiers.

Algorithme RSA

Le protocole RSA comprend 3 parties [10] :

- La génération des clés publiques et privées.
- Le chiffrement du message M qui une fonction dont le sujet est une paire, constituée d'une clé publique e et du message M et l'image message chiffré A. On peut donc le noter comme une fonction que l'on appelle C pour chiffrement : A = C(M,e).

C produit le message chiffré A à partir du message d'origine M et de la clé publique e.

- Le déchiffrement; en utilisant la même notation fonctionnelle, M = D(A,d), retrouve le message original M à partir du message chiffré A et de la clé privée d.

Il y a donc deux clés, e et d : une publique et une privée.

Protocole RSA

1. On choisit 2 grands nombres premiers p et q.
2. On calcule le produit $n = p \times q$
3. Donc $\varphi(n) = \varphi(p) \times \varphi(q) = (p-1)(q-1)$, car p et q sont premiers.
4. On choisit un nombre e premier avec $\varphi(n)$.

5. Ensuite on calcule d tel que :

$\exists\, m \in \aleph / \; ed + m(p-1)(q-1) = 1$

6. La paire (n,e) est la clé publique, d est la clé privée. On remarque que $d \equiv \frac{1}{e}(mod\ \varphi(n))$ car $e \times d - 1 = m\,(p-1)(q-1) = m\,\varphi(n)$ donc $ed \equiv 1 + m\varphi(n)$ donc

$ed \equiv 1\ (mod\ \varphi(n)) \Rightarrow d \equiv \frac{1}{e}(mod\ \varphi(n))$

7. On calcule A la version chiffrée de M :

$A = C(M,e) = M^e\ mod(n)$

8. Pour déchiffrer A, c'est à dire retrouver le message original M, on calcule $A^d\ (mod\ n)$ car

$A^d\ (mod\ n) = M^{e^d}\ (mod\ n) = M^{ed}\ (mod\ n) = M\ (mod\ n)$

Exemple avec 2 petits nombres premiers :

1. p = 17 et q = 11
2. n = p x q = 187, φ(n) = (17 − 1) x (11 − 1) = 160
3. On choisit e premier avec 160, par exemple e = 7
4. Ensuite on calcule d tel que :

$\exists m/\ ed + m(p-1)(q-1) = 1$. On remarque que avec $m = -1$ on obtient

$ed - 1 \times (17 - 1)\,x\,(11 - 1) = 1$

donc $ed - 160 = 1$ donc $ed = 161$

donc $d = \frac{161}{7} = 23$

On peut utiliser l'algorithme d'Euclide si on ne trouve pas par tâtonnement.

5. La clé publique est donc (187, 7) et la clé privée est 2

Clé publique RSA= (187, 7), Clé privée RSA = 23.

Pierre publie sa clé publique afin de recevoir un message de Paul : RSA de Pierre : (187, 7) .
Paul veut lui envoyer son code de carte bleue 1024. Il le découpe en 2 nombres : 10 et 24. Paul envoie 10 en utilisant la clé publique. Il calcule
A=C(10,7)=$10^{7}(mod\ 187)$= 175 et l'envoie à Paul.
Pierre reçoit 175 et le déchiffre grâce à sa clé privé
$M = 175^{23}(mod\ 187) =$
$3889332921869611871983352102688513696193695068359375$
$(mod\ 187) = 10$
Paul fait ensuite de même pour 24.

Paul a pu chiffrer 10 car il connaît la clé publique de Pierre (187,7). Pierre est le seul à pouvoir déchiffrer le message, car lui seul connait 23, nécessaire au déchiffrement. Calculer 23 à partir de 187 et 7 est possible car ce sont de petits nombres, c'est impossible pour des très grands nombres.
On remarque que la puissance du protocole RSA vient du fait qu'il est plus facile de calculer une puissance d'un

grand nombre modulo un autre nombre que d'effectuer l'opération réciproque que l'on appelle calcul du logarithme discret. C'est à dire calculer $c = a^e \ (mod\ m)$ appelé puissance modulaire plutôt que calculer e à partir de c. La méthode RSA utilise une optimisation du calcul de puissance modulaire basé sur l'exponentiation rapide (voir en annexe pour les informaticiens !).

Des clés RSA basées sur des nombres n semi-premiers de plus de 500 chiffres ont pu être fracturées. C'est à dire que l'on a pu retrouver la clé privé à partir de la clé publique à l'aide de beaucoup de calculs et d'astuces mathématiques.
On note ces grands nombres semi-premiers RSA-X ou X est le nombre de chiffres du nombre semi-premier en système binaire.

Par exemple : RSA-576 qui compte 158 chiffres en base 10 compte 576 0 ou 1 en base binaire.

```
RSA-576 (base 10) =
188198812920607963838697239461650439807163
563379417382700763356422988859715234665485
319060606504743045317388011303396716199692
321205734031879550656996221305168759307650
257059
```

RSA-576 a été factorisé le 3 décembre 2003 par J. Franke et T. Kleinjung de l'Université de Bonn (Allemagne) en utilisant l'algorithme GNFS.

Ils ont trouvé que

```
RSA-576 =
3980750864240649373971255005503864911990643623425267084063851895759463889572617685833317
        ×
4727721461074353025362230719730482246329146953020971164598521711305207112563635903975527
```

La société "RSA security" qui publie des nombres semi-premiers difficiles à factoriser offre une prime de 20000€ à qui saura factoriser la clé :

RSA-2048 =

```
2519590847565789349402718324004839857142928212620403202777713783604366202070759555626401852588078440691829064124951508218929855914917618450280848912007284499268739280728777673597141834727026189637501497182469116507761337985909570009733045974880842840179742910064245869181719511874612151517265463228221686998754918242243363725908514186546204357679842338718477444792073993423658485
```

```
238242811981638150106748104516603773060562
016196762561338441436038339044149526344321
901146575444541784240209246165157233507787
077498171257724679629263863563732899121548
314381678998850404453640235273819513786365
643912120103971228221207203 57
```

Personne n’a encore réussi. C’est pourquoi, on recommande aujourd’hui l’utilisation de nombres à 2048 bits. Des articles de presse mentionnant que les ordinateurs quantiques pourront factoriser facilement ces clés. C’est théoriquement vrai. Des informaticiens ont même développé des programmes de factorisation pour de tels ordinateurs. Mais aujourd’hui l’ordinateur quantique est un prototype de laboratoire qui manipule quelques bits. Les cryptologues travaillent sur des principes de chiffrement qui seront difficiles à déchiffrer même pour des ordinateurs quantiques. Les électroniciens mettent au point des moyens de communications basés sur la transmission de photons qui rendra impossible l’interception d’un message dans le modifier. La cryptologie est un secteur stratégique pour l’industrie et la défense. Le pays des nombres premiers contient des ressources critiques pour notre futur. Cela devrait dégager des budgets de recherche dans le domaine. L’hypothèse de Riemann va peut-être être bientôt être démontrée !

Revenons à une utilisation journalière, voyons comment est utilisé ce protocole RSA dans le cas de la sécurisation des cartes bancaires. Pour plus de détail, je vous conseille l'excellent article [11] sur la sécurité des cartes bancaires. Ce qui suit est un résumé.

Il y a deux étapes d'authentification :

- L'authentification de la carte. Le terminal vérifie que la carte est bien issue du groupement des cartes bancaires. Chaque carte contient sur sa puce, un couple de données propre à la carte (nom du porteur, numéro de la carte,...) et le chiffrement de ces mêmes données à l'aide de la clé privée s du groupement des cartes bancaires. Notons ce couple (D,C(D,s)). Le terminal du commerçant connaît lui la clé publique et peut grâce au protocole RSA, déchiffrer C(D,s) à l'aide de la clé publique e et vérifier qu'il retrouve bien les données D. La sécurité est assurée par le fait que même si le pirate connaît la clé publique disponible sur le lecteur, il ne peut calculer la clé privée S. Notons que la clé privée est présente sur la puce de la carte bancaire. Il faut donc que cette puce soit fabriquée et programmée dans des conditions de sécurité maximale.
- Ensuite l'authentification par le code confidentiel, le client rentre en clair son code sur le clavier, la puce sur la carte le compare avec le code stocké sur la carte. Si le code est bon, la carte répond "Oui" au terminal. Pas de codage RSA complexe, une simple transmission de

données et une vérification. Cette étape est assez facile à pirater.

- C'est pourquoi pour les gros paiements, le terminal interroge les ordinateurs de la banque. La carte contient un code secret dans une partie illisible de la puce, notons le K. La banque envoie une valeur aléatoire (différente pour chaque transaction), notons la x. La carte calcule par un algorithme de chiffrement à clé symétrique une valeur que l'on note f(K,x). Le chiffrement à clé symétrique à la différence du chiffrement à clé asymétrique utilise une seule clé pour le chiffrage et le déchiffrage. Il est donc moins sûr car il implique une transmission de la clé. Le chiffrement le plus utilisé est le chiffrement DES ou AES, voir [12]. La banque calcule de même f(K,x). Si les deux résultats sont identiques, la transaction est validée.

-

Pourquoi tous ces détails sur la sécurité des cartes bancaires dans un livre sur les nombres premiers ?

Car en 1998 un ingénieur Français, Serge Humpich, a découvert une faille dans le système. Il a voulu prévenir le groupement des cartes bancaires qui l'a superbement ignoré. Pour se faire entendre, il a démontré cette faille en achetant un carnet de tickets de métro devant les caméras de télévision avec une fausse carte utilisant cette faille. Ce qui lui a valu …. : 10 mois de prison avec sursis. Il avait en fait utilisé 2 failles dont une est que le chiffrement asymétrique basé sur le protocole RSA

utilisait une clé de 320 bits. La taille de la clé était largement suffisante lors de sa création en 1990, mais calculable par un ordinateur en 1998 ! Depuis le groupement des cartes bancaires a augmenté la taille de la clé et amélioré son algorithme de validation.

Démonstrations

Introduction

Nous avons vu dans les chapitres précédents les principaux théorèmes sur les nombres premiers. Nous sommes passés de l'infinité des nombres premiers, énoncé il y a plus de 2000 ans, à la fonction de Riemann et au chiffrement RSA développé en 1977.
Nous avons contemplé les sommets du continent des nombres premiers. Certaines de ces montagnes ont été gravies par des explorateurs mathématiciens géniaux et courageux, d'autres sont encore à conquérir. Les explorateurs sont parties des axiomes, des énoncés considérés vrais dans la théorie choisie, et ont défriché et parcouru les sentiers qui menaient aux points culminants du paysage qui s'offrait à leurs curiosités.
Ces sentiers sont des raisonnements logiques, obéissants à des règles de progression strictes. Les mathématiciens les appellent démonstrations ou preuves. Ils relient les axiomes aux énoncés des théorèmes.

Décidabilité

La notion de démonstration ou de preuve a beaucoup évolué depuis Euclide. Il a fallu attendre des mathématiciens comme Peano (1858-1932) et ensuite Gödel (1906-1978) pour formaliser la notion d'axiomes, de systèmes cohérents et de raisonnements logiques. La littérature sur ce sujet est abondante et les concepts souvent abscons. Avant de présenter des démonstrations liées aux nombres premiers, il est intéressant de regarder les principes de la démonstration qui permettent d'établir les théorèmes présentés dans les chapitres précédents. Pour cela il nous faut décrire rapidement comment la notion de démonstration a évolué d' Euclide à Riemann et pourquoi certains énoncés qui, hier étaient considérés comme des "vérités", sont aujourd'hui des conjectures.

Au début du $20^{ème}$siècle les mathématiciens se sont posés des problèmes de décidabilité : Est-il possible de trouver une preuve ou une démonstration d'un théorème à partir d'un ensemble d'axiomes donnés ?
Existe t'il des théorèmes inatteignables ? Des théorèmes isolés, pour lesquels, il n'existe pas de "chemins", qui les relient aux axiomes de la théorie considérée. Les axiomes de la théorie seraient situés sur un continent alors que les théorèmes seraient situés sur une île. Ils seraient inatteignables. Dans ces cas d'indécidabilité, le

raisonnement logique ne permet que la randonnée pédestre, la nage est interdite !

L'univers des nombres premiers est peuplé de conjectures : des énoncés qui semblent vrais, pour lesquels on a pu trouver aucun contre-exemple mais qui résistent depuis des siècles à toutes les tentatives de démonstrations. Ces conjectures sont elles des théorèmes inatteignables ou des énoncés attendant le mathématicien qui trouvera la bonne démonstration.
Au siècle précédent, une nouvelle catégorie de mathématiciens a vu le jour : les logiciens. Ce sont des "méta-mathématiciens" : les mathématiciens de la mathématique. Ils s'intéressent aux contextes (axiomes de la théorie) et aux moyens (règles du raisonnement logique) qui permettent de décider si un théorème est considéré vrai ou faux.
Une blague entre mathématiciens permet d'illustrer le raisonnement d'un logicien : un physicien, un mathématicien et un logicien voyagent en train en Angleterre. Ils voient 3 vaches blanches avec des tâches noires. Le physicien dit "En Angleterre les vaches sont blanches et noires". Le mathématicien dit "En Angleterre, il existe au moins 3 vaches blanches et noires". Le logicien déclare "Dans ce train de Londres à Manchester, en ce jour du 14 Décembre 2023, sur le coté droit du train, nous avons vu 3 vaches dont un coté au moins est blanc avec des tâches noires". Les logiciens

s'intéressent aux points de départs : les axiomes, et aux cheminements qui permettent de relier ces camps de base aux sommets que sont les théorèmes. Ils définissent quels sont les points de départ qui permettraient d'accéder à tel ou tel sommet, si un sommet est accessible à partir d'un camp de base donné et quels sont les contraintes et les règles du cheminement.

Systèmes Formels

Pour les logiciens, le contexte et le mécanisme qui permet d"établir des "vérités" ou "théorèmes" constituent un système formel.
Ils ont développé des outils permettant d'étudier de tels systèmes. Il y a beaucoup de littérature à ce sujet et de nombreux mathématiciens ont contribué ainsi à rendre leur science plus rigoureuse et complète.

Les mathématiciens travaillant sur les nombres premiers évoluent principalement dans le cadre de deux systèmes formels:

1. Le système formel de l'arithmétique de Peano, nommé Pa, qui résulte du travail du logicien Giuseppe Peano (1858-1932). Ce système formel englobe les entiers naturels et utilise des axiomes (propositions considérées comme vraies par hypothèse du système formel) basés sur les opération arithmétiques (+, -, x, ÷)

et sur les raisonnements basés sur la logique du deuxième ordre (inférence, quantification) et la récurrence. Nous définirons ces concepts plus loin.

2. Le système formel de la théorie des ensembles : cher à tous ceux qui ont subi où apprécié les mathématiques dites “modernes” dans les années 60-70. On considère ici le système ZFC, nommé ainsi d’après les logiciens Ernst Zermelo, Adolf Abraham Fraenkel et l’introduction de l’axiome du choix. L’axiome du choix affirme qu' étant donné un ensemble non vide d’ensembles non vides, on peut lui associer un ensemble en prenant “au choix” un élément dans chacun des ensembles. Pour faire simple, on admet que l’on peut choisir un élément parmi d’autres. Cela semble évident mais c’est la nature des logiciens de différencier ce qui est évident de ce qui ne l’est pas. Ce système formel très puissant permet d’englober tous les entiers naturels du système de Peano mais aussi les nombres réels, les fonctions et aussi tous les objets abstraits manipulés par les mathématiciens. On montre que tout théorème démontrable dans Pa l’est aussi dans ZFC. Un théorème d’arithmétique, concernant les nombres entiers, non démontrable dans Pa mais démontrable dans ZFC (ou ZF : ZFC privé de l’axiome du choix) est considéré comme “transcendant”.

Existent-t-ils des énoncés arithmétiques transcendants ? Kurt Gödel a démontré que la démonstration que Pa est

cohérent, un énoncé ne peut être à la fois vrai et faux, est transcendante. Il faut utiliser ZFC ou ZF pour démontrer cet énoncé.
Les démonstrations des théorèmes sur la raréfaction des nombres premiers que nous avons vus aux chapitres précédents font appel à l'extension de la fonction Zêta aux nombres complexes, Elles sont donc transcendantes. Existent-ils des démonstrations élémentaires (non transcendantes) de ces énoncés ? On ne peut l'affirmer. Les mathématiciens travaillent toujours dessus.

Une fois que le système est défini, il faut aussi s'intéresser aux mécanismes de la preuve.

Logique Mathématique

On s'intéresse ici à la logique classique développée à la fin du 19^{eme}siècle. Elle définit la syntaxe et la sémantique d'un langage qui permet de dériver des énoncés ou théorèmes à partir d'axiomes considérés commé vrais dans le système formel considéré.
Cette syntaxe est présentée au début de l'ouvrage. Nous ne reviendrons pas dessus.
Le principe de la démonstration utilise des règles de déduction logique permettant de prouver un énoncé à partir d'énoncés considérés comme vrais :

Par exemple :
Si A est vrai et si $A \Rightarrow B$ (A entraîne B ou A implique B) alors B est vrai.
Cela peut s'écrire de manière formelle : $(A \wedge (A \Rightarrow B)) \Rightarrow B$

Définissons la fonction Pair(x) comme Pair(x) = vrai si x est divisible par 2 et Pair(x) -= faux dans le cas contraire.
On peut l'écrire :
$\forall x \in \aleph, Pair(x) \Leftrightarrow 2|x$

Attention la ligne qui précéde n'est ni un axiome, ni un théorème, c'est simplement la définition d'un fonction que l'on nomme $Pair(x)$. Notez que l'on n'a pas besoin d'expliciter $Pair(x) = vrai$. Il suffit d'écrire $Pair(x)$, cela à la même signification.

Nous pouvons déduire de cette définition $Pair(6)$ en effet $6 \div 2 = 3 \Rightarrow 2|6 \Rightarrow Pair(6)$.
Voila un premier exemple de démonstration trè simple. Nous avons démontré que $Pair(6)$ est vrai, à l'aide de la définition de $Pair(x)$ et les règles de la logique. Dans ce cas précis, la signification du signe ⇒.

De manière formelle, on peut écrire le théorème découvert par Euclide sur l'infinité des nombres premiers :

$\forall P \in \aleph / premier(P), \exists Q \in \aleph / Q > P$

Démontrons que si x est pair alors $x + 1$ n'est pas pair.
On en profitera pour définir $Impair(x) \Leftrightarrow \neg Pair(x)$
Démonstration :
$Pair(x) \Rightarrow 2|x \Rightarrow x \div 2 = 0 \Rightarrow (x + 1) \div 2 = 1$
$2 \dagger (x + 1) \Rightarrow \neg Pair(x + 1)$
Une manière compliquée de dire que tout nombre entier est pair ou non pair (impair). Mais cette syntaxe et ce raisonnement est compris par tout mathématicien du monde quelque-soit sa langue. En anglais "pair" se dit "even" mais la phrase : "$\forall x \in \aleph, 2|x$" qui définit un nombre "pair" ou "even" s'écrit de la même façon. Les mathématiciens ont inventé un Espéranto des mathématiques !

Cette Espéranto des mathématiques a une propriété particulièrement intéressante. Comme nous l'avons vu dans le chapître sur la notation et la syntaxe. L'avantage de ce langage est d'éviter les imprécisions du langage naturel. On appelle langage naturel par opposition à langage formel, le langage que nous utilisons chaque jour. Un langage formel est un langage mathématique ou informatique dont la syntaxe et la grammaire ne permettent pas les ambiguïtés. Tous les mathématiciens parlent le même langage formel et le comprennent de la même façon.

Un langage formel peut facilement être lu ou manipulé par des ordinateurs qui seront ainsi capables de déterminer la validité d'une preuve ou les valeurs de variables rendant un énoncé vrai. C'est ainsi que dans les années 70 Alain Colmerauer et Philippe Roussel de l'université de Marseille ont inventé le langage PROLOG (programmation logique) à la base de la tempête médiatique sur l'intelligence artificielle et les ordinateurs de la 5^{eme} génération [13]. Tempête qui relativise l'engouement actuel pour le "machine learning" ou l'intelligence artificielle qui ne sont pas vraiment des ruptures technologiques mais des applications de l'analyse statistique rendues plus performantes grâce à la formidable montée en puissance des puces électroniques et des ordinateurs. Il suffit de regarder le cours de l'action NVidia, fabricant de circuits équipant les ordinateurs permettant ces calculs d'analyses statistiques, pour s'en convaincre.
Ces méthodes de déduction et ces systèmes formels ont aussi permis de formaliser la notion de preuves et de démonstrations. Les logiciens en étudient aussi les limites et développent des systèmes formels et des logiques différentes.

Il est intéressant de comprendre le premier théorème d'incomplétude de Gödel qui s'énonce ainsi [9] :

“Une théorie cohérente suffisante pour y démontrer les théorèmes de base de l'arithmétique est nécessairement incomplète, au sens où il existe des énoncés qui n'y sont ni démontrables, ni réfutables (un énoncé est démontrable si on peut le déduire des axiomes de la théorie, il est réfutable si on peut déduire sa négation). On parle alors d'énoncés indécidables dans la théorie.”

Ce théorème et la manière innovante de le démontrer a été une révolution dans l’univers mathématique qui était perçu depuis l’antiquité comme un univers parfait. Un univers dans lequel un énoncé est soit vrai ou faux mais ne peut être les deux à la fois.

Gödel nous dit que quelque soit les axiomes choisis, il existera toujours dans toute théorie cohérente de l’arithmétique des théorèmes qui ne peuvent être démontrés. Une théorie cohérente est une théorie ou les axiomes de base de la théorie ne peuvent mener à des énoncés contradictoires : des énoncés qui seraient à la fois vrais et faux.

Ce théorème nous dit aussi que si les mathématiciens n’ont pas trouvé de démonstration pour un théorème, il faut soit continuer à chercher le chemin le reliant aux axiomes de la théorie, soit changer de théorie..

Certaines conjectures non démontrés à ce jour, telle la conjecture de Goldbach : “Tout nombre pair est la

somme de 2 nombres premiers “ sont peut être de ce type. Notons que si cette conjecture est indécidable dans Pa, elle pourrait être démontrable dans ZFC. Tout dépend des axiomes qui définissent le système formel.

Assez de logique ! Cela risquerait de vous faire croire que les mathématiciens, trop centrés sur la cohérence et la complétude de leur science n’ont même plus besoin de problèmes mathématiques pour s'amuser ! Retournons aux nombres premiers et à la démonstration de certains théorèmes.

Les démonstrations des théorèmes de base sur les nombres premiers suivent souvent deux démarches différentes : l’approche classique basée sur la division Euclidienne [14] et une approche plus moderne basée sur l’arithmétique modulaire [15].
Le chapître suivant donne quelques démonstrations accessibles et importantes. Néanmoins ces démonstrations constituent une partie plus difficile du livre. On ne lit pas une démonstration comme on lit un roman à moins de s’appeler Ramanujan (1887-1920) qui a appris tout seul les mathématiques avec seulement deux livres contenant des théorèmes et des démonstrations. Il a été un explorateur important du domaine des nombres premiers. Pour apprécier une démonstration, il faut du papier, un stylo, du temps et des efforts pour comprendre le raisonnement qui permet de

passer d'une affirmation à la suivante. C’est difficile parfois décourageant mais la compréhension d’une démonstration génère un plaisir égal à celui de la résolution d’une grille de mots croisés compliquée ou la pose de la dernière pièce d’un puzzle. Comme pour beaucoup de domaines dans notre vie, le plaisir de réussir est à la mesure de l’effort. On peut apprécier le style, l’intuition et la créativité de l’auteur comme on apprécie le style d’un grand écrivain. On peut dire d’une démonstration qu’elle est “élégante”. Souvent la beauté est liée à la concision. Mon professeur de mathématiques au lycée : Mr Tournadre annotait les devoirs avec ses appréciations sur le type de démonstration utilisé. Quand la démonstration était trop scolaire et trop longue alors qu’il s’attendait à une démonstration plus concise et astucieuse, il annotait dans la marge “Meuh !”. La méthode était celle du bœuf !

Si vous n’êtes pas prêt, vous pouvez vous arrêter à tout moment dans le chapître qui suit et même le sauter ! Je vous conseille cependant de lire au moins les premières démonstrations datant de l’époque d'Euclide.

Démonstrations

Commençons par quelque-chose de simple :
Nous avons énoncé dans le chapitre sur les constellations de nombres premiers, que dans une série

de 3 nombres impairs consécutifs, il y avait forcément un nombre qui n'était pas premier. Notons p, p+2 et p+4, ces 3 nombres impairs consécutifs. Par exemple si p=11, la série sera 11,13 et 15.

Nous allons montrer que si p est premier alors forcément p+2 ou p+4 ne l'est pas.
Comme p est premier, ce n'est pas un multiple de 3. On peut donc l'écrire sous la forme
$p = 3 \times k + x$ avec $x = 1 \, ou \, x = 2$

Regardons ces 2 cas :

1. $x = 1$

   Dans ce cas $p = 3 \times k + 1$,

   Le nombre impair suivant est $p + 2$.

   $p + 2 = 3 \times k + 1 + 2$

   $= 3 \times k + 3 = 3 \times (k + 1)$

   Donc $p + 2$ n'est pas premier car c'est un multiple de 3

2. $x = 2$

Le nombre impair suivant est toujours p + 2 et
$p + 2 = 3 \times k + 2 + 2 = 3 \times k + 4$
Le nombre impair suivant est $p + 4 = 3 \times k + x + 4$
$p + 4 = 3 \times k + 6 = 3 \times (k + 2)$ donc dans ce cas p + 4 n'est pas premier car c'est un multiple de 3.

On a donc démontré que dans tous les cas si p est premier, p + 2 ou p + 4 ne peuvent être premiers.

Ce type de démonstration directe est appelé démonstration par disjonction de cas. En effet pour démontrer notre proposition on a considéré plusieurs cas possibles.
Cela vous parait difficile, n'hésitez pas à relire ce paragraphe et même à l'illustrer avec des exemples.

Par exemple 7 est premier. Donc ce n'est pas un multiple de 3. On peut l'écrire sous la forme $7 = 3 \times 2 + 1$
Nous sommes dans le cas ou $x = 1$
Le nombre impair suivant 7 est 9.
$9 = 7 + 2 = 3 \times 2 + 1 + 2 = 3 \times 2 + 3 = 3 \times 3$
donc 7 + 2 n'est pas premier.

Un autre exemple pour illustrer le cas x = 2.
Prenons p = 11, p est premier. $p = 11 = 3 \times 3 + 2$
Nous sommes dans le cas ou $x = 2$
Le nombre impair suivant est toujours
$p + 2 = 3 \times 3 + 2 + 2$ et le suivant
$p + 4 = 3 \times 3 + 2 + 2 + 2 = 3 \times 3 + 3 \times 2$
$p + 4 = 3 \times (3 + 2) = 3 \times 5$ donc il n'est pas premier.

Une autre démonstration sympathique :
Quand nous avons introduit la notation de somme tel que $\sum_{i=1}^{10}$, nous avons vu la formule que Gauss utilisait pour calculer la somme les n premiers nombres :

$\sum_{i=1}^{1} = \frac{n(n+1)}{2}$.

La démonstration, bien connue des étudiants, est astucieuse. Il s'agit de faire la somme $S_n = 1 + 2 + \ldots + n$

Pour cela, on l'écrit dans une sens et dans le sens inverse. Cela ne change pas le résultat car l'addition est commutative dans l'ensemble des réels. On effectue donc

$S_n + S_n =$ $1 + 2 + \ldots + (n-1) + n$

$+ n + (n-1) + \ldots + 2 + 1$

On regroupe tous les termes situés les uns au dessus des autres et on obtient :

$= (1 + n) + (2 + n - 1) + \ldots + (n - 1 + 2) + (n + 1)$

$= (n + 1) + (n + 1) + \ldots + (n + 1) + (n + 1)$

$= n \times (n + 1)$

Nous trouvons donc : $S_n + S_n = 2 \times S_n = n \times (n + 1)$

Donc $S_n = \frac{n \times (n+1)}{2}$

On aurait pu aussi démontrer cette formule par récurrence mais c'est moins astucieux. Je vous laisse le faire.

Ainsi la somme des 500 premiers nombres vaut : $S_{500} = \frac{500 \times (500+1)}{2}$

A l'aide d'une calculatrice on trouve facilement en 1 multiplication et 1 division S_{500}= 12750. On a remplacé 499 additions par 2 opérations !

Les étudiants en mathématiques Français sont férus de ces astuces. J'ai commencé ma carrière dans la Silicon Valley. Un ingénieur en électronique m'a demandé comment on pouvait calculer la somme des n premiers nombres. Au lieu de lui donner la formule, je lui ai montré comment la calculer. Il m'a regardé avec étonnement et m'a posé la question : "Est ce que ça marche ?". J'étais surpris. Je lui demande "Que veux-tu dire ?". Il me dit "As tu essayé avec de vrais nombres pour voir si la formule est bonne ?". Nous avons donc essayé avec 9 en effectuant au tableau les 8 additions $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9$ pour arriver à 45 et ensuite nous avons calculé $\frac{n(n+1)}{2} = \frac{9\times10}{é} = 45$. Il est sorti content de mon bureau. Cet exemple illustre bien la différence de formation entre un ingénieur électronicien Français passé par les classes préparatoires aux mathématiques omniprésentes et un ingénieur en électronique (MSEE) américain pour qui les mathématiques ne sont qu'un outil pratique. Il ne voyait aucune élégance dans cette astuce. Il n'était pas convaincu, que la validité de la démonstration de la formule, le dispensait de sa vérification. Par contre il était très doué en électronique car pourvu de solides bases de calcul et d'un sens pratique qui lui faisait

vérifier rigoureusement les circuits qu'il calculait. De même, leurs cours d'électronique contenaient beaucoup d'applications numériques de la même formule avec des valeurs différentes alors qu'en France les cours d'électronique insistent beaucoup sur les formules mathématiques et peu sur les applications numériques. Notre approche peut parfois amener l'étudiant à des résultats stupides que le bon sens de l'étudiant américain aurait remis en question. Je donnais un cours de Physique à un lycéen. L'exercice consistait à utiliser une formule donnant la vitesse d'un cycliste.

Le cycliste roule à une vitesse constante v. Il franchit la ligne d'arrivée après t heures. Combien de kms a il parcouru :

La formule est $l = v * t$, en s'assurant que v est exprimé en heures.

Il y avait une application numérique avect = 120 mn et $v = 20$ km/h .

Le résultat était donc $l = 20 \times \frac{120}{60} = 40$ km.

L'étudiant calcula $l = 20 \times 120 = 2400$ kilomètres !

Il m'assura qu'il avait vérifié sa solution plusieurs fois et que sa formule était bonne. Pourtant il était évident qu'elle ne marchait pas. Un cycliste ne peut pas faire 2400 kms en 2 heures, même en le supposant fortement dopé. Il avait oublié d'exprimer de transformer la vitesse de km/mn en km/h. Il avait trop confiance dans ses capacités mathématiques et avait oublié d'utiliser son sens pratique pour comprendre le résultat.

Revenons maintenant presque 2000 ans en arrière, habillons nous d'une toge et attaquons nous au théorème sur l'infinité des nombres premiers.

L'infinité des nombres premiers

Énoncé : Il y a une infinité de nombre premiers.

Cela a été démontré pour la première fois par Euclide au 3^{eme} siècle avant JC.

C'est une démonstration par l'absurde (voir plus loin). C'est à dire que l'on fait l'hypothèse que ce que l'on veut démontrer est faux et on arrive par un raisonnement logique à une conséquence contredisant l'hypothèse. C'est donc que l'hypothèse est fausse donc le théorème à démontrer est vrai !

Une démonstration verbeuse pour commencer :

Supposons qu'il n'y ait pas une infinité de nombres premiers. Si l'ensemble des nombres premiers n'est pas infini, il possède un plus grand nombre, supérieur à tous les autres éléments de l'ensemble. Appelons le N.
Considérons le nombre
$P = N! + 1 = N(N - 1)(N - 2)\ldots 2 \times 1 + 1$

2 cas sont possibles

- Soit P n'a pas de diviseur et comme P > N alors P est premier et plus grand que N ce qui contredit l"hypothèse.
- Soit P a un diviseur premier Q et dans ce cas Q est plus grand que N car la division de P par tout nombre inférieur à N donne 1. En effet, si Q est un inférieur à N, c'est un facteur de N!.

$$P = N! + 1 = (N - 1) \times (N - 2) \ldots \times Q \times \ldots 2 \times 1 + 1$$

Donc Q est plus grand que N ce qui contredit aussi l'hypothèse.

Donc il n'existe pas de nombre N qui serait le plus grand nombre premier. C'est-à-dire que quel que soit un nombre premier P on peut toujours trouver un nombre premier plus grand. L'ensemble des nombres premiers est infini.

Typologie de la démonstration

Nous venons de voir un type de démonstration particulier : la démonstration par l'absurde. Il y a 3 méthodes de démonstrations principales :

La démonstration directe :

On sait que la proposition A est vraie (A est un axiome, une définition ou a été démontrée précédemment) et on

sait aussi que $A \Rightarrow B$ (A implique B), on en déduit que B est vraie.

Montrons que la somme de 2 nombres impairs est pair :
Soit a et b ∈ N, a et b impair.
On sait par définition que si a est impair,
$\exists\, k \in N \,/\, a = 2 \times k + 1$
De même pour b
$\exists\, l \in N \,/\, b = 2 \times l + 1$
Donc $a + b = 2 \times k + 1 + 2 \times l + 1$. Appelons cette assertion *a1.*
Donc $a + b = 2(k + l + 1)$ Appelons cette assertion *a2.*
Soit $j = k + l + 1\, alors\, a + b = 2 \times j$
Donc $a + b$ est le double d'un nombre. Ce qui est la définition d'un nombre pair. On a donc démontré que $a + b$ est pair.

Remarquons que pour passer de l"assertion a1 à l'assertion a2 on a utilisé des propriétés de l'addition et de la multiplication des nombres entiers : la commutativité, l'associativité et la distributivité de la multiplication sur l"addition. Nous ne reviendrons pas sur la définition de ces propriétés détaillées dans le chapître sur la notion de groupe mais il est important de noter que toute démonstration dépend d'un certain nombre d'acquis. Ces acquis sont des théorèmes que l'on suppose évidents pour le lecteur et dont nous n'avons

pas besoin de rappeler l'existence. C'est ce qui rend parfois difficile la lecture d'une démonstration, les acquis d'un agrégé de mathématique sont supérieurs à celle d'un étudiant de terminale et ce dernier aura besoin de plus d'étapes intermédiaires dans la démonstration pour retomber sur un de ses "acquis". C'est pourquoi on dit souvent que une démonstration se place dans le cadre d'une "théorie". Dans le cas précédent, c'est la théorie des groupes commutatifs. Cela rend inutile de redémontrer les énoncés dèjà démontrés dans cette théorie.

La démonstration par contraposition

On peut démontrer B en utilisant la définition des connecteurs logique :

$A \Rightarrow B \; est \; équivalent \; A \; \vee \; \neg B$

et

$A \Rightarrow B \; est \; équivalent \; \neg B \Rightarrow \neg A$

En d'autres termes "A est vrai implique que B est vrai" est équivalent à " A est vrai ou B est faux" et "B est faux implique que A est faux".

En effet si $\neg B \Rightarrow \neg A$ cela veut dire que quand B est faux alors A est faux en effet si A était vrai comme $A \Rightarrow B$, B serait vrai.

Donc dans certains cas, sachant que A est vrai et $A \Rightarrow B$ on va utiliser $\neg B \Rightarrow \neg A$ pour démontrer que B est vrai.

On peut illustrer cette équivalence par ce que l'on appelle une table de vérité.

A	B	non A	non A ou B	A ⇒ B (par définition)
Vrai	Vrai	Faux	Vrai	Vrai
Vrai	Faux	Faux	Faux	Faux
Faux	Vrai	Vrai	Vrai	Vrai
Faux	Faux	Vrai	Vrai	Vrai

Par exemple, Appelons A la proposition

$a, b \in N \ / \ a \neq 0 \ et \ a \neq b$

C'est à dire que a et b sont des entiers naturels tels que a est différent de 0 et b est différent de a. C'est tout ce que l'on sait sur a et b. C'est notre hypothèse.

Et la proposition

$3a + 1 \neq 3b + 1$

Montrons que si A est vraie alors B est vraie :

Considérons la proposition $\neg B$:

$\neg(3a + 1 \neq 3b + 1)$ est équivalent à :

$3a + 1 = 3b + 1$ donc $3a - 3b = 1 - 1$ donc $3(a - b) = 0$ donc $a - b = 0$ donc $a = b$ ce qui contredit A.

On peut donc conclure par $\neg A$ est vrai.

On a montré “laborieusement” que $\neg B \Rightarrow \neg A$ on peut en déduire que $A \Rightarrow B$ donc si A est vraie alors B est vraie donc $3a + 1 \neq 3b + 1$ est vrai. Mon professeur de mathématiques modernes aurait sûrement écrit un “Meuh” dans la marge devant une telle démonstration.

On a utilisé dans cette démonstration des propriétés de l’addition, de la multiplication et de la relation d’égalité (compatibilité de la relation d'égalité avec l’addition et la multiplication) qui s’énonce ainsi:
$\forall a, b, c \in N, (a = b) \Rightarrow (a + c = b + c)$
En langage de tous les jours, si deux nombres sont égaux, les résultats de leurs sommes par un même nombre sont égaux aussi. Cela semble évident mais ce sont des propriétés spécifiques à certaines opérations comme l’addition et la multiplication et certaines relations comme l’égalité.

Dans les débuts et durant l’expérimentation de l’enseignement des mathématiques dites “modernes” dans les années 70, on demandait aux élèves du collège de rappeler ces propriétés quand il mentionnait “Donc” dans leur démonstration. Dans le genre
"$3a + 1 = 3b + 1$ donc $3a - 3b = 1 - 1$ car l’addition est compatible avec l’égalité dans N”.
Cela rendait les démonstrations un peu longues et il n’était pas rare de rendre 4 pages de démonstrations lors des examens. Les mathématiques, ainsi enseignées,

formaient les esprits à une rigueur logique dans la démonstration et à une critique des faits et des raisonnements qui les produisent. Une approche bien utile à l'époque des réseaux sociaux, des vérités alternatives et des raisonnements "douteux" qui enfreignentt les lois de la logique. Cet apport des mathématiques est bien décrit dans le livre de Francis Su "Mathematics for human flourishing" [16].

La démonstration par récurrence

On veut démontrer qu"une proposition P(n) est vraie pour toute valeur de n entier naturel.

Récurrence simple:

On démontre que la proposition P est vraie pour une valeur initiale, souvent 0 ou 1. On démontre ensuite que si elle est vraie pour n alors elle est vraie pour n+1.
On en déduit par le principe de récurrence (parfois appelé hérédité) que la proposition est vraie pour toute valeur de n à partir de la valeur initiale.

En langage mathématique:

$(P(a) \ \wedge \ (P(n) \ \Rightarrow P(n+1)) \Leftrightarrow P(n), \ \forall n \in N/n \geq a$
Note: Quand on écrit simplement P(n) cela veut dire P(n) est vrai.

Exemple :
On définit une suite de nombres u_n :

$u_0 = 3 \; et \; u_{n+1} = 4u_n$

Démontrons que la propriété, P(n) :

$\forall n \in N, \; u_n = 4^n \times 3$, est vraie.

On initialise la récurrence à partir de $n = 0$:

$u_0 = 3 \; = 1 \times 3 = 4^0 \times 3$ donc P(0) est vraie.

Supposons P(n) vrai : $u_n = 4^n \times 3$

Par définition

$u_{n+1} = 4u_n \; donc \; u_{n+1} = 4(4^n \times 3) = 4^{n+1} \times 3$

On a donc démontré $P(n) \Rightarrow P(n+1)$
En appliquant le principe d'hérédité on a bien démontré

$\forall n \in N, \; u_n = 4^n \times 3$ CQFD

Les démonstrations finissent souvent par CQFD. C'est en mathématiques l'équivalent du joueur de football qui glisse sur la pelouse les bras en l'air après avoir marqué un but. Ce sont les initiales de "Ce Qu'il Fallait Démontrer". Le mathématicien est content alors il annonce haut et fort ce "CQFD".

Récurrence forte:

Il existe une autre démonstration par récurrence qui sera utilisée dans les pages suivantes, la récurrence forte.

Comme pour la récurrence simple, on démontre que la proposition P est vraie pour un nombre initial a : P(a). 0 ou 1 sont souvent choisis comme valeur de a.
On considère ensuite que P(i) est vrai, $\forall i \in N / a \leq i \leq n$, et on démontre que dans ce cas P(n+1) est vrai.
On peut en déduire par hérédité que P(n) est vraie pour toute valeur de n à partir de la valeur initiale a.

En langage mathématique
$(P(a) \ \wedge \ ((P(i)\,, \forall i \in N,\, a \leq i \leq n)$
$\Rightarrow P(n+1)) \Leftrightarrow (P(n),\, \forall n \in N / n \geq a)$
On utilisera la récurrence forte dans la démonstration de l'unicité de la décomposition en nombres premiers (voir plus bas).

La récurrence forte et la récurrence simple sont assez similaires, la récurrence forte permet simplement de considérer dans la démonstration que si la propriété est vraie pour une valeur a et que si elle est vraie aussi pour toutes valeurs entre a et n entraine qu'elle est vraie pour $n + 1$ alors elle est vraie pour toute valeur supérieure à n.

Nous sommes prêts maintenant à nous attaquer au théorème fondamental de l'arithmétique:

Théorème fondamental de l'arithmétique

Tout entier naturel peut être écrit comme un produit de nombres premiers d'une unique façon, à l'ordre près des facteurs.

Cette démonstration utilise le théorème de Gauss (voir plus haut) dont la démonstration moderne est basée sur le théorème de Bezout (voir aussi dans le chapître sur les théorèmes fondamentaux).

Nous allons donc nous attaquer à ces monuments de l'arithmétique dans cet ordre.

Théorème de Bezoux et de Gauss.

Rappel du théorème de Gauss :

Soient p, a et b trois entiers naturels non nuls tels que p | ab et p est premier avec a alors p | b.

Rappelons que *p* | *b* veut dire p divise b. C'est à dire que b est un multiple de p donc que la division euclidienne de b par p donne un reste nul.

Soit aZ l'ensemble des multiples de a, et pZ l"ensemble des multiples de p. Nous avons vu que ce sont des idéaux de Z. Soit aZ+pZ l'ensemble de toutes les combinaisons linéaires du type $ax + py$ avec x et y appartenant à Z, c'est aussi un idéal de Z. Nous avons

vu dans le chapître sur les idéaux que tout idéal de Z est du type αZ, avec $\alpha \in Z$. Il existe donc un α dans Z tel que aZ+pZ est l'ensemble des multiples de α. Si on considère x = 1 et p = 0 : $a \times 1 + 0 \times y = a$. Cet idéal contient donc a. On peut appliquer le même raisonnement pour démontrer que cet idéal contient aussi p.

Donc α|a et α|p. Comme p est premier avec a, ils n'ont pas de diviseur commun autre que 1.

Donc α=1 et a Z+ p Z = 1Z = Z.

Donc quelque soit un nombre v de Z on peut trouver deux nombres x et y de Z tel que $ax + py = v$. En particulier pour v = 1

Donc $\exists x, y \in Z / ax + py = 1$.

Remarquons que nous venons de démontrer en passant le théorème de Bezoux !

Continuons.

$p \mid ab$ *donc* $\exists k \in Z$ / $\frac{ab}{p} = k$

En multipliant chaque côté de l'égalité par b on obtient

$ax + py = 1 \Rightarrow b(ax + py) = b$

$\Rightarrow abx + pby = b \Rightarrow p(\frac{ab}{p}x + by) = b$

$\Rightarrow p(kx + by) = b \Rightarrow p|b$. CQFD

Et voila nous avons démontré grâce aux propriétés de l'arithmétique modulaire le théorème de Gauss.

Attaquons nous maintenant au théorème fondamental de l'arithmétique : l'unicité de la décomposition en facteurs premiers de tout nombre entier naturel.

$\forall n \in N, \exists! \{p_1 \dots p_k\} et \{e_1 \dots e_k\}$ / n = $\prod_{i=1}^{k} p_i^{e_i}$

Appelons H(n) ce thèorème appliqué au nombre n. L'existence de la décomposition en nombre premier est facile à démontrer. Il suffit d'utiliser le mécanisme de récurrence forte.

H(2) est vrai. En effet 2 peut se décomposer sous la forme 2 = 2 et 2 est premier.
Supposons que H(n) est vrai pour $n \in [2, n]$montrons que H(n+1) est vrai.

Posons m = n+1.
Soit m est premier, alors m = m est la décomposition en nombres premiers de n+1.
Soit m a un diviseur k $\Rightarrow \exists k, l \in N / m = k \times l$

$k \neq m,\ k|n,\ l|m$ donc $k < m,\ l < m$ donc
k $\in [2, n]$ et l $\in [2, n]$ donc k et l sont un produit de diviseurs premiers, donc m est le produit de ces produits, c'est donc aussi un produit de diviseurs premiers. CQFD

L'unicité est plus complexe. Rappelons que Euclide ne l'avait pas démontrée ! Il nous faut pour cela utiliser le théorème de Gauss et une démonstration par récurrence.

Initialisation de la récurrence :
Supposons que la décomposition est unique pour n=2
Supposons aussi qu'elle est unique $\forall i \in [2, n-1]$

Montrons que la décomposition est unique pour n.
Nous allons utliliser une démonstration par l'absurde.
Supposons qu'il existe 2 décompositions pour n :
Sans utiliser les puissances pour regrouper les facteurs égaux on peut l'écrire ainsi :
$n = q_1 q_2 \dots q_m \ et \ n = s_1 s_2 \dots s_l$
Nous allons utiliser une disjonction de cas :

1. Soit $q_1 = s_1 \Rightarrow \frac{n}{q_1} = q_2 \dots q_m = s_2 \dots s_l$

Or $\frac{n}{q_1} < n$ donc sa décomposition est unique. Donc

$m = l \ et \ \forall i \in \{2, m\}, q_i = s_i$

2. Soit $q_1 \neq s_1$. Or $q_1 | n$ car

$n = q_1 q_2 \dots q_m$ et $n = s_1 s_2 \dots s_l$ donc $q_1 | s_1 s_2 \dots s_l$

Or q_1 et s_1 sont des nombres premiers donc premiers entre eux. En utlisant le théorème de Gauss, on peut en déduire que $q_1 | s_2 \dots s_l$

Notons $k = s_2 \dots s_l$. Or $k < n$ donc k a une décomposition unique et puisque $q_1 |$ k, on peut diviser par q_1 les deux décomposition de n : $q_1 q_2 \dots q_m$ et $s_1 s_2 \dots s_l$. Appelons $j = \frac{n}{q_1} = q_2 \dots q_m$

Comme précédemment, j < n et la décomposition de j est unique par hypothèse de récurrence. Donc les deux décompositions d'origine étaient uniques à l'ordre près.

Pas facile ? Rappelez vous Euclide ne l'avez pas trouvé. Il n'avait pas développé l'arithmétique modulaire et ne pouvait donc suivre cette voie. Il existe une autre démonstration utilisant la division euclidienne, plus laborieuse. Il ne l'avait pas trouvée non plus. Alors ne vous découragez pas, ce n'est pas facile. C'est ce qui fait l'intérêt et la beauté de ces démonstrations.

Si vous avez suivi jusqu'ici sans trop être perdu ou découragé, bravo !
Vous avez déjà sans doute compris la difficulté de la démonstration. Il faut bien connaître les axiomes, garder en mémoire les hypothèses et choisir une méthode de

démonstration. La lecture simple est compliquée car elle oblige à reproduire le raisonnement logique suivi par l'auteur de la démonstration. Plus vous avancez dans le domaine des mathématiques, plus l'auteur d'une démonstration saute des lignes en pensant que le lecteur du même niveau que lui trouvera facilement les passages intermédiaires. Un peu comme quand vous suivez les instructions d'une randonnée sur un guide de rando, 5 kms se résument parfois en 2 lignes : "prenez à droite après la balise 108". Alors que vous avez rencontré multitudes de chemins à droite, sans jamais être sûr de ne pas avoir loupé la balise 108. La démonstration est le résumé de la randonnée du mathématicien qui décrit son parcours, du début de son périple jusqu'au sommet convoité. Certains sont patients et généreux et vont décrire toutes les étapes intermédiaires ainsi que les paysages, d'autres sont plus elliptiques et par fainéantise ou pour décourager les amateurs, ne vous indiqueront que quelques bifurcations importantes.

Dans ce livre dont le but est de vous accompagner dans le domaine des mathématiques quel que soit votre niveau, nous détaillerons le plus possible les étapes des démonstrations. Vous trouverez par exemple 4 pages pour la démonstration du postulat de Bertrand alors que Wikipedia vous la livre en une demi-page.

Les démonstrations qui suivent demandent de comprendre les notions de partie entières et partie décimale d'un nombre réel, des notions de base sur les logarithmes et sur la combinatoire. Avant de les aborder, je vous recommande de les revoir dans la partie annexe.

Démonstration sur la partie entière du double d'un nombre.

Vous avez vu en annexe ou bien vous connaissez déjà la définition de la partie entière d'un nombre rationnel x, notée E(x) et de la partie décimale, notée D(x). Nous allons montrer que $E(2x) - 2E(x)$ est égal à 0 ou 1.

Pour cela nous allons, comme le ferait un mathématicien, face à un nouveau problème, nous familiariser avec celui-ci en étudiant des exemples.

x	E(x)	D(x)	2x	E(2x)	D(2x)	E(2x)-E(x)
3,125	3	0,125	6,25	6	0,25	3
2,456	2	0,456	4,912	4	0,912	2
1,854	1	0,854	3,708	3	0,708	2
32,4	32	0	64,8	64	0,8	32
33	33	0	66	66	0	33
0,92	0	0,92	1,84	1	0,84	1

Etudions la colonne de gauche. Essayons de trouver un lien, une corrélation comme disent les statisticiens avec

les colonnes de droite. Il apparait que lorsque la partie décimale D(x) est inférieure à $\frac{1}{2}$:

$E(2x) - 2E(x) = 0$

et lorsque D(x) est supérieure ou égal à $\frac{1}{2}$:

$E(2x) - 2E(x) = 1$.

A cette étape de notre investigation, nous avons simplement une intuition basée sur nos expériences. Ce que les mathématiciens appellent une conjecture. Appelons la “conjecture du double de la partie entière”. Ça sonne bien !

Il nous faut maintenant la démontrer. Nous allons nous limiter pour plus de simplicité au cas ou x > 0 . Nous allons utiliser une méthode par disjonction de cas.

Soit k le plus grand entier tel que $k \leq x < k + 1$
$k = E(x)$ par définition de E(x) (voir annexe).
Donc $2k = 2E(x)$

Calculons maintenant E(2x)
Notre intuition basée sur le tableau nous montre qu’il faut différencier 2 cas :
Cas 1: $d < \frac{1}{2}$, $x = k + d \Rightarrow 2x = 2k + 2d < 2k + 1$
or $k \leq x \Rightarrow 2k \leq 2x$ donc $2k \leq 2x < 2k + 1$ donc $E(2x) = 2k$ donc $E(2x) - 2E(x) = 2k - 2k = 0$
Donc $E(2x) = 2E(x)$

Cas 2: $d \geq \frac{1}{2}$, $x = k + d$ donc $2d = 1 + j$

avec $0 \leq j < \frac{1}{2}$

Donc $2x = 2k + 2d = 2k + 1 + j$

Donc $2k + 1 \leq 2x < 2x + 2$

Donc $E(2x) = 2k + 1$

Donc $E(2x) - 2E(x) = 2k + 1 - 2k = 1$

Donc $E(2x) = 2E(x)$+1

CQFD

Nous sommes passés de l'intuition basée sur l'étude de quelques nombres particuliers à la généralité confirmée par la démonstration. C'est un raccourci de la démarche mathématique. Je me souviens de certains élèves, qui après avoir séché sur un problème de mathématiques demandant un peu d'astuce, demandaient de l'aide. Le dialogue suivant n'était pas rare :

- Relis l'énoncé.
- Je l'ai déjà fait.
- Oui, mais imprègne toi du problème en le relisant.
- Je l'ai relu, je ne comprends toujours pas.

"Je ne comprends pas", voulait dire, "je ne trouve pas la solution". Le dialogue évoluait vers :

- Pas grave, joue avec les données du problème.
- Qu'est ce que ça veut dire ?

- Manipule les, additionne les nombres, déduit des énoncés que l'on ne te demande pas de démontrer. La lumière viendra.

C'est ce que nous avons fait en prenant des exemples. Cela nous a emmené vers une démonstration basée sur une disjonction de deux cas. On ne commence jamais par comprendre ou trouver la solution. La solution émerge de notre esprit grâce à l'effort, au travail et un brin d'intelligence : 90% de sueur, 10% d'intelligence. Ceux qui font des mots croisés, partagent cette expérience. Ils lisent et relisent 100 fois la définition et subitement le mot correct surgit dans leur esprit. Cette apparition est accompagnée d'un sentiment de satisfaction, de contentement, voire de plaisir. Le bonheur ressentit par un mathématicien trouvant la démonstration après de longues heures, journées ou années de recherches est du même ordre. On peut même dire en paraphrasant Corneille que "le plaisir s'accroît, quand la solution se recule". Continuons cette poursuite du bonheur avec des démonstrations de plus en plus compliquées. N'hésitez pas à quitter la lecture du livre pour essayer de trouver les démonstrations par vous mêmes, à parcourir le net, ou à utiliser "le chat" ou "chatGPT" pour vous guider. L'intelligence artificielle ne trouvera pas la solution complète à des problèmes jamais résolus mais pourra vous guider vers des étapes intermédiaires déjà documentées.

Démonstration avec les logarithmes

Montrons que :

$$\forall n, p, k \in Z^{*+} / k > \frac{ln(n)}{ln(p)} \Rightarrow E(\frac{n}{p^k}) = 0$$

La compatibilité de la relation d'ordre avec la multiplication par un nombre positif nous permet de déduire :

$k > \frac{ln(n)}{ln(p)} \Rightarrow k \times ln(p) > ln(n)$, notons (1) cet énoncé.

Prenons l'exponentielle des 2 parties de l'inégalité. Cette inégalité est préservée car l'exponentielle est une fontion croissante et positive.

(1) $\Rightarrow e^{kln(p)} > e^{ln(n)}$

Le logarithme est la fonction réciproque de l'exponentielle $e^{ln(x)} = x$ et $e^{x^y} = e^{xy}$

$(1) \Rightarrow e^{ln(p)^k} > n \Rightarrow p^k > n \Rightarrow 1 > \frac{n}{p^k}$

or $\frac{n}{p^k} \geq 0$ car n,p,k sont des entiers positifs.

donc $0 \leq \frac{n}{p^k} < 1 \Rightarrow E(\frac{n}{p^k}) = 0$ CQFD

Comme vous l'avez constaté, dans cette démonstration nous tirons partie à chaque pas des propriétés de la fonction exponentielle et de la fonction logarithme. Trouver la bonne démonstration demande de l'intuition mais aussi de la mémoire. Il faut bien avoir en tête les

propriétés des fonctions que l'on manipulent. Il faut souvent se référer à un ensemble de propriétés ou de théorèmes pour passer d'une étape à l'autre. Nous avons vu que l'on appelle "théorie", les ensembles de théorème dans un domaine particulier. Nous pouvons parler ici de la théorie des fonctions logarithmiques ou exponentielles. L'apprentissage de ces théories fait partie de l'enseignement des mathématiques. Les théories sont des boîtes à outils que l'on doit connaître et maîtriser pour progresser dans une théorie nouvelle. Il faut vous munir des outils de plomberie (clés, poste de soudure,...) et d'électricité (tournevis, voltmètre,...) pour vous attaquer à l'installation de votre pompe à chaleur et bien connaître ces deux artisanats avant de vous aventurer dans la découverte d'un nouveau savoir faire. C'est pourquoi l'apprentissage des mathématiques est parfois perçu comme laborieux et complexe. Il est difficile d'aborder de nouvelles théories avec des lacunes dans les théories de base. Quand un élève perd pied dans une classe, il est souvent difficile de comprendre les sujets abordés dans la classe suivante. Ce côté accumulatif des connaissances rend difficile le papillonnage. On ne passe pas d'une fleur à l'autre aussi facilement tel un passionné d'histoire qui lirait un livre sur l'histoire antique romaine et ensuite un autre sur la deuxième guerre mondiale.

Démonstration de la relation de Pascal

$\forall\, n, k \in N / k \leq n$ alors
$C(n,k) = C(n-1,k-1) + C(n-1,k)$

Nous appelons cela une démonstration mais en fait, il s'agit d'un simple calcul. Pas besoin de recourir à des méthodes de récurrence, de disjonction de cas ou de démonstration par l'absurde. Il suffit d'appliquer les règles de la multiplication, de la division et de l'addition dans le bon ordre.

Rappelons que $C(n,k) = \frac{n!}{k!(n-k)!}$

La démonstration est simple, elle se fait par le calcul de la partie droite de l'égalité en réduisant les 2 facteurs de la somme au même dénominateur :

$C(n-1,k-1) = \frac{(n-1)!}{(k-1)!(n-1-(k-1))!} = \frac{(n-1)!}{(k-1)!(n-k)!}$

$= \frac{(n-1)!k}{(k-1)!(n-k)!k} = \frac{(n-1)!k}{k!(n-k)!}$

$C(n-1,k) = \frac{(n-1)!}{k!(n-1-k)!} = \frac{(n-1)!(n-k)}{k!(n-k-1)!(n-k)} = \frac{(n-1)!(n-k)}{k!(n-k)!}$

Donc

$C(n-1,k-1) + C(n-1,k) = \frac{(n-1)!k + (n-1)!(n-k)}{k!(n-k)}$

$= \frac{(n-1)!(k+n-k)}{k!(n-k)} = \frac{(n-1)!n}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = C(n,k)$

CQFD

Formule de Legendre

Regardons maintenant des démonstrations un peu plus compliquées. Commençons par la formule de Legendre, vue au chapitre précédent.

Rappel de la définition de la vualtion p-adique :

Soit p un nombre premier, l'exposant de p dans la décomposition en facteurs premiers de n!, ou encore le plus grand entier k tel que
p^k| n! est la valuation p-adique de n!. On le note $v_p(n!)$

La formule de Legendre donne une expression de sa valeur sous forme d'une somme infinie :

$$v_p(n!) = E(\frac{n}{p}) + E(\frac{n}{p^2}) + E(\frac{n}{p^3}) + \ldots = \sum_{k=1}^{\infty} E(\frac{n}{p^k})$$

Avant d'attaquer la démonstration, nous allons démontrer un petit théorème que l'on appelle lemme :

$$v_p(a \times b) = v_p(a) + v_p(b).$$

Pour faciliter l'écriture appelons $k = v_p(a)$ et $l = v_p(b)$, k et l sont les plus grands entiers tels que p^kdivise a et p^l

divise b. Ce sont donc les exposant de p dans la décomposition en facteurs premiers de a et b. Donc $a = p^k \times X$ et $b = p^l \times Y$. X et Y étant le produit des autres facteurs premiers. On en déduit que :

$$a \times b = p^k \times X \times p^l \times Y = p^{k+l} \times XY$$

Donc $k + l = v_p(a) + v_p(b)$ est le plus grand exposant de p dans la décomposition de $a \times b$.

Donc $v_p(a \times b) = v_p(a) + v_p(b)$

CQFD

Une fois ce lemme démontré, Revenons à la démonstration initiale comme beaucoup de démonstrations complexes elle va nécessiter plusieurs parties :

On considère un entier naturel n et un nombre premier p. On considère aussi un entier N tel que $p^N \geq n$.

1ère partie:

Intéressons nous à la question suivante, soit u un entier naturel, combien y'a t'il de multiples de u dans l'ensemble {1,...,n} ?

Soit $m \times u = mu$ le plus grand multiple de u inférieur à n. On peut donc écrire ;

$$mu < n < (m + 1)u \Rightarrow m < \frac{n}{u} < m + 1$$

On reconnaît la définition de $E(\frac{n}{u})$ (voir annexe sur la partie entière et la partie décimale d'un nombre rationnel). Donc $m = E(\frac{n}{u})$

Il y a donc $E(\frac{n}{u})$ multiple de u dans {1,...,n}.

Cette formule peut paraître compliquée. Il suffit souvent de prendre des exemples pour mieux comprendre :

Prenons u = 5 et n = 92. Combien y a t'il de multiples de 5 entre 1 et 92. Il y en E($\frac{92}{5}$) $= 18$
5,10,15,20,25,30,35,40,45,50,55,60,65,70,75,80,85,90

2ème partie
On appelle $A_k = \{l \in \{1 \dots n\}, v_p(l) = k\}$ calculons le nombre d'éléments dans A_k c'est à dire card(A_k).

$v_p(l) = k \Leftrightarrow (p^k \mid l) \wedge (p^{k+1} \nmid l)$ en effet $v_p(l)$ est le grand exposant de p qui divise l.
Donc $card(A_k)$ est égal au nombre de multiples de p^k moins le nombre de multiples de p^{k+1}. Nous avons vu dans la première partie que ce nombre est égale à $E(\frac{n}{p^k}) - E(\frac{n}{p^{k+1}})$. Si cela ne vous semble pas évident, lisez l'exemple plus bas.
Donc $card(A_k)$ = $E(\frac{n}{p^k}) - E(\frac{n}{p^{k+1}})$

3ème partie

$v_p(a \times b) = v_p(a) + v_p(b)$

donc $v_p(n!) = v_p(n \times (n-1) \times (n-2) \ldots \times 2 \times 1))$

$= \sum_{l=1}^{n} v_p(l) = v_p(1) + v_p(2) + \ldots + v_p(n-1) + v_p(n)$.

Notons (a) cette somme pour y revenir plus tard.

Tous les $v_p(l)$ sont égales à un nombre k compris entre 0 et N. Pour chaque k tel que $0 < k < N$, il y a $card(A_k)$ nombres

$l \in$ {1,...n} tel que $v_p(l) = k$ et

$card(A_k) = E(\frac{n}{p^k}) - E(\frac{n}{p^{k+1}})$

On peut donc regrouper la somme (a) par valeur de k.

$(a) = \sum_{k=1}^{N} k(card(A_k)) = \sum_{k=1}^{N} k(E(\frac{n}{p^k}) - E(\frac{n}{p^{k+1}}))$

Cette partie est peut-être un peu dure à comprendre. Dans ces cas là, comme d'habitude, il faut faire une pause et jouer avec les entités manipulées en prenant des exemples :

Exemple :

Prenons n=137. Considérons l'ensemble {1,2,3…136,137}, prenons p = 3.

Il y a $E(\frac{137}{3}) = 45$ multiples de 3 : 3, 6, 9, 12…142, 145,

$v_p(l)$ est l'exposant de p dans la décomposition en facteurs premiers de l. Donc pour $l = 4$, $v_3(4) = 0$ comme pour tous les l qui ne sont pas multiples de 3.
Pour les multiples de 3
$6 = 2 \times 3$, $v_3(6) = 1$; $9 = 3^2$ donc $v_3(9) = 2$, $v_3(12) = 1$ car $12 = 2^2 \times 3$.

On comprend mieux la formule $E(\frac{n}{p^k}) - E(\frac{n}{p^{k+1}})$
car on ne s'intéresse pour $v_3(k)$ qu'au nombre dont l'exposant est k et pas aux nombres à exposants supérieurs.
$A_3 = \{l \in \{1\ldots 137\}, v_3(l) = 3\}$ contient donc tous les nombres entre 1 et 137 qui incluent $3^3 = 27$ dans leur décomposition en facteurs premiers mais pas 3^4
Donc $A_3 = \{l \in \{1\ldots 137\}, v_3(l) = 3\} = \{27, 54, 108, 135\}$
, Le cardinal est 4. La formule vue plus haut donne.
$card(A_3) = E(\frac{137}{3^3}) - E(\frac{131}{3^4}) = 5 - 1 = 4$. Banco !
$A_2 = \{l \in \{1\ldots 137\}, v_3(l) = 2\} = \{9, 18, 36, 45, 63, 72, 90, 99, 126\}$
$card(A_2) = E(\frac{137}{3^2}) - E(\frac{131}{3^3}) = 14 - 5 = 9$.
Super-Banco ! De même
$A_4 = \{l \in \{1\ldots 137\}, v_3(l) = 4\} = \{81\}$
et

$A_5 = \{l \in \{1\ldots 137\}, v_3(l) = 5\} = \{\}$

car $3^5 = 243 > 137$, Voilà pourquoi on peut s'arrêter à

N tel que $3^N > 137$

On a donc bien dans les cas vus ci-dessus

$$\sum_{l=1}^{137} v_3(l) = v_3(1) + \ldots + v_3(137)$$

Que l'on calcule en regroupant les valeurs de k

$$\sum_{l=1}^{137} v_3(l) = 1(card(A_1)) + 2(card(A_2)) + 3(card(A_3)) + 4(card(A_4)) + 0$$

$$= \sum_{k=1}^{5} k(card(A_k)) = \sum_{k=1}^{5} k(E(\frac{137}{3^k}) - E(\frac{137}{3^{k+1}})$$

Continuez à jouer avec des exemples, jusqu'à temps que la formule vous paraisse évidente. Pour les génies comme Legendre, la formule s'impose à leur esprit sans passer par des exemples. Dans mon cas, je dois avouer que des exemples et plusieurs lectures de la formule ont été nécessaires pour m'approprier cette démonstration et apprécier son élégance. Je suis émerveillé par l'intuition et l'intelligence de ceux qui voient la formule sans ou avec peu d'exemples.

Revenons à nos moutons : Il suffit maintenant de distribuer k et de jouer avec les valeurs des sommes avec une petite astuce en introduisant (k-1).

$$v_p(n!) = \sum_{k=1}^{N} k(E(\frac{n}{p^k}) - E(\frac{n}{p^{k+1}})) = \sum_{k=1}^{N} kE(\frac{n}{p^k}) - \sum_{k=1}^{N} kE(\frac{n}{p^{k+1}})$$

$$= \sum_{k=1}^{N} kE(\frac{n}{p^k}) - \sum_{k=2}^{N+1} (k-1)E(\frac{n}{p^k})$$

Si ses signes de sommes tels que $\sum_{k=1}^{N}$ obscurcissent le raisonnement. Rappelez vous que vous pouvez toujours les développer en utilisant “+...+” pour représenter les facteurs intermédiaires de la somme. Par exemple :

$$= E(\frac{n}{p^1}) + 2E(\frac{n}{p^2}) + \ldots + NE(\frac{n}{p^N}) - E(\frac{n}{p^2}) - 2E(\frac{n}{p^3}) - \ldots - NE(\frac{n}{p^{N+1}})$$

en regroupant les puissance de p identiques, on obtient :

$$= E(\frac{n}{p^1}) + (2E(\frac{n}{p^2}) - E(\frac{n}{p^2})) + (3E(\frac{n}{p^3}) - 2E(\frac{n}{p^3})) + \ldots + NE(\frac{n}{p^{N+1}})$$

$$= E(\frac{n}{p^1}) + E(\frac{n}{p^2}) + E(\frac{n}{p^3}) + \ldots + NE(\frac{n}{p^{N+1}})$$

On repasse au signe de sommes $\sum_{k=1}^{N}$ pour la beauté de la conclusion

$$= \sum_{k=1}^{N} E(\frac{n}{p^k}) - NE(\frac{n}{p^{N+1}})$$

$$= \sum_{k=1}^{N} E(\frac{n}{p^k}) \text{ car } E(\frac{n}{p^{N+1}}) = 0 \text{ CQFD}$$

Et voilà vous avez suivi du début à la fin, votre première démonstration complexe. Bravo. N’hésitez pas à revenir dessus.

Postulat de Bertrand

Le postulat lui -même est facile à comprendre. Pour tout entier naturel, il existe un nombre premier entre cet entier et son double.

Pour tout entier n supérieur à 2, il existe un nombre premier entre n et 2n.
$\forall n \in N / n \geq 2, \exists\, p\, premier / \, n < \ p \ < \ 2 \times n$

Bertrand l'a énoncé en 1845 et vérifié lui-même pour les nombres jusqu'à 2 millions. A cette époque il n'y avait pas d'ordinateur, il a dû faire tous les calculs à la main ce qui prend plusieurs semaines !
Mais il n'a pas trouvé de démonstration. C'est pourquoi, cet énoncé a été appelé postulat de Bertrand. On aurait pu dire conjecture de Bertrand, avant la première démonstration due à Pafnouti Tchebychev en 1850, soit 5 ans après. Une démonstration plus simple fut trouvée par Ramanujan en 1932. Ce sont des démonstrations dites *transcendantes* car elle utilisent des outils mathématiques, basés sur l'analyse des nombres complexe, pour encadrer les nombres premiers. Dans ces méthodes on cherche 2 nombres, l'un inférieur au nombre premier qui suit n, l'autre supérieur à ce nombre premier. On montre que ces 2 nombres sont compris

entre n et 2n. Cela s'appelle un encadrement. On encadre le nombre premier p par 2 nombres. Ces 2 nombres étant compris entre n et 2n, on en déduit, que le nombre premier p encadré, est aussi compris entre n et 2n. On peut trouver un exemple dans [17].

Paul Erdös (1913-1996) a trouvé une démonstration qualifiée d'*élémentaire* car elle est basée sur l'arithmétique. Elémentaire ne veut pas dire simple. Si vous peinez, n'oubliez pas que Bertrand ne l'a pas démontré ! Pourtant il était loin d'être mauvais ! Il a fallu 6 ans à Tchebychev pour la première démonstration. 70 ans après Ramanujan, un des plus grands génies des mathématiques, doué d'une intuition exceptionnelle, propose une seconde démonstration plus élégante. C'est seulement 100 ans après que Erdös finit par trouver une démonstration dite élémentaire. Il est intéressant de voir qu'une recherche de l'esthétisme a amené des générations de mathématiciens à travailler sur un énoncé déjà démontré pour trouver une méthode de démonstration plus élégante. La démonstration qui vient est basée sur l'excellente démonstration proposée par wikipedia [18]. Son énoncé est dense, il faut de la pratique pour la comprendre.

Cette démonstration est un peu l'Everest de ce livre. Si vous avez lu le texte jusqu'ici et si le sujet vous intéresse, vous y arriverez. Si vous peinez, pas de problème, la démonstration est difficile. C'est la

pédagogie du livre qu'il faut remettre en cause pas vos compétences !

Avant d'attaquer l'Everest, nous allons remplir notre sac à dos des outils nécessaires :

- La notion de décomposition en facteurs premiers d'un nombre entier.
- Les notions de sommes et de produits de nombres entiers : $\prod_{k=1}^{n} p_i$ pour n produits de p_i : $p_1 \times p_2 \times \ldots \times p_n$ et $\sum_{i=1}^{n} p_i$ pour la somme de n p_i .: $p_1 + p_2 + \ldots + p_n$
- Les notions de coefficients binomiaux et de triangle de Pascal : $C(n, m)\ et$ $\sum_{k=0}^{n} C(n,k) x^k y^{n-k} = (x + y)^n$
- Les notions de partie entière et partie décimale d'un nombre rationnel : E(x) et D(x).
- Les notions de logarithmes.

Revoyez ces notions dans la section notions de base, notations et syntaxe et dans les annexes : triangle de Pascal, les parties entières et les logarithmes.

Nous n'allons pas détailler la démonstration dans les pages qui suivent. Les nombreuses étapes et calculs sont expliqués dans les annexes. Nous allons revoir les grandes étapes afin de montrer la créativité et l'élégance de la démonstration sans se perdre dans la complexité des calculs.

Prêt ?

Préliminaires.

L'idée de Erdös est de trouver une formule liant une valeur fixe et un produit de facteurs dont l'un des facteurs dépend du nombre de nombres premiers entre n et 2n :

$N = P_1 \times P_2 \times P_3 \times P_4$ avec $P_4 > 1$ si il y a au moins un nombre premier entre n et 2n.

Pour cela il va d'abord fixer N et ensuite majorer (trouver des bornes supérieures) à P_1, P_2, P_3 . Appelons ces bornes supérieures M_1, M_2, M_3 ainsi si $\frac{N}{M_1 \times M_2 \times M_3} > 1$, il aura démontrer que $P_4 > 1$.

Imaginons que vous devez diviser un sac de 25 pommes en 4 parts

P_1, P_2, P_3, P_4 si vous savez que P_1, P_2, P_3 sont tous strictement inférieurs à 8 vous savez que la part P_4 contient au moins une pomme.

Il faut d'abord trouver ce N. Pour cela Erdös se sert d'un théorème intermédiaire.. Comme il n'a d'importance que pour cette démonstration. On l'appelle un lemme comme dans le cas de la démonstration de la formule de Legendre.

Le lemme que nous voulons démontrer est le suivant :

Erdös définit la fonction θ

$$\theta(x) = \sum_{p \in P, p=2}^{x} ln(p)$$

La formule ci-dessus indique que l'on effectue la somme de tous les logarithmes des nombres premiers p inférieurs à x.

Le lemme s'énonce :

$$\forall n \in N,\ n \geq 1 \Rightarrow \theta(n) < n \times ln(4)$$

Nous appelons ce type de lemme une majoration de fonction. Nous cherchons une formule qui pour tout n

sera toujours supérieur à $\Theta(n)$. La formule proposée par Erdös est : $n \times ln(4)$

Démonstration du lemme

Voir en annexe

Démonstration du Postulat

Vous avez lu l'annexe, vous voila bien échauffé, pas de risque de surchauffe des neurones. Nous pouvons maintenant revenir à la démonstration du postulat de Bertrand.

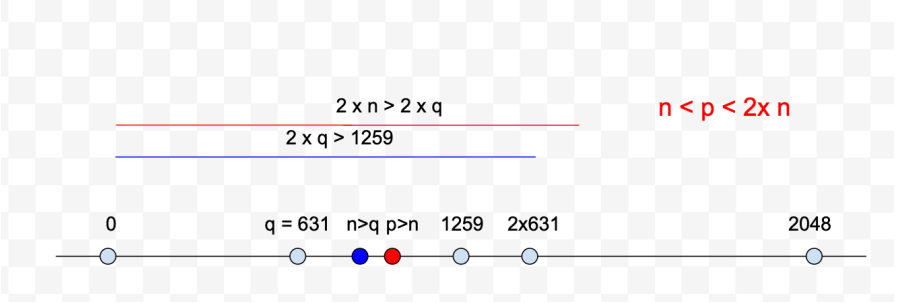
Nous allons différencier 2 cas, le cas n $\leq$ 2048 et n > 2048.

n $\leq$ 2048

Cette étape est nécessaire avant d'attaquer la méthode passant par la majoration de facteurs. Vous allez comprendre pourquoi à la fin. Patience !
Considérons la suite de nombres premiers
3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259 et 2503
Vous remarquerez que chacun des nombres de cette suite est strictement inférieur au double de son prédécesseur. 83 par exemple est inférieur au double de 43.

Soit un nombre entier naturel n tel que $n \leq 2048$, donc n est inférieur à 2503. Montrons que tout nombre premier p qui suit immédiatement n est inférieur à $2 \times n$
Si p = 3 alors n = 2 et le théorème est vrai car 2 < 3 < 4.
Il y a bien un nombre premier entre n et 2n.
Si $p \neq 3$ considérons q le nombre de la suite qui précède p : $q \leq n$ car p est le plus petit nombre premier qui suit n.
Si $q \leq n$ alors $2q \leq 2n$.
Par construction de la liste p < 2q donc p < 2n.

Par exemple : prenons n = 135, p vaut 163 et q vaut 83. 2q vaut 166 qui est bien supérieur à 163.
Pour n compris entre 631 et 1259, on peut représenter la relation sous cette forme graphique.



Nous avons donc démontré n < p < 2n. Le théorème est vrai jusqu'à n = 2048. Attaquons nous maintenant au cas général.

n > 2048

Par la formule du binôme de Newton, nous avons

$$4^n = (1 + 1)^{2n} = \sum_{k=1}^{2n-1} C(2n, k)$$

Le coefficient binomial C(2n,n) est le plus grand de cette somme. On peut démontrer qu'il est supérieur à la moyenne de tous les coefficients de la somme. La démonstration se fait par récurrence. Si vous êtes arrivés jusque là, elle est à votre portée.

Donc $C(2n, n) \geq \frac{4^n}{2n}$

Appelons R(p,n) le plus grand nombre x tel que p^x| C(2n,n). On en déduit que la décomposition en nombres premiers de C(2n,n) est

$$C(2n, n) = \prod_{p \in P} p^{R(p,n)}$$

Erdös décompose ce produit en 4 produits.

$$\frac{4^n}{2n} \leq C(2n, n) = \prod_{p \in P} p^{R(p,n)} = P_1 P_2 P_3 P_4$$

Chaque P_i correspond à un intervalle différent pour p :

$$P_1 = \prod_{p \in P, p \leq \sqrt{2n}} p^{R(p,n)}$$

$$P_2 = \prod_{p \in P \sqrt{2n} < p \leq \frac{2n}{3}} p^{R(p,n)}$$

$$P_3 = \prod_{p\in P, \frac{2n}{3}<p\leq n} p^{R(p,n)}$$

$$P_4 = \prod_{p\in P, n<p<2n} p^{R(p,n)}$$

Pourquoi introduire ces 4 facteurs dans la décomposition en nombre premiers de C(2n,n) ?
C'est la formule que Erdös va utiliser, car P_4 dépend de l'existence d"un nombre premier entre n et 2n. Malin !

Erdös va utiliser ce produit pour minorer P_4.
Pour minorer P_4, Il majore P_1, $P_2 et\ P_3$
Pour cela, Il faut calculer les R(p,n).

Rappelons la formule de Legendre (voir plus haut) qui donne le nombre $x = v_p(n!) = R(p,n)$ qui est l'exposant de p dans la décomposition en facteurs premiers de n!. Donc le plus grand entier x tel que p^x| n! est R(p,n)

$$R(p,n) = E(\frac{n}{p}) + E(\frac{n}{p^2}) + E(\frac{n}{p^3}) + \ldots = \sum_{k=1}^{\infty} E(\frac{n}{p^k})$$

On démontre que $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$.
Or $C(2n,n) = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{2\times n!}$

on en déduit

$$v_p(C(2n,n)) = R(p,n) = v_p((2n)!) - 2 \times v_p(n!)$$

$$= \sum_{k=1}^{\infty} E\left(\frac{2n}{p^k}\right) - 2 \sum_{k=1}^{\infty} E\left(\frac{n}{p^k}\right) = \sum_{k=1}^{\infty} E\left(\frac{2n}{p^k}\right) - 2E\left(\frac{n}{p^k}\right)$$

Majoration de P_1

$$P_1 = \prod_{p \in P, 2 \leq p \leq \sqrt{2n}} p^{R(p,n)}$$

On peut démontrer que

$$P_1 \leq (2n)^{\sqrt{2n}}$$

Voir la démonstration en annexe.

Majoration de P_2

$$P_2 = \prod_{p \in P \sqrt{2n} < p \leq \frac{2n}{3}} p^{R(p,n)}$$

On en déduit que :

$$P_2 < 4^{\frac{2n}{3}}$$

Nous avons donc bien majoré P_2. La démonstration est en annexe.

Majoration de P_3

$$P_3 = \prod_{p\in P,\frac{2n}{3}<p\leq n} p^{R(p,n)}$$

En fait $P_3 = 1$, c'est le point clé et illustre l'intelligence de Erdös.

En effet nous avons vu que

R(p,n) = $E(\frac{2n}{p}) - 2E(\frac{n}{p})$ dans le cas ou $\frac{2n}{3} < p \leq n$

on en déduit

$E(\frac{2n}{p}) - 2E(\frac{n}{p}) \leq 2 - 2 = 0$

Donc $P_3 = p^0 = 1$

Minoration de P_4

Nous pouvons maintenant minorer P_4

$$\frac{4^n}{2n} \leq P_1P_2P_3P_4 \Rightarrow 4^n < 2n\,2n^{\sqrt{2n}}4^{\frac{2n}{3}}1\,P_4 = 2n^{1+\sqrt{2n}}4^{\frac{2n}{3}}P_4$$

On en déduit

$$P_4 > \frac{4^n}{2n^{1+\sqrt{2n}}4^{\frac{2n}{3}}} = \frac{4^n4^{\frac{-20}{3}}}{2n^{1+\sqrt{2n}}} = \frac{4^{\frac{-20}{3}+n}}{2n^{1+\sqrt{2n}}} = \frac{4^{\frac{n}{3}}}{2n^{1+\sqrt{2n}}}$$

Astuce : on pose $2n = 2^{2t}$ et comme d'habitude on prend le logarithme pour transformer les divisions en soustractions et multiplications en additions.

$ln(P_4) > ln(\frac{4^{\frac{n}{3}}}{2n^{1+\sqrt{2n}}}) = ln(4^{\frac{n}{3}}) - ln(2n^{1+\sqrt{2n}}) =$

$= \frac{n}{3}ln(4) - (1+\sqrt{2n})ln(2n)$

$= \frac{2^{2t}}{6}ln(4) - (1+2^t)\,2t\,ln(2)$

Après quelques factorisations laborieuses on obtient :

$= \frac{t2^t ln(2)}{3}(\frac{2^t}{t} - 6(1+2^{-t}))$ (1)

Rappelons nous que nous voulons minorer P_4.

Afin de prouver que $P_4 > 1$, et qu' il y a donc un nombre premier entre n et 2n. Il suffit pour cela de montrer que $\frac{2^t}{t} - 6(1+2^{-t}) > 0$

or $n > 2048$ donc $2n > 1024$ et 1024 = 2^{10}

Donc $2^{2t} > 2^{10}$ donc $t > 5$

Donc $\frac{2^t}{t} > \frac{2^5}{5} > 6(1+2^{-5}) > 6(1+2^{-t})$

Donc (1) = $A \times B$ avec $A > 0$ et $B > 0$

Donc $ln(P_4) > 0 \Rightarrow P_4 > 1$

Rappelons nous que

$$P_4 = \prod_{p\in P, n<p<2n} p^{R(p,n)}$$

CQFD Ouf !

Il y a donc bien un nombre premier p entre n et 2n.

SI vous avez compris chaque étape de cette démonstration, même si vous n”êtes pas capable de la reproduire sur une page blanche, bravo !!! C’était votre Everest, c’est aussi le mien. Il m’a fallu plus de 15 jours pour la comprendre suffisamment afin de la détailler et de l’expliquer dans l’annexe.

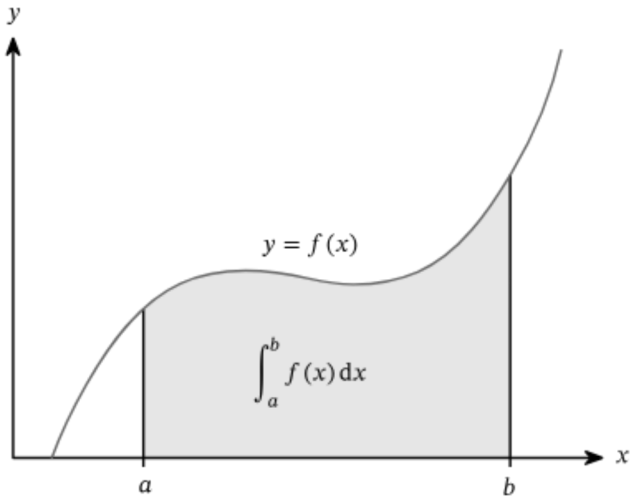
Nous voilà arrivés au terme de cette balade dans le pays des nombres premiers. Durant cette randonnée qui est partie des plaines des notions de base, a traversé les collines des énoncés des théorèmes avant de gravir les cols des démonstrations, vous avez pu découvrir ou re-découvrir le monde de l'arithmétique mais l'objectif principal de cet ouvrage était de vous initier à la méthode mathématique. Mao disait « Donnez un poisson à un homme et vous le nourrissez pour un jour ; apprenez-lui à pêcher et vous le nourrirez toute sa vie. ». C'est humblement le but de ce livre : vous donner les bases, les outils et surtout l'envie de vous nourrir toute votre vie de la beauté du monde mathématique. J'ai choisi l'arithmétique et les nombres premiers car c'est un domaine abordable avec un niveau de mathématique du niveau terminale et qu'un lecteur attentif peut atteindre l'état de l'art dans le domaine. Il est possible de résumer en 200 pages, 2000 ans de recherches et de découvertes des mathématiciens. Il y a peu de domaines scientifiques qui possèdent cette propriété. Si on avait choisi l'analyse complexe ou la géométrie, cela aurait nécessité les dizaines de livres remplies de formules qu'étudient les étudiants en mathématiques et des années d'apprentissage. Et encore nous n'aurions pas atteint l'état de l'art mais difficilement le niveau d'un étudiant en master de mathématique. Toutefois, si ce plongeon dans l'abstraction vous a plu, vous pouvez vous lancer dans l'étude de sous-domaines des

mathématiques comme la théorie des groupes, la géométrie algébrique ou la théorie des ensembles. La mathématique est un vaste continent divisé parfois de manière arbitraire, en de nombreuses régions aux frontières mal définies dans lesquelles vous pourrez randonner grâce aux notions de base abordées dans ce livre.

Annexes

Intégrale

Considérons une fonction f(x) qui associe un nombre réel y à un nombre réel x. On suppose que f est définie et continue sur un intervalle [a,b]. Cela veut dire, en résumant grossièrement, que l'on peut tracer la courbe de f entre a et b sans lever le crayon.

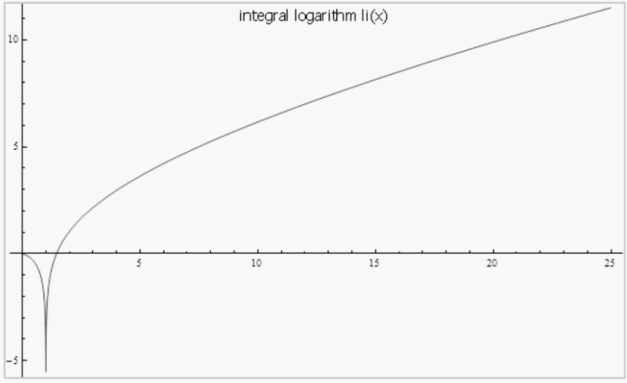


$\int_a^b f(x)dx$ est égal à l'aire en gris sur le graphique.

On définit le logarithme intégrale pour tout nombre réel strictement positif différent de 1 de la manière suivante :

$$li(x) : \int_0^x \frac{dt}{ln(t)}$$

Sa courbe est :



Courbe du logarithme intégral.

Puissance modulaire

L'algorithme RSA utilise l'algorithme d'exponentiation rapide. Cet algorithme permet de calculer rapidement par ordinateur la puissance modulaire d'un nombre.

La puissance modulaire consiste à élever un nombre a à la puissance e et de calculer le résultat c modulo m

$c = a^{e} \ (mod\ m)$

La méthode simpliste consiste à effectuer e multiplications de a par lui même et à utiliser la division euclidienne pour calculer le reste de ces multiplications par m.

Par exemple : $3^{5} \ (mod\ 7)$
On calcule :
$3^{5} = 3 \times 3 \times 3 \times 3 \times 3 = 9 \times 9 \times 3 = 243$
Ensuite on calcule $243 \ (mod\ 7)$. Rappelez vous c'est le reste du plus grand multiple de 7 inférieur à 243. Il suffit donc de diviser 243 par 7 jusqu'à trouver un reste inférieur à 7.
$243 \div 7 = 34 \times 7 + 5$ donc $243 = 5\ mod(7)$
Donc $3^{5} \ (mod\ 7) = 5$

Pour les grands nombres (1000 chiffres) cet algorithme prend trop de temps de calcul (des années) :
On préfère utiliser l'exponentiation rapide basé sur un algorithme récursif [19]:

Pour calculer x^n ,on écrit n en base 2. Pourquoi la base 2, car c'est la base utilisée par les ordinateurs. Le nombre n est ainsi décomposé en puissance de 2

$$n = \sum_{k=0}^{d} a_k \, 2^k \; avec \; a_k \in \{0, 1\} \quad (1)$$

Par exemple pour $n = 5$ on obtient

$$5 = 4 + 1 = 2^2 + 1 = 2^2 + 0 \times 2^1 + 1 \times 2^0$$

donc 5 = 101 en base 2.

Revenons à la formule 1, nous savons que

$x^{b+c} = x^b \times x^c$ et $x^{bc} = x^{b^c}$

En appliquant la formule à la décomposition en base 2 de n
La formule (1) exprime n sous la forme d"une somme :

$$n = a_0 2^0 + a_1 2^1 + a_2 2^2 + \ldots + a_d 2^d$$

Donc

$$x^n = x^{a_0 2^0 + a_1 2^1 + a_2 2^2 + \ldots + a_d 2^d} = x a^0 (x^{a_1 2^1})(x^{a_2 2^2}) \ldots (x^{a_d 2^d})$$

Donc $x^n = xa^0 (x^{2^1})^{a_1} (x^{2^2})^{a_2} \dots (x^{2^d})^{a_d}$

d qui apparait dans $x = \sum_{k=0}^{d} a_k 2^k$ est le nombre de bits de n en base 2. Il dépend de la valeur de $\frac{ln(n)}{ln(2)}$. Une valeur qui croît beaucoup moins vite que n. Il faut d multiplications pour calculer chaque $(x^{2^i})^{a_i}$ et d multiplications supplémentaires pour faire le produit des multiplications intermédiaires. On a en tout 2d multiplications à effectuer. Donc le nombre de multiplications dépend de ln(n) et non pas de n ! Ce qui réduit considérablement le temps de calcul pour les grandes valeurs de n.

Pour les informaticiens qui lisent cette annexe, l'algorithme est utilisé dans de nombreux calculs sur les grands nombres. Il est implémenté de manière récursive grâce à l'astuce suivante :

si n est pair on calcule $x^n = (x^2)^{n/2}$, il suffit alors de calculer

$y^{\frac{n}{2}}$ pour $y = x^2$

si n est impair on calcule $x^n = x(x^2)^{(n-1)/2}$ il suffit alors de calculer
$y^{\frac{n-1}{2}}$ pour $y = x^2$ et de multiplier par x.

On obtient ainsi un algorithme récursif
$puissance(x, n) = si\ (n = 0) : 1\ sinon\ si\ n\ est\ pair$: $puissance(x^2, \frac{n}{2})$ sinon $x \times puissance(x^2, \frac{n-1}{2}))$

On peut ainsi utiliser cet algorithme avec des nombres premiers de 1024 ou 2048 bits, dont le produit est impossible à factoriser avec les ordinateurs actuels.

La combinatoire et les coefficients polynomiaux.

Nous avons aussi besoin dans la partie démonstration de notions de base de combinatoire. La combinatoire est un domaine des mathématiques très utilisé en calcul des probabilités car elle permet de calculer le nombre de combinaisons possibles de p éléments dans un ensemble de n éléments, noté C(n,p)

Par exemple, vous avez une équipe de 10 joueurs de basket, vous ne pouvez en faire jouer sur le terrain que 5

à la fois, C(10,5) est le nombre de combinaisons possibles. On montre que

$$C(n,p) = \frac{n!}{p!(n-p)!}$$

Donc $C(10,5) = \frac{10!}{5!(10-5)!} = \frac{10!}{5!\times 5!} = \frac{10\times 9\times 8\times 7\times 6}{5\times 4\times 3\times 2}$
$= 2 \times 3 \times 2 \times 7 \times 3 = 252$

Il y a 252 groupes de 5 joueurs distincts parmis les 10 joueurs. Respect à l'entraineur !
On remarquera que choisir p éléments parmis n revient à choisir les (n-p) éléments qu'on laisse de côté (les joueurs sur le banc). Donc

C(n,p) = C(n, n-p)

De même Pascal (1623-1662) a démontré une formule qui porte son nom qui permet de calculer C(n,p) par itération :

C(n,k) = C(n-1,k-1) + C(n-1,k)

Cette formule permet de représenter les C(n,p) sous forme d'un tableau indexé par n et p. Ce tableau peut être construit à l'aide de cette égalité.

n\k	0	1	2	3	4	…
1	1	1				…
2	1	2	1			…
3	1	3	3	1		…
4	1	4	6	4	1	…
…	…	…	…	…	…	…

Newton (1642-1727) plus tard a démontré que C(n,p) permettait de calculer les coefficients du polynôme obtenu en élevant $x + y$ à la puissance n.

Formule du Binôme de Newton :

$$\sum_{k=0}^{n} C(n,k) x^{k} y^{n-k} = (x + y)^{n}$$

Par exemple

$(x + y)^{4} = x^{4} + 4x^{3}y + 6x^{2}y^{2} + 4xy^{3} + y^{4}$

Coefficient que l'on peut déduire du triangle de Pascal ci-dessus.

La partie entière et la partie décimale d'un nombre rationnel.

Soit x un nombre rationnel positif,

$x \in Q^+ \Rightarrow \exists p, q \in Z / x = \frac{p}{q}$

On appelle partie entière de x, la fonction que l'on note E(x) qui fait correspondre à x le plus grand entier naturel inférieur ou égal à x.

$$E(x) = n / n \in N \; et \; n \leq x < n + 1$$

Cela paraît compliqué mais quand on écrit le nombre sous sa forme décimale, il s'agit simplement du nombre à gauche de la virgule. Par exemple si $x = 3,456$ alors $E(x) = 3$.

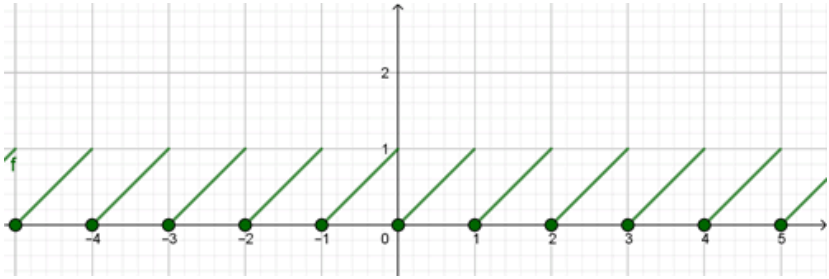
$D(x) = x - E(x)$ est la partie décimale de x.
C'est-à-dire le nombre constitué de 0 à gauche de la virgule et des décimales de x à droite de la virgule.
si $x = 3,456$ alors $D(x) = 0,456$

On remarque $\forall x \in Q^+, \; D(x) < 1$.
Et que $E(x + y) \leq E(x) + E(y)$
On a démontré dans le chapître démonstration :

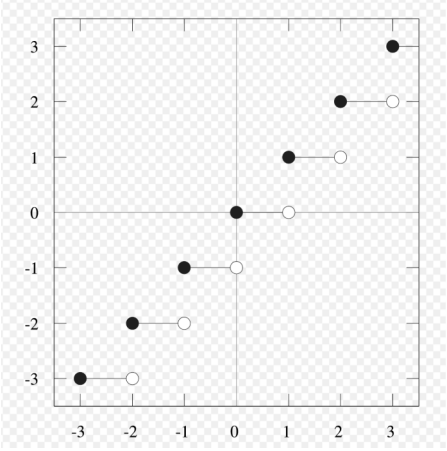
$E(2x) - E(x) = 0 \; si \; D(x) < \frac{1}{2}$

$E(2x) - E(x) = 1 \; si \; D(x) \geq \frac{1}{2}$

Le graphe de la fonctions D(x) est :



Et pour E(x)



Vous comprenez pourquoi on appelle ces fonctions, des fonctions en escalier et fonctions en dents de scie.

Démonstration détaillée du Postulat de Bertrand

Nous avons vu les grandes étapes dans la partie démonstration. Reprenons le texte en détaillant les démonstrations de chaque étape. Désolé pour les répétitions, mais cela vous évitera de tourner les pages du livre en sens inverse pour retrouver la suite des étapes.

Préliminaires.

L'idée de Erdös est de trouver une formule liant une valeur fixe et un produit de facteurs dont l'un des facteurs dépend du nombre de nombres premiers entre n et 2n :

$N = P_1 \times P_2 \times P_3 \times P_4$ avec $P_4 > 1$ si il y a au moins un nombre premier entre n et 2n.

Pour cela il va d'abord fixer N et ensuite majorer (trouver des bornes supérieures) P_1, P_2, P_3 . Appelons ces bornes supérieures M_1, M_2, M_3 ainsi si $\frac{N}{M_1 \times M_2 \times M_3} > 1$, il aura démontrer que $P_4 > 1$.

Le lemme que nous voulons démontrer est le suivant :

Erdös définit la fonction

$$\theta(x) = \sum_{p \in P, p=2}^{x} ln(p)$$

La formule ci-dessus indique que l'on effectue la somme de tous les logarithmes népériens des nombres premiers p inférieurs à x.

Le lemme s'énonce :
$\forall n \in N,\ n \geq 1 \Rightarrow \theta(n) < n \times ln(4)$

Démonstration du lemme

Nous allons utiliser une démonstration par récurrence (voir plus haut la section "Typologie de la démonstration").

- Initialisons la récurrence avec n = 1.

$\Theta(1) = \sum_{p \in P, p=2}^{1} ln(p) = 0$:

Car la somme débute pour p = 2. Donc $\Theta(1) < 1 \times ln(4)$

- Regardons maintenant n = 2.

$\Theta(2) = ln(2)$, en effet 2 est le seul nombre premier entre 2 et 2.

Comme $2 < 4 \times ln(2)$, le lemme est vrai pour n = 2

- Considérons maintenant n > 2 et n pair

Par hypothèse de récurrence, nous considérons que le lemme est vrai pour (n-1) et nous allons essayer de prouver qu'il est vrai pour n.

Si n est pair il n'est pas premier donc $\Theta(n) = \Theta(n-1)$, n étant pair il n'est pas premier et ne fait pas partie de la somme

$$\sum_{p \in P, p=2}^{n} ln(p)$$

Le lemme est vrai pour n - 1 par hypothèse de récurrence.
Donc $\Theta(n-1) < 4 \times ln(n-1)$

le logarithme népérien étant une fonction croissante
$ln(n-1) < ln(n)$

On peut en déduire
$\Theta(n) = \Theta(n-1) < 4 \times ln(n-1) < 4 \times ln(n)$

- Considérons maintenant le cas plus délicat où n est impair et supérieur à 2.

Il est temps maintenant de se référer à la combinatoire et les formules de Pascal que nous avons vu précédemment.
Si n est impair alors $\exists m \in N / n = 2m + 1$ (définition d'un nombre impair).

$$4^m = 2^{2^m} = 2^{2m} = \frac{2^{2m+1}}{2} = \frac{(1+1)^{2m+1}}{2}$$

$$= \frac{\sum_{k=0}^{2m+1} C(2m+1,k)}{2}$$

$$= \frac{X+C(2m+1,m)+C(2m+1,m+1)+Y}{2}$$

Nous avons choisi d'appeler X et Y les premiers et derniers termes de la somme. Or

$$C(2m + 1, m) = \frac{(2m+1)!}{m!(2m+1-m)!} = \frac{(2m+1)!}{m!(m+1)!}$$

et

$$C(2m + 1, m + 1) = \frac{(2m+1)!}{(m+1)!(2m+1-(m+1))!} = \frac{(2m+1)!}{(m+1)!m!}$$

Nous trouvons les mêmes expressions.
donc

$$C(2m + 1, m) + C(2m + 1, m + 1) = 2 \times C(2m + 1, m))$$

donc $\frac{X+C(2m+1,m)+C(2m+1,m+1)+Y}{2} = \frac{X+Y}{2} + C(2m + 1, m)$

X et Y étant positif et supérieur à 0, $\frac{X+Y}{2} > 0$

donc $4^m \geq C(2m + 1, m)$

On a prouvé $4^m \geq C(2m + 1, m)$

Considérons les nombres premiers entre m+1 et 2m+1

$p_i \in P \; et \; m + 1 < p_i < 2m + 1 \Rightarrow p_i \mid C(2m + 1, m)$

Nous sommes sûrs qu'il y en a au moins m par hypothèse de récurrence car m est strictement inférieur à n.

$C(2m + 1, m) = \frac{(2m+1)\times 2m\times \ldots \times m\times \ldots \times 1}{m!(m+1)!}$ (le produit en numérateur contient chaque p_i, tel que $m + 1 < p_i < 2m + 1$).

On peut donc écrire $C((2m + 1, m))$ sous la forme

$$C(2m + 1, m) = \prod_{m+1<p_i<2m+1} p_i \times \frac{A\times(m+1)!}{m!(m+1)!}$$

En posant A = $\frac{(2m+1-(m+1)!}{\prod_{m+1<p_i<2m+1} p_i}$, le produit de tous les nombres non premiers de (m+1) à (2m+1), on obtient la formule :

$$C(2m + 1, m) = \prod_{m+1<p_i<2m+1} p_i \times \frac{A}{m!}$$

on en déduit

$$ln(C(2m + 1, m)) = \sum_{m+1<p_i<2m+1} ln(p_i) + ln(\frac{A}{m!})$$

Rappelez vous le logarithme d'un produit est une somme.

en posant $ln(\frac{A}{m!}) > 0$ car tout logarithme d'un nombre positif est strictement positif.

On voit que $\sum_{m+1<p_i<2m+1} ln(p_i) \leq ln(C(2m+1,m))$

donc

$$\Theta(2m+1) - \Theta(m+1) = \sum_{m+1<p_i<2m+1} ln(p_i) \leq ln(C(2m+1,m))$$

On a vu plus haut que $4^m \geq C(2m+1,m)$

$\Rightarrow ln(4^m) \geq \Theta(2m+1) - \Theta(m+1)$

$\Rightarrow m\,ln(4) \geq \Theta(2m+1) - \Theta(m+1)$

$\Rightarrow m\,ln(4) + \Theta(m+1) \geq \Theta(2m+1)$ (2)

or par hypothèse d'induction

$m+1 < n \Rightarrow \Theta(m+1) \leq (m+1)ln(4)$

Donc

(2) $\Rightarrow m\,ln(4) + (m+1)ln(4) \geq \Theta(2m+1)$

En mettant ln(4) en facteur dans le membre de gauche.

$\Rightarrow (2m+1)\,ln(4) \geq \Theta(2m+1)$

$\Rightarrow \Theta(2m+1) \leq (2m+1)\,ln(4)$

En remplaçant 2m+1 par n.

$\Rightarrow \Theta(n) \leq nln(4)$

(CQFD)

Démonstration du Postulat

Nous pouvons maintenant revenir à la démonstration du postulat de Bertrand.

Nous allons différencier 2 cas, le cas n ≤ 2048 et n > 2048.

n ≤ 2048

Cette étape est nécessaire avant d'attaquer la méthode passant par la majoration de facteurs. Vous allez comprendre pourquoi à la fin. Patience !
Considérons la suite de nombres premiers
3, 5, 7, 13, 23, 43, 83, 163, 317, 631, 1259 et 2503

Chacun est strictement inférieur au double de son prédécesseur.
83 par exemple est inférieur au double de 43.

$n \leq 2048$, donc n est inférieur à 2503. Donc il existe dans cette suite un plus petit nombre premier p supérieur à n : n < p

- Si p = 3 alors n = 2 et le théorème est vrai car 2 < 3 < 4. Il y a bien un nombre premier entre n et 2n.
- Si $p \neq 3$ considérons q le nombre de la suite qui précède p : $q \leq n$ car p est le plus petit nombre premier qui suit n.

SI $q \leq n$ alors $2q \leq 2n$

Par construction de la liste p < 2q donc p < 2n.

Par exemple : prenons n = 135, p vaut 163 et q vaut 83. 2q vaut 166 qui est bien supérieur à 163.

Nous avons donc démontré n < p < 2n. Le théorème est vrai jusqu'à n=2048. Attaquons nous maintenant au cas général.

n > 2048

Par la formule du binôme de Newton, nous avons

$$4^n = (1 + 1)^{2n} = \sum_{k=1}^{2n-1} C(2n, k)$$

Le coefficient binomial C(2n,n) est le plus grand de cette somme. On peut démontrer qu'il est supérieur à la moyenne de tous les coefficients de la somme : $\frac{4^n}{2n}$.

La démonstration se fait par récurrence. Si vous êtes arrivés jusque là, elle est à votre portée.

Donc $C(2n, n) \geq \frac{4^n}{2n}$

Appelons R(p,n) le plus grand nombre x tel que p^x| C(2n,n). On en déduit que la décomposition en nombres premiers de C(2n,n) est

$$C(2n, n) = \prod_{p \in P} p^{R(p,n)}$$

Erdös décompose ce produit en 4 produits.

$$\frac{4^n}{2n} \leq C(2n,n) = \prod_{p \in P} p^{R(p,n)} = P_1 P_2 P_3 P_4$$

Chaque P_i correspond à un intervalle différent pour p :

$$P_1 = \prod_{p \in P, p \leq \sqrt{2n}} p^{R(p,n)}$$

$$P_2 = \prod_{p \in P \sqrt{2n} < p \leq \frac{2n}{3}} p^{R(p,n)}$$

$$P_3 = \prod_{p \in P, \frac{2n}{3} < p \leq n} p^{R(p,n)}$$

$$P_4 = \prod_{p \in P, n < p < 2n} p^{R(p,n)}$$

Pourquoi introduire ces 4 facteurs dans la décomposition en nombre premiers de C(2n,n) ?
C'est la formule que Erdös va utiliser, car P_4 dépend de l'existence d"un nombre premier entre n et 2n. En effet P_4 est le produit des nombres premiers munis de leurs exposants entre n et 2n. Malin !

Nous allons utiliser ce produit pour minorer P_4.
Pour minorer P_4, nous allons majorer P_1, $P_2 et\ P_3$

Il va falloir pour cela calculer les R(p,n).

Rappelons la formule de Legendre (voir plus haut) qui donne le nombre $x = v_p(n!) = R(p,n)$ qui est l'exposant de p dans la décomposition en facteurs premiers de n!. Donc le plus grand entier x tel que p^x| n! est R(p,n)

$$R(p,n) = E(\frac{n}{p}) + E(\frac{n}{p^2}) + E(\frac{n}{p^3}) + \ldots = \sum_{k=1}^{\infty} E(\frac{n}{p^k})$$

On démontre que $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$.

Or $C(2n,n) = \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{2\times n!}$

on en déduit

$$v_p(C(2n,n)) = R(p,n) = v_p((2n)!) - 2 \times v_p(n!)$$

$$= \sum_{k=1}^{\infty} E(\frac{2n}{p^k}) - 2\sum_{k=1}^{\infty} E(\frac{n}{p^k}) = \sum_{k=1}^{\infty} E(\frac{2n}{p^k}) - 2E(\frac{n}{p^k})$$

Majoration de P_1

$$P_1 = \prod_{p\in P, 2\le p\le\sqrt{2n}} p^{R(p,n)}$$

Chaque terme $E(\frac{2n}{p^k}) - 2E(\frac{n}{p^k})$ vaut soit 0 lorsque $D(\frac{n}{p^k}) < \frac{1}{2}$ soit 1 lorsque $D(\frac{n}{p^k}) \ge \frac{1}{2}$ (voir la section

partie entière et partie décimale dans la section notions de base).

De plus si

$k > E(\frac{ln(2n)}{ln(p)}) \Rightarrow k > \frac{ln(2n)}{ln(p)} \Rightarrow p > \frac{2n}{p^k} \Rightarrow E(\frac{2n}{p^k}) = 0$

De même

$k > E(\frac{ln(2n)}{ln(p)}) \Rightarrow k > \frac{ln(n)}{ln(p)} \Rightarrow p > \frac{n}{p^k} \Rightarrow E(\frac{n}{p^k}) = 0$

Donc lorsque $k > E(\frac{ln(2n)}{ln(p)})$ les termes $E(\frac{2n}{p^k}) - 2E(\frac{n}{p^k})$ valent 0.

En résumé, les termes de la somme $\sum_{k=1}^{\infty} E(\frac{2n}{p^k}) - 2E(\frac{n}{p^k})$ valent soit 0 ou 1 pour $k \leq E(\frac{ln(2n)}{ln(p)})$ et 0 ensuite.

On peut donc en déduire que R(p,n) =

$\sum_{k=1}^{\infty} E(\frac{2n}{p^k}) - 2E(\frac{n}{p^k}) = 1 + 0 + \dots 1 + 0 + 0 + 0 \dots$

Les premiers termes de la somme étant égales soit à 0 ou 1 jusqu'a$E(\frac{ln(2n)}{ln(p)})$ et 0 ensuite. La sommes est donc inférieure à $E(\frac{ln(2n)}{ln(p)})$.

Donc $p^{R(p,n)} \leq p^{E(ln(2n/ln(p))}$

Or

$p = e^{ln(p)} \Rightarrow p^{\frac{ln(2n)}{ln(p)}} = e^{ln(p)^{\frac{ln(2n)}{ln(p)}}} = e^{ln(p)\frac{ln(én)}{ln(p)}} = e^{ln(2n)} = 2n$

Donc

$E(\frac{ln(2n)}{ln(p)}) \leq \frac{ln(2n)}{ln(p)} \Rightarrow p^{E(\frac{ln(2n)}{ln(p)})} \leq p^{\frac{ln(2n)}{ln(p)}} \Rightarrow p^{E(\frac{ln(2n)}{ln(p)})} \leq 2n$

$$P_1 = \prod_{p \in P, p \leq \sqrt{2n}} p^{R(p,n)}$$

Chaque terme du produit est inférieur à $2n$, il y a au plus $\sqrt{2n}$ facteurs dans le produit, donc $P_1 \leq (2n)^{\sqrt{2n}}$

Nous pouvons maintenant nous attaquer à la majoration de P_2

Majoration de P_2

$$P_2 = \prod_{p \in P \sqrt{2n} < p \leq \frac{2n}{3}} p^{R(p,n)}$$

Donc dans le cas $\sqrt{2n} < p$

R(p,n) = $\sum_{k=1}^{\infty} E(\frac{2n}{p^k}) - 2E(\frac{n}{p^k})$

est réduit à son premier terme, k=1, et

R(p,n)= $E(\frac{2n}{p}) - 2E(\frac{n}{p})$

en effet pour k=2, $E(\frac{2n}{p^k}) - 2E(\frac{n}{p^k})$ = 0 car

$p^2 > 2n > n$ donc les parties entières sont nulles.

$E(\frac{2n}{p}) - 2E(\frac{n}{p})$ comme nous l'avons montré plus haut vaut soit 0 ou 1
Donc R(p,n)≤ 1.

$$P_2 = \prod_{p \in P \sqrt{2n} < p \leq \frac{2n}{3}} p$$

Nous allons transformer ce produit en somme grâce au logarithme !

$$ln(P_2) = \sum_{p \in P \sqrt{2n} < p \leq \frac{2n}{3}} ln(p) \leq \sum_{p \in P,\, p=2}^{\frac{2n}{3}} ln(p) = \Theta(\frac{2n}{3})$$

Ce qui nous permet de retomber sur la fonction Θ donc sur le lemme démontré plus haut dont on déduit.

$$\Theta(\frac{2n}{3}) < \frac{2n}{3} ln(4)$$

Nous avons donc

$$ln(P_2) < \frac{2n}{3} \times ln(4)$$

En prenant l'exponentielle du coté gauche et du coté droit de l'inégalité, celle-ci est préservée car la fonction exponentielle toujours positive préserve les inégalités, on obtient :

$$exp(ln(P_2)) < exp(\frac{2n}{3} \times ln(4)) \Rightarrow P_2 < exp(ln(4^{2n/3}))$$

d'où

$P_2 < 4^{2n/3}$, nous avons donc bien majoré P_2

Majoration de P_3

$$P_3 = \prod_{p\in P, \frac{2n}{3}<p\leq n} p^{R(p,n)}$$

En fait $P_3 = 1$, c'est le point clé et illustre l'intelligence de Erdös.

En effet nous avons vu que

R(p,n) = $E(\frac{2n}{p}) - 2E(\frac{n}{p})$ dans le cas ou $\frac{2n}{3} < p \leq n$

on en déduit

$E(\frac{2n}{p}) - 2E(\frac{n}{p}) \leq 2 - 2 = 0$

Donc $P_3 = p^0 = 1$

Nous avons donc majoré P_3

Minoration de P_4

Nous pouvons maintenant minorer P_4

$\frac{4^n}{2n} \leq P_1 P_2 P_3 P_4 \Rightarrow$

$4^n < 2n \times 2n^{\sqrt{2n}} \times 4^{\frac{2n}{3}} \times 1 \times P_4 = 2n^{1+\sqrt{2n}} \times 4^{\frac{2n}{3}} \times P_4$

On en déduit

$$P_4 > \frac{4^n}{2n^{1+\sqrt{2n}} 4^{\frac{2n}{3}}} = \frac{4^n 4^{\frac{-20}{3}}}{2n^{1+\sqrt{2n}}} = \frac{4^{\frac{-20}{3}+n}}{2n^{1+\sqrt{2n}}} = \frac{4^{\frac{n}{3}}}{2n^{1+\sqrt{2n}}}$$

Astuce : on pose $2n = 2^{2t}$ et comme d'habitude on prend le logarithme pour transformer les divisions en soustractions et multiplications en additions.

$ln(P_4) > ln(\frac{4^{\frac{n}{3}}}{2n^{1+\sqrt{2n}}}) = ln(4^{\frac{n}{3}}) - ln(2n^{1+\sqrt{2n}}) =$

$= \frac{n}{3}ln(4) - (1+\sqrt{2n})ln(2n)$

$= \frac{2^{2t}}{6}ln(4) - (1 + 2^t)\,2t\,ln(2)$

Après quelques factorisations laborieuses on obtient :

$= \frac{t2^t ln(2)}{3}(\frac{2^t}{t} - 6(1 + 2^{-t}))$ (1)

Rappelons nous que nous voulons minorer P_4

Afin de prouver que $P_4 > 1$, et qu' il y a un nombre premier entre n et 2n. Il suffit pour cela de montrer que

$\frac{2^t}{t} - 6(1 + 2^{-t}) > 0$

or $n > 2048$ donc $2n > 1024$ et 1024 = 2^{10}

Donc $2^{2t} > 2^{10}$ donc $t > 5$

Donc $\frac{2^t}{t} > \frac{2^5}{5} > 6(1 + 2^{-5}) > 6(1 + 2^{-t})$

Donc (1) $= A \times B$ avec $A > 0$ et $B > 0$

Donc $ln(P_4) > 0 \Rightarrow P_4 > 1$

Rappelons nous que

$$P_4 = \prod_{p \in P, n<p<2n} p^{R(p,n)}$$

CQFD Ouf !

Il y a donc bien un nombre premier p entre n et 2n.

Ce n'était pas facile. Rappelez vous que Bertrand ne l'avait pas démontré. Ramanujan avait trouvé une démonstration mais elle sortait du cadre de l'arithmétique. Il a fallu 100 ans pour que Erdös trouve cette démonstration élégante. Il m'a fallu quelques jours pour la développer et l'expliquer à partir de la version succinte de Wikipédia. Alors accrochez-vous, relisez la et quand vous l'aurez bien compris votre plaisir sera à la hauteur de vos efforts.

Références

[1] Olivier Sacks, “L'homme qui prenait sa femme pour un chapeau : Et autres récits cliniques”, EAN / ISBN : 9782757840214

[2] Carl Sagan, “Contact”, EAN / ISBN **:** 9782266079990

[3] Hardy, G. H., A Mathematician's Apology (Canto Classics). ISBN

[4] “La promesse du hasard” par François Vannucci, Edition Odile Jacob?

[5] “Matières à pensées” par Jean-Pierre Changeux et Alain Connes, Edition Odile Jacob.

[6] Rubik’s cube et théorie des groupes.https://math.univ-lille1.fr/~bhowmik/enseignement/Mem_master/mem_rubik.pdf

[7] https://fr.wikipedia.org/wiki/Probl%C3%A8mes_de_Hilbert

[8] “La guerre des nombres premiers”, Yan Pradeau, Flammarion

[9] “Vers la sobriété heureuse” par Pierre Rabhi. Edité par Actes Sud. ISBN : 978-2-7427-8967-2

[10] https://www.tangente-mag.com/article.php?id=7059 et https://interstices.info/nombres-premiers-et-cryptologie-lalgorithme-rsa/

[11] Sécurité des cartes bancaires. https://www.bibmath.net/crypto/index.php?action=affiche&quoi=moderne/cb

[12] Chiffrement symétrique par Pierre -Alin Fouque, Département cryptographie de l'ENS : https://www.di.ens.fr/~fouque/mpri/des-aes.pd

[13] F. Giannesini, H. Kanoui, R. Pasero, M. Van Caneghem , *Prolog*, Interéditions, 1985 : définition du Prolog "de Marseille", avec une préface d'A. Colmerauer

[14] "Merveilleux nombres premiers" de Jean-Paul Delahaye, edition BELIN . POUR LA SCIENCE

[15] Les nombres premiers entre l'ordre et le chaos, Gérald Tenenbaum et Michel Mendès France, DUNOD.

[16] Mathematic for human flourishing. Francis Su, Edition Yale.

[17] https://math.univ-lyon1.fr/~caldero/Alborghetti.pdf

[18] https://fr.wikipedia.org/wiki/Postulat_de_Bertrand

[19]: exponentiation rapide wikipedia. https://fr.wikipedia.org/wiki/Exponentiation_rapide

D'autres livres intéressants sur le sujet :

Rieman, le géomètre de la nature, Pour la Science, Aoüt 2002.

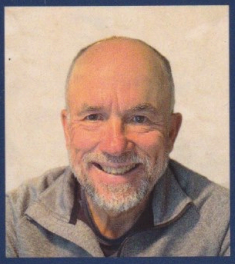
Evariste Gallois, Les génies de la science; Edition "Pour la science"

"Erdős, l'homme qui n'aimait que les nombres" par Paul Hoffman, Éditions Belin, 2000 (ISBN 2-7011-2539-1).

Remerciements

`Mes remerciements vont à :
Mme Mignonneau, mon institutrice de CM1 et CM2 (à l"époque on disait 8ème et 7ème), qui dirigeait une classe unique du CM1, CM2 et certificat d'études. Elle avait remarqué la rapidité relative avec laquelle je levais mon ardoise dans les exercices de calcul mental et avait soumis ma candidature pour une classe expérimentale de mathématiques modernes.
Mr Lamy et Mr Tournadre, mes professeurs de mathématiques modernes de la 6ème à la Terminale, qui m'ont fait découvrir un monde merveilleux d'objets abstraits aux propriétés étonnantes. Ces objets me semblaient plus réels que le monde imparfait qui m'entourait.
Jean-Claude Raimbault, pourfendeur de fautes d'orthographe et de grammaire; qui a corrigé les épreuves de ce livre.
Isabelle Raimbault : mon épouse qui a supporté de me voir passer des heures de ma retraite récente à lire des livres de mathématiques, à lui décrire la beauté de l'arithmétique et de son histoire.
A mes enfants : Laure, Sébastien, Martin que j'ai "tannés" pendant des années avec la nécessité de bien travailler en classe de mathématiques (ce qu'ils ont fait) et mes nombreuses tentatives de leur faire partager mon émotion et mon admiration devant certains théorèmes ou mathématiciens.

Le pays des nombres premiers



J.O PIEDNOIR

Jacques-Olivier PIEDNOIR est ingénieur en informatique. Il a dirigé des équipes de recherche et développement dans des entreprises de la Silicon Valley spécialisées dans l'informatique scientifique, présidé le conseil scientifique de l'ESEO et promu les études scientifiques auprès des lycéens.

Bienvenue au pays des nombres premiers. Que vous soyez un passionné de mathématiques ou un curieux pour lequel les mathématiques sont un souvenir lointain, ce guide vous entrainera dans une randonnée à travers les paysages de ces nombres merveilleux. Vous y découvrirez des anecdotes passionnantes sur les explorateurs de ces contrées aux régions encore inexplorées. Les premiers chapitres, à travers l'apprentissage du langage mathématique et du raisonnement logique, vous prépareront pour l'ascension des sommets vertigineux que sont les théorèmes fondamentaux sur les nombres premiers.
Vous randonnerez sur les traces d'Euclide, Gauss, Riemann et les nombreux mathématiciens des centres de recherches des universités les plus prestigieuses et découvrirez en version originale ces monuments de granit indivisibles que sont les nombres premiers et leurs cohortes de conjectures et de théorèmes.
Autrefois objets de curiosités pour passionnés d'arithmétique, vous découvrirez comment ces nombres sont devenus indispensables aux infrastructures de l'internet et aux monnaies numériques.
Cet essai vous donnera les outils et l'envie de futures randonnées dans l' univers des mathématiques, ossature de notre réalité.