Chapitre 1 Arithmétique
Partie 7 : Nombres premiers – Culture générale

I. Rappels des chapitres précédents

On rappelle ici les principaux résultats sur les nombres premiers démontrés lors des parties précédentes et qu'il faut connaître en terminale S :

Définition : *Nombres premiers*

Un entier naturel *n* supérieur ou égal à 2 est un nombre premier si et seulement si ses seuls diviseurs positifs sont 1 et *n*.

Propriété 1 : *Critère de primalité*

Soit *n* un entier naturel **supérieur ou égal à 2**.

- L'entier naturel *n* admet au moins un diviseur premier.
- Si *n* n'est pas premier, alors *n* admet au moins un diviseur premier *p* tel que $p \leq \sqrt{n}$.

Propriété 2 : *Infinitude de l'ensemble des nombres premiers*

Il existe une infinité de nombres premiers.

Propriété 3 : *Théorème fondamental de l'arithmétique*

Tout entier naturel *n* strictement supérieur à 1 se décompose en produit de facteurs premiers.

Cette décomposition est unique à l'ordre près des facteurs.

On note $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ avec $p_1 ; p_2 ; ... ; p_r$ des nombres premiers distincts et $\alpha_1, \alpha_2, ..., \alpha_r$ des entiers naturels non nuls.

Propriété 4 : *Nombre de diviseurs d'un entier*

Soit $p_1^{\alpha_1} \times p_2^{\alpha_2} \times ... \times p_r^{\alpha_r}$ la décomposition en produit de facteurs premiers d'un entier naturel *n* non nul.

n admet alors $N = (\alpha_1 + 1) \times (\alpha_2 + 1) \times ... \times (\alpha_r + 1)$ diviseurs positifs et donc $2N$ diviseurs dans $\mathbb{Z}$.

Propriété 5 : *Caractérisation des nombres premiers*

Soit *p* un nombre premier et *a* et *b* deux entiers relatifs, si *p* divise $a \times b$ alors *p* divise *a* ou *p* divise *b*

II. Des résultats sur les nombres premiers d'hier, d'aujourd'hui et de demain

Alors que la définition d'un nombre premier semble ne receler aucun mystère, on échoue à trouver une régularité quelconque dans leur succession. Connus dès les débuts de l'arithmétique, les nombres premiers ont excité la curiosité de milliers de mathématiciens.

Ils sont au cœur de la science des nombres, car tout entier se décompose de façon unique en un produit de facteurs premiers. Ils sont aussi à l'origine de certains des problèmes les plus difficiles des mathématiques et ont acquis, avec les progrès de la cryptographie, une importance économique considérable.
(Voir méthode RSA)

Les résultats suivants, dont les démonstrations sont inaccessibles pour le non initié, ont pour but de donner une vision globale des connaissances ou méconnaissances sur cette catégorie de nombres à la lumière de deux millénaires de recherche.

1. D'hier…

Théorème 1 : ***Théorème de la progression arithmétique de Dirichlet*** **(1837)**

Soient a et b deux entiers naturels non nuls premiers entre eux.

Il existe alors une infinité de nombres premiers de la forme $a+bn$ avec $n \in \mathbb{N}$

(Autrement dit, l'ensemble des termes de la suite arithmétique de raison b et de premier terme a contient une infinité de nombres premiers)

Ce résultat fut conjecturé par Legendre en 1785 sans que celui-ci ne puisse le démontrer.
Dirichlet en fournit une démonstration en 1837 sortant du cadre de l'arithmétique pure en utilisant exclusivement des résultats d'analyse dans l'ensemble des nombres complexes.

Théorème 2 : ***Postulat de Bertrand*** **(1845)**

Entre un entier naturel non nul et son double existe toujours un nombre premier.

Ce résultat fut démontré en 1850 par Pafnouti Tchebychev.

2. D'aujourd'hui…

Propriété : ***Plus grand nombre premier connu***

Découvert le 25 janvier 2013, le plus grand nombre premier connu est le nombre premier de Mersenne « $2^{57\,885\,161} - 1$ », qui comporte plus de 17 millions de chiffres en écriture décimale.

On le doit à l'équipe de Curtis Cooper, à l'université du Central Missouri, dans le cadre de la grande chasse aux nombres premiers de Mersenne (GIMPS).
Écrits les uns à la suite des autres, ses chiffres occuperaient plus de 4 000 pages en police Times New Roman taille 12. Voir l'exercice 1 pour la notion de nombre de Mersenne.

3. Et de demain…

Les deux résultats suivants sont en l'état de célèbres conjectures, elles font toujours l'objet de recherches.

Conjecture de Goldbach **(Mathématicien allemand 1690-1764)**

Tout nombre pair strictement supérieur à 2 peut s'écrire comme somme de deux nombres premiers.

L'éditeur britannique Tony Faber offrit en 2000 un prix de 1 000 000 $ pour une preuve de la conjecture. Le prix ne pouvait être attribué qu'à condition que la preuve soit soumise à publication avant avril 2002.

Il n'a jamais été réclamé…

La conjecture de Legendre **(Mathématicien français 1752-1833)**

Soit n un entier naturel supérieur ou égal à 2.
Il existe toujours au moins un nombre premier entre n^2 et $(n+1)^2$.

Cette conjecture est l'un des problèmes de Landau (Ensemble de quatre problèmes à propos des nombres premiers qu'Edmund Landau présenta lors du congrès international des mathématiciens de 1912 à Cambridge). En 2012, aucun d'entre eux n'a été résolu. Ces problèmes furent caractérisés dans son discours comme étant « inattaquables dans l'état actuel des connaissances »

III. Répartition des nombres premiers

Tous les problèmes posés par les nombres premiers aux mathématiciens résident dans l'irrégularité de leur répartition dans l'ensemble des entiers naturels.

Cette anarchie positionnelle est présentée au travers des résultats suivants :

Théorème : ***Ensemble d'entiers consécutifs sans nombres premiers***

Il existe une séquence arbitrairement longue d'entiers consécutifs ne contenant aucun nombre premier.

Ce résultat suivant a été démontré lors de l'exercice 22

Le théorème de répartition des nombres premiers

1. Répondre aux question suivantes à l'aide d'un algorithme que vous programmerez sous Algobox :
a. Combien y a-t-il de nombres premiers compris entre 50 et 60 ?
b. Entre 850 et 860 ? **c.** Entre 1850 et 1860 ? **d.** Entre 2850 et 2860 ?
e. La répartition des nombres premiers est-elle régulière ?

2. Soit *n* un entier naturel non nul, on note $\pi(n)$ le nombre d'entiers naturels premiers inférieurs ou égaux à *n* et $p(n)=\dfrac{\pi(n)}{n}$ la proportion de nombres premiers inférieurs ou égaux à *n*.

Remplir le tableau suivant :

n	$\pi(n)$	$p(n)$ en %	$\dfrac{n}{\ln(n)}$
10			
100			
1000	168		
10000	1 229		
$\mathbf{10^5}$	9 592		
$\mathbf{10^6}$	78 498		
$\mathbf{10^7}$	664 579		
$\mathbf{10^8}$	5 761 455		
$\mathbf{10^9}$	50 847 534		
$\mathbf{10^{10}}$	455 052 511		
$\mathbf{10^{11}}$	4 118 054 813		
$\mathbf{10^{12}}$	37 607 912 018		
$\mathbf{10^{13}}$	346 065 536 839		
$\mathbf{10^{14}}$	3 204 941 750 802		
$\mathbf{10^{15}}$	29 844 570 422 669		
$\mathbf{10^{16}}$	279 238 341 033 925		
$\mathbf{10^{17}}$	2 623 557 157 654 233		
$\mathbf{10^{18}}$	24 739 954 287 740 860		
$\mathbf{10^{19}}$	234 057 667 276 344 607		
$\mathbf{10^{20}}$	2 220 819 602 560 918 840		

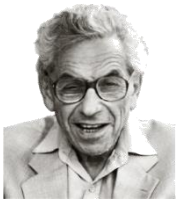
Que constatez-vous ?

Théorème : *Hadamard* / *de La Vallée Poussin* (répartition et raréfaction des nombres premiers)

Soit *n* un entier naturel non nul, on note $\pi(n)$ le nombre d'entiers naturels premiers inférieurs ou égaux à *n*. On a alors :

- $\pi(n)\simeq\dfrac{n}{\ln(n)}$ lorsque *n* est grand.
- La proportion de nombres premiers inférieurs ou égaux à *n* est approximativement égale à $\dfrac{\pi(n)}{n}\simeq\dfrac{1}{\ln(n)}$ lorsque *n* est grand et tend donc vers 0 lorsque *n* tend vers $+\infty$ (puisque $\lim\limits_{n\to+\infty}\ln(n)=+\infty$)

***Remarques* :** Conjecturé par Gauss en 1792 (il avait alors 15 ans), ce résultat fût démontré indépendamment par Hadamard et de La Vallée Poussin près de 100 ans plus tard en 1896 en utilisant l'analyse complexe.



P. Erdös

Paul Erdös et Atle Selberg publient en 1949 une démonstration élémentaire (et géniale) de ce résultat sans sortir du cadre de l'arithmétique pure, faisant par la même taire l'intégralité de la communauté mathématique de l'époque qui avait assuré de l'impossibilité de la démarche.

L'auteur de ces lignes encourage vivement le lecteur à s'informer sur la vie excentrique et absolument passionnante de Paul Erdös qui était certainement l'un des plus grands génies du XX ième siècle.
Paul Erdös était un mathématicien sans domicile fixe, Hongrois, né à Budapest en 1913 et mort dans une chambre d'hôtel à Varsovie (Pologne) en 1996 à l'âge de 86 ans.

Et pour terminer, un peu de régularité dans un monde régi par l'anarchie

Nous terminerons cet exposé par le lumineux :

Théorème : *Green – Tao* (2004)

Soit k un entier naturel non nul quelconque fixé.

Il existe alors k nombres premiers $p_1 ; p_2 ; \ldots ; p_k$ en progression arithmétique.
(i.e. tels que $p_2 - p_1 = p_3 - p_2 = \ldots = p_k - p_{k-1}$)

En fait, on a encore bien mieux, il existe une infinité de telles progressions !


Ben Green


Terence Tao

Ce résultat dont l'énoncé est simplissime et accessible à tous admet une démonstration d'une effroyable (et le mot est faible) technicité même si elle reste élémentaire au sens où elle ne fait intervenir aucun argument de l'analyse complexe ! (Ce que toute la communauté mathématique jugeait impossible, le scénario de Paul Erdös et du théorème d'Hadamard / de La Vallée Poussin se reproduisant à nouveau)

Elle valut la médaille Fields à Terence Tao en 2006 alors âgé de 31 ans ainsi qu'une admiration absolue de la part de ses confrères.

Ce théorème exprime que malgré la répartition chaotique des nombres premiers dans l'ensemble des entiers naturels, il existe une infinité de listes arbitrairement longues de nombres premiers remarquablement bien rangées ! Un peu d'ordre dans un sacrément beau foutoir en somme…

Terence Tao, personnage d'une gentillesse et d'une humilité extraordinaires, est reconnu comme l'un des plus grands (si ce n'est le plus grand) mathématiciens actuellement en vie.

Exercices sur les nombres premiers

Exercice 1 ***Nombres de Mersenne…***

On pourra utiliser que pour tout réel *a* et *n* un entier naturel supérieur ou égal à 2, on a alors la factorisation :

$$a^n - 1 = (a-1)\left(1 + a + a^2 + ... + a^{n-1}\right)$$

On considère les nombres de Mersenne $M_n = 2^n - 1$, pour *n* entier naturel non nul.

1. a. En utilisant un tableur, émettre une conjecture sur *n* pour que M_n soit un multiple de 3.
b. Démontrer cette conjecture à l'aide des congruences.

2. a. En utilisant un tableur, émettre une conjecture sur *n* pour que M_n soit un multiple de 5.
b. Démontrer cette conjecture à l'aide des congruences.

3. a. Le nombre M_{11} est-il premier ?
b. On suppose que $n = pq$ avec *p* et *q* entiers supérieurs ou égaux à 2.
Trouver une factorisation de M_n en produit de deux entiers supérieurs ou égaux à 2.
c. En déduire que si M_n est premier, alors *n* est premier. La réciproque est-elle vraie ?

4. Soient *a* et *n* deux entiers supérieurs ou égaux à 2.
Montrer que si $a^n - 1$ est premier, alors $a = 2$ et *n* est premier.

***Remarque* :** Lorsque *n* est premier, M_n n'est pas forcément premier mais est un bon candidat à l'être.
La recherche pratique de très grands nombres premiers se fait souvent sous la forme d'un nombre de Mersenne M_n avec *n* premier.

En particulier, les nombres M_2 ; M_3 ; M_5 ; M_7 ; M_{13} ; M_{17} ; M_{19} ; M_{31} ; M_{61} ; M_{89} ; M_{107} ; M_{127} ; M_{521} et M_{607} sont premiers. Le plus grand nombre de Mersenne premier connu est $M_{57885161}$.

Exercice 2 ***Nombres de Fermat…***

Les nombres de Fermat sont les entiers de la forme $F_n = 2^{(2^n)} + 1$ avec $n \in \mathbb{N}$.
Au XVII è siècle, Pierre de Fermat émit la conjecture que ces nombres étaient premiers.

1. a. En utilisant un algorithme, Vérifier que F_0 ; F_1 ; F_2 ; F_3 et F_4 sont premiers.
b. Qu'en est-il de F_5 ? Qu'en déduire pour la conjecture de Fermat ?

2. a. Vérifier que pour tout entier naturel *n*, $F_{n+1} = (F_n - 1)^2 + 1$ et en déduire que $F_{n+1} - 2 = F_n(F_n - 2)$.
b. Montrer par récurrence que pour tout entier naturel *n*, $F_{n+1} - 2 = F_0 \times F_1 \times ... \times F_n$
c. Soient *n* et *n'* deux entiers naturels tels que $n < n'$. Montrer qu'un diviseur commun de F_n et $F_{n'}$ divise 2.
d. En déduire que deux nombres de Fermat distincts sont premiers entre eux.

***Remarque* :** En fait les seuls nombres de Fermat premiers connus actuellement sont F_0 ; F_1 ; F_2 ; F_3 et F_4.
On sait qu'aucun nombre de Fermat F_n n'est premier pour $5 \leq n \leq 32$.
On ne sait toujours pas dire à l'heure actuelle si F_{33} est premier ou non…

Exercice 3 ***Nombres de Carmichael…***

On sait, par le petit théorème de Fermat, (voir l'activité sur la méthode RSA) que pour tout nombre premier p et tout entier a premier avec p, $a^{p-1} \equiv 1 \ (p)$.
La réciproque de ce résultat, appelée test de Fermat, est fausse, c'est-à-dire qu'il existe des nombres vérifiant les congruences précédentes sans qu'ils soient premiers : ce sont les nombres de Carmichael.

Un nombre de Carmichael est un nombre entier n avec $n > 1$ qui n'est pas premier et pour lequel $a^{n-1} \equiv 1 \ (n)$ pour tout entier a premier avec n.

Soit n un nombre de Carmichael et p un facteur premier de n.

1. a. Expliquer pourquoi $p^n \equiv p \ (n)$.

b. En déduire que p^2 ne divise pas n.

c. En déduire qu'un nombre de Carmichael s'écrit sous la forme $n = p_1 \times p_2 \times ... \times p_r$ où $p_1 ; p_2 ; ... ; p_r$ sont des nombres premiers distincts.

d. Montrer qu'un entier naturel n qui s'écrit sous la forme $n = p_1 \times p_2 \times ... \times p_r$ où $p_1 ; p_2 ; ... ; p_r$ sont des nombres premiers distincts n'est pas nécessairement un nombre de Carmichael.

2. Le théorème de Korselt

Le critère de Korselt permet de reconnaître un nombre de Carmichael à partir de sa décomposition en produit de facteurs premiers. On admet le théorème suivant :

Théorème de Korselt

Un entier n est un nombre de Carmichael si, et seulement si, n est strictement positif, non premier, sans facteur carré, et tel que pour tout nombre premier p divisant n, $p-1$ divise $n-1$.

a. Montrer que les nombres de Carmichael sont impairs.
b. Montrer qu'un nombre de Carmichael possède au moins trois facteurs premiers distincts.
c. Vérifier que 561 est un nombre de Carmichael

Remarque **:** Les premiers nombres de Carmichael sont 561, 1105, 1729, 2465, 2821, 6601, 8911, …