Lycée Les 3 Sources **Bourg-Lès-Valence**
Maths/NSI Année **2023-24**

Les étranges régularités des nombres premiers

Trouver les nombres premiers

Dans ce document on ne considérera que des nombres entiers positifs. Ainsi, on pourra utiliser “entier” pour dire “entier positif”.
Un **nombre premier** est un entier qui a exactement 2 diviseurs : 1 et lui-même. Ainsi, 2, 3, 5, 7 et 11 sont premiers, mais pas 4, 6 ou 9. On remarque que le nombre 1 n’est pas premier vu qu’il n’a qu’un seul diviseur : lui-même.
Les nombres premiers ont été beaucoup étudiés en Grèce antique, même s’ils étaient connus avant.

Érathostène a notamment mis en place une méthode pour les détecter, appelée **crible d’Érathostène** :

- Faire la liste de tous les entiers de 2 à n.
- On commence avec 2.
- On l’entoure et on barre tous ses multiples.
- On prend le plus petit entier non barré et on recommence l’étape précédente.

	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	100

Exercice 1 : En utilisant le crible d’Érathostène, déterminer tous les nombres premiers inférieurs à 100.

On peut remarquer qu’à partir de 11, plus aucun nombre n’est barré. Nous y reviendrons.

Exercice 2 : À l’aide du tableau, donner des contre-exemples aux propositions suivantes :

1) Tous les nombres premiers sont impairs.
2) Tous les nombres premiers impairs se terminent par 1, 3, 7 ou 9.
3) Il n’y a pas 2 nombres premiers qui sont des entiers consécutifs.

Pour déterminer si un entier n est premier, on peut vérifier qu’il n’a pas de diviseur entre 2 et $n-1$. Si le nombre n est très grand, cela fait de nombreux calculs. Pour optimiser, on peut juste vérifier que n n’est pas pair et ensuite diviser uniquement par les nombres impairs.
On dit qu’un entier est **composé** s’il n’est pas premier. Tout nombre composé n peut s’écrire comme le produit de deux entiers a et b, tous deux, strictement compris entre 1 et n. Par conséquent, tout nombre composé n a au moins un diviseur premier qui est inférieur ou égal à $\sqrt{n}$. Ainsi, pour savoir si 101 est premier, il suffit de tester les diviseurs potentiels inférieurs à $\sqrt{101}$.
Quand on cherche les diviseurs d’un nombre, on peut donc s’arrêter à sa racine carrée. Pour déterminer si un nombre n est premier, on peut donc utiliser la méthode suivante :

- On vérifie qu’il n’est pas pair.
- On vérifie qu’il n’est divisible par aucun nombre impair compris entre 3 et $\sqrt{n}$.

Si on a la liste des nombres premiers inférieurs à $\sqrt{n}$, on peut essayer de diviser par ces nombres au lieu de le faire avec tous les nombres impairs.

Exercice 3 : Déterminer si les nombres suivants sont premiers ou non.

1) 101 2) 129 3) 2023 4) 9973

C'est pas bientôt fini ?

Quand on regarde le crible d'Érathostène, on peut se dire qu'à partir d'un certain seuil, tous les nombres seront barrés et qu'il ne restera plus de nombres premiers à découvrir. Ce n'est pas le cas. En effet, il y a une infinité de nombres premiers et Euclide l'a démontré il y a 2300 ans. Pour comprendre sa démonstration, il faut utiliser la propriété suivante :

Si un entier n divise a et $a+b$, alors n divise b.

Exercice 4 : Compléter la démonstration de cette propriété.
Si n est un diviseur de a, alors il existe un entier k_1 tel que $a =$ .....
De même, si n est un diviseur de $a+b$, alors il existe un entier k_2 tel que $a+b =$ .....
Donc $b = (a+b) - a =$ ..... D'où .....

Attention, ce n'est pas parce que n divise $a+b$, qu'il divise a et b.

Exercice 5 : Donner un contre exemple à l'énoncé précédent.

Exercice 6 : Faisons une preuve par l'absurde du Théorème d'Euclide. Supposons qu'il y a un nombre fini de nombres premiers, notés $p_1, p_2, \ldots, p_k$. Aucun autre nombre ne peut être premier.
On note $\mathrm{N} = p_1 \times p_2 \times \cdots \times p_k + 1$.

1) Expliquer pourquoi il existe au moins un nombre premier p_i qui divise N.
2) En déduire que p_i doit diviser 1.
3) Expliquer pourquoi c'est une absurdité et conclure.

Attention, cette construction ne permet pas d'obtenir des nombres premiers arbitrairement grands. Ajouter 1 au produit des k premiers nombres premiers ne donne pas toujours un nombre premiers. En effet, il peut y avoir d'autres nombres premiers entre le dernier utilisé dans le produit et la racine carrée du nombre obtenu.

Chaos ou régularité

Il y a donc une infinité de nombres premiers. Mais comment sont-ils répartis ?
En regardant dans le tableau on peut remarquer qu'initialement, les nombres premiers sont assez rapprochés. On dit que deux nombres premiers p et $p' = p+2$ sont jumeaux. C'est le cas de 3 et 5 ou de 11 et 13.

Exercice 7 : Déterminer toutes les paires de nombres premiers jumeaux inférieurs à 100.

Plus on se rapproche de 100, moins il y a de premiers jumeaux. Pourtant, la **conjecture des nombres premiers jumeaux** suppose qu'il y a un nombre infini de nombres premiers jumeaux. Cela veut dire que pour tout entier n, aussi grand soit-il, il y a une infinité de nombres premiers jumeaux supérieurs à n.
Les paires de nombres premiers de la forme $(p; p+4)$ sont dit **cousins** et ceux de la forme $(p; p+6)$ sont **sexy**. La **conjecture de Polignac** suppose qu'il existe une infinité de paires de nombres premiers $(p; p+n)$ pour tout n pair. Aucune de ces deux conjectures n'a été démontrée.
Un résultat de 2014, de Yitang Zhang, montre qu'il existe un entier $\mathrm{N} < 7 \times 10^7$ tel qu'il y a une infinité de paires de nombres premiers de la forme $(p; p+\mathrm{N})$. Par contre, le résultat ne dit pas quelle est la valeur de N. Mais le simple fait de savoir qu'il existe est déjà une avancée majeure.

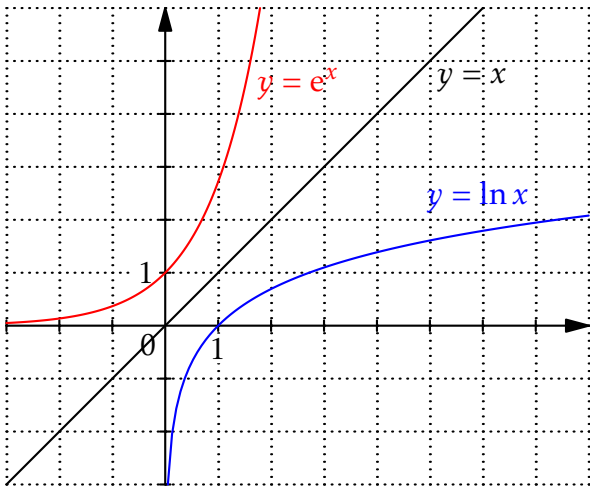
À l'inverse de ces résultats, qui montrent que même sur les nombres extrêmement grands, il y a des nombres premiers très proches les uns des autres, il peut y avoir un grand écart entre deux nombres premiers consécutifs. On appelle **factorielle de** n, ou n **factorielle**, le produit de tous les entiers de 1 à n. Ainsi : $n! = 1 \times 2 \times 3 \times \cdots \times n$.

Exercice 8 : On considère le nombre $\mathrm{N} = 100!$.

1) Expliquer pourquoi $\mathrm{N}+2$ et $\mathrm{N}+3$ ne peuvent pas être premiers.
2) Combien d'entiers consécutifs, à partir de $\mathrm{N}+2$, ne peuvent pas être premiers ?
3) Donner une façon de trouver un intervalle de k nombres consécutifs qui ne sont pas premiers.

Il y a donc de très grands écarts entre 2 nombres premiers consécutifs, mais aussi de très petits écarts, même lorsqu'on considère des nombres infiniment grands.
Peut-on en déduire que la répartition des nombres premiers est totalement chaotique ? Pas vraiment.

Pour avoir un élément de réponse, il faut utiliser le **logarithme népérien**. C'est la fonction réciproque à la fonction exponentielle, tout comme la fonction racine carrée est la fonction réciproque à la fonction carrée. Ainsi, si $y = \mathrm{e}^x$ alors $x = \ln y$. Puisque la fonction exponentielle grandit de plus en plus vite lorsque x devient grand, le logarithme népérien grandit de moins en moins lorsque x devient grand. Il continue d'augmenter, mais à partir d'un certain rang, il faut que x augmente énormément pour que le logarithme augmente de 1.



À la fin du 18e siècle, Gauss, alors qu'il n'avait que 15 ou 16 ans, et Legendre ont tous les deux conjecturé de façon indépendante le **théorème des nombres premiers** qui n'a été démontré que 100 ans plus tard : pour tout entier n, le nombre de nombres premiers inférieurs à n est environ $\dfrac{n}{\ln n}$. Cette approximation devient plus précise lorsque n devient très grand. Il faut la considérer comme un ordre de grandeur.

Exercice 9 :

1) Calculer le nombre de nombres premiers devant être inférieurs à 100 d'après cette formule. Comparer ce résultat avec la réalité.
2) Calculer le nombre de nombres premiers devant être inférieurs à 1 000 000 d'après cette formule.
3) Calculer le nombre de nombres premiers devant être inférieurs à 1 000 000 000 d'après cette formule.

Il y a deux corollaires à ce théorème :

- L'écart moyen entre tous les nombres premiers inférieurs à n est d'environ $\ln n$.
- Le n-ième nombre premier est environ $n \times \ln n$.

Pour l'écart moyen, cette valeur n'est pas forcément très précise puisque, comme nous l'avons vu, l'écart entre deux nombres premiers peut être très variable. Ces résultats donnent au moins une idée de la densité des nombres premiers parmi les entiers.

Exercice 10 :

1) Calculer l'écart moyen entre les nombres premiers inférieurs à n, avec :
   a) $n = 1000$ b) $n = 1\,000\,000$ c) $n = 1\,000\,000\,000$
2) Calculer une valeur approchée du n-ième nombre premier avec :
   a) $n = 1000$ b) $n = 1\,000\,000$ c) $n = 1\,000\,000\,000$

On connait, depuis, des formules plus précises. Par exemple, le n-ième nombre premier est environ égal à $n(\ln(n) + \ln(\ln n) - 1)$.
Le **Théorème de Tchébycheff** (1850) dit également que pour tout entier $n > 2$, il y a au moins un nombre premier entre n et $2n$.
On peut aussi observer une forme de régularité si on se concentre sur le dernier chiffre des nombres premiers. Si on met de côté 2 et 5, tous les nombres premiers se terminent par 1, 3, 7 ou 9. La proportion de nombres premiers se terminant par chacun de ces chiffres est d'environ 25 %. Ils sont donc relativement équitablement distribués.
Par contre, étant donné un nombre premier, les probabilités que le chiffre des unités du prochain soit 1, 3, 7 ou 9 ne sont pas les mêmes. En effet, la probabilité que le nombre premier suivant ait le même chiffre des unités est inférieure à 25 %. La probabilité de chacun des autres chiffres est, au contraire, supérieure à 25 %. Par exemple, si un nombre premier se termine par 1, le nombre premier suivant a moins de chances de se terminer par 1 que par 3, par 7 ou par 9. Ces résultats récents (2016) n'ont pas été démontrés mais observés sur 400 milliards de nombres premiers.
Il y a néanmoins des propriétés que l'on sait démontrer. La **racine numérique** d'un entier est la somme de ses chiffres, éventuellement répétée jusqu'à obtenir un seul chiffre. Par exemple, la racine numérique de 247 est 4 parce que $2 + 4 + 7 = 13$ et $1 + 3 = 4$.
Nous avons alors la propriété suivante : la racine numérique du produit de deux nombres premiers jumeaux supérieurs à 3 est toujours égale à 8.

Exercice 11 : Vérifier le résultat pour les nombres premiers jumeaux suivants :
1) 5 et 7 2) 17 et 19 3) 8231 et 8233

Pour démontrer cette propriété, il faut utiliser deux autres propriétés.
Tout d'abord, la racine numérique d'un nombre est égale au reste de la division de ce nombre par 9. Par exemple :

$$247 = 2 \times 99 + 2 + 4 \times 9 + 4 + 7 = 9(2 \times 11 + 4) + 2 + 4 + 7 = 9 \times 26 + 9 + 4 = 9 \times 27 + 4$$

En faisant la division de 247 par 9, on obtient un reste de 4, ce qui est la racine numérique trouvée précédemment.
De plus, dans tout triplets d'entiers consécutifs, il y en a un qui est un multiple de 3.
Nous pouvons maintenant démontrer la propriété.

Exercice 12 : Soient a et b deux nombres premiers jumeaux supérieurs à 3. Soit n l'entier tel que $a = n - 1$ et $b = n + 1$.
1) Expliquer pourquoi n est forcément un multiple de 3.
2) En posant $n = 3k$, exprimer a et b à l'aide de k.
3) En déduire une expression de $a \times b$ en fonction de k.
4) En admettant que le reste de la division de -1 par 9 est 8, conclure.

En fait cette propriété est vraie pour tout couple d'entiers encadrant un multiple de 3. Il se trouve que c'est le cas de tous les nombres premiers jumeaux, à l'exception de 3 et de 5.