Chapitre 8 Les nombres premiers

I – Généralités et propriétés élémentaires

Définition

Un entier naturel est un nombre premier si et seulement s'il admet, dans $\mathbb{N}$, ***exactement deux diviseurs distincts*** : ……

Exemples

2 est un nombre premier car les seuls diviseurs positifs de 2 sont : 1 et 2.

De même, 3 ; 5 ; 7 ; 11 sont quelques exemples de nombres premiers.

Le nombre 0 n'est pas premier. Pourquoi ?

Le nombre 1 est-il un nombre premier ?

Un entier pair est-il un nombre premier ?

Que peut-on dire de deux nombres premiers distincts ?

Remarques

2 est le seul nombre premier pair.

Un nombre premier supérieur ou égal à 3 est donc nécessairement impair.

On note $\mathbb{P}$ l'ensemble formé par les nombres premiers.

Un entier supérieur ou égal à 2 qui n'est pas premier est dit composé.

Mini propriété fort utile

Soit p un nombre premier et n un entier naturel.

On a l'alternative suivante : ou bien p divise n, ou bien p et n sont premiers entre eux.

Preuve :

✂----------

Théorème

1) ***Tout entier naturel $N \geq 2$ admet au moins un diviseur premier.***

2) ***Si $N \geq 2$ est NON PREMIER, alors N admet au moins un diviseur premier p tel que $p \leq \sqrt{N}$.***

Preuve :

✂----------

Attention, un tel entier N peut admettre un diviseur premier strictement supérieurs à $\sqrt{N}$.

Par exemple pour $N = 22$: les diviseurs premiers de 22 sont 2 et 11.

11 est un nombre premier et $11 > \sqrt{22}$.

Test de primalité

Soit n un entier naturel supérieur ou égal à 2.

Si n n'est divisible par aucun des nombres premiers inférieurs ou égaux à $\sqrt{n}$, alors n est un nombre premier.

Pourquoi ? Ecrire la contraposée du point 2) du théorème précédent :

En fait la réciproque est aussi vraie (mais ne dit rien de transcendant : si un nombre est premier, alors il n'est divisible par aucun nombre premier inférieur ou égaux à $\sqrt{n}$).

En effet $n \geqslant 2$, donc $n > 1$, donc par stricte croissance de la fonction racine sur $[0 ; +\infty[$, $\sqrt{n} > \sqrt{1}$, donc en multipliant les deux membres de la précédente inégalité par $\sqrt{n} > 0$, on a : $n > \sqrt{n}$, et vu que n est premier, son seul diviseur autre que n est 1, et 1 n'est pas un nombre premier.

Remarque : ce test de primalité fournit un critère d'arrêt dans la recherche des diviseurs premiers d'un entier naturel donné.

Application* : *le crible* d'*Erathostène

Dresser la liste L des nombres premiers inférieurs à 100.

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	100

$L =$

***Exercice* 1**

Le nombre 4561 est-il un nombre premier ?

Exercice 2

Ecrire un algorithme avec Python, qui demande à l'utilisateur l'entier naturel $N \geq 2$ de son choix, et qui affiche en sortie si cet entier choisi est un nombre premier ou pas.

✂----------

Théorème

Il existe une infinité de nombres premiers.

Preuve : (*essayer deux preuves différentes*)

✂----------

On va s'intéresser à la répartition des nombres premiers.

A titre culturel, pour tout entier naturel $n > 1$, il existe au moins un nombre premier appartenant à l'intervalle $]n\ ;2n[$.

Ce résultat, dont la démonstration est difficile, est connu sous le nom de *Postulat de Bertrand*.

Exercice 3

a) Fabriquer un intervalle de longueur respective : 2 puis 3 puis 4 puis 5 puis 6 ne contenant aucun nombre premier.

b) Démontrer qu'on peut fabriquer un intervalle de longueur arbitraire, ne contenant aucun nombre premier.

c) Qu'en déduit-on quant à la répartition des nombres premiers ?

✂----------

Exercice 4

Soit p un nombre premier et a et b deux entiers. On suppose que p divise ab.

Démontrer que p divise a ou p divise b.

Ce résultat reste-t-il vrai si on ne suppose plus que p est un nombre premier ?

✂----------

Exercice 5

Démontrer que la somme des carrés de trois nombres premiers strictement supérieurs à 3 n'est jamais un nombre premier.

Indication **:** on pourra raisonner modulo 3.

✂----------

II – Applications

Théorème fondamental de l'arithmétique

Tout entier naturel n supérieur ou égal à 2 est décomposable en un produit de nombres premiers.

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

On peut donc toujours écrire n sous la forme : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots p_k^{\alpha_k}$ où $p_1, p_2, \ldots\ldots\ldots p_k$ ***sont des nombres premiers deux à deux distincts et*** $\alpha_1, \alpha_2, \ldots\ldots \alpha_k$ ***sont des entiers naturels non nuls.***

Avec les notations ci-dessus : $n = \prod_{j=1}^{k} p_j^{\alpha_j}$

Preuve : Nous allons procéder en deux temps : d'abord l'existence, ensuite l'unicité.

Existence : Soit $n \geq 2$. Si n est premier, alors $n = n^1$ et c'est terminé.

Si n n'est pas premier, comme $n \geq 2$, alors n admet au moins un diviseur premier. Notons p_1 le plus petit diviseur premier de n : il existe donc un entier $n_1 \geq 1$ tel que $n = p_1 \times n_1$.

Observons que $n_1 < n$ car $p_1 > 1$!

Si n_1 *est premier, alors c'est terminé, n est égal au produit de deux facteurs premiers.*

Sinon, on recommence le processus, appliqué cette fois-ci à n_1.

Notons p_2 *le plus petit diviseur premier de* n_1 *: il existe donc un entier* $n_2 \geq 1$ *tel que :* $n_1 = p_2 \times n_2$.

On a : $n_2 < n_1$ *car* $p_2 > 1$.

En réitérant le procédé autant de fois que nécessaire, on fabrique donc une suite (n_k) *d'entiers naturels qui est strictement décroissante par construction et minorée par* 1.

D'après le principe de la descente infinie de Fermat, cette suite est nécessairement finie.

Il existe donc un rang m tel que $n_m = 1$ *et donc,* $n = p_1 \times p_2 \times \ldots\ldots\ldots \times p_m$ *avec les nombres premiers* $p_1, p_2 \ldots\ldots\ldots, p_m$ *non nécessairement distincts.*

En regroupant les facteurs premiers égaux entre eux, on obtient : $n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots p_k^{\alpha_k}$.

Unicité : *On procède par récurrence dite forte sur l'entier n.*

L'unicité de la décomposition est claire pour $n = 2$.
On suppose que la décomposition est unique pour tout entier inférieur strictement à un n donné et on montre que la décomposition de n en produit de facteurs premiers est unique.
On suppose que n admette deux décompositions distinctes en produit de facteurs premiers :

$$n = p_1 \times p_2 \times \ldots \times p_r = q_1 \times q_2 \times \ldots \times q_s$$

Si p_1 était premier avec q_i pour tout $1 \leqslant i \leqslant s$, alors d'après un corollaire du théorème de Gauss, p_1 serait premier avec $q_1 \times q_2 \times \ldots \times q_s$; or p_1 divise $q_1 \times q_2 \times \ldots \times q_s$ d'où une contradiction.
Donc il existe i tel que p_1 et q_i ne sont pas premiers entre eux. Comme ce sont des nombres premiers, on a nécessairement $p_1 = q_i$.
Le nombre $n_1 = \dfrac{n}{p_1}$ admettrait donc deux décompositions distinctes :

$$n_1 = p_2 \times p_3 \times \ldots \times p_r = q_1 \times q_2 \times \ldots \times q_{i-1} \times q_{i+1} \times \ldots \times q_s$$

ce qui contredit l'hypothèse de récurrence car $n_1 < n$ (car $p_2 \geqslant 2$). On en déduit que n admet une décomposition unique.
On a ainsi démontré par récurrence l'unicité de la décomposition pour tout $n \geqslant 2$. ■

Exemple

Donner la décomposition en produit de facteurs premiers de : 140 ; 1001.

✂----------

Exercice 6

Ecrire un algorithme donnant les facteurs premiers, d'un entier naturel $N > 1$ choisi par l'utilisateur.

✂----------

Nombre de diviseurs d'un entier naturel non nul

Un exemple : Déterminer la liste de tous les diviseurs entiers naturels du nombre 180.

Comment ne pas en oublier ?

✂----------

Propriété

Soit n un entier naturel supérieur ou égal à 2.

La décomposition en produit de facteurs premiers de n est : n = $p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots\ldots p_k^{\alpha_k}$ ***où*** $p_1, p_2, \ldots\ldots\ldots p_k$ ***sont des nombres premiers deux à deux distincts et*** $\alpha_1, \alpha_2, \ldots\ldots \alpha_k$ ***sont des entiers naturels non nuls.***

Tout diviseur d de l'entier n a une décomposition en produit de facteurs premiers de la forme :

Le nombre de diviseur de n est égal à :

Preuve :

✂----------

Propriété

Soit a et b deux entiers naturels supérieurs ou égaux à 2.

Ecrivons la décomposition en produit de facteurs premiers de a et b :

$a = \prod_{j=1}^{k} p_j^{a_j}$ et $b = \prod_{j=1}^{m} p_j^{\beta_j}$ avec les nombres p_j tous premiers et les exposants α_i et β_j

sont des entiers naturels non nuls.

Alors on a : ***PGCD(a ; b)*** =

✂----------

Exercice 7

Notons $p_1, p_2, \ldots\ldots\ldots\ldots\ldots\ldots, p_n, \ldots\ldots$ la liste ordonnée par ordre croissant des nombres premiers.

1) Démontrer, en raisonnant par l'absurde, que $p_{n+1} < \prod_{k=1}^{n} p_k$. On pourra utiliser le postulat de Bertrand pour conclure.

2) En déduire que $p_n < 2^{2^n}$.

✂----------

Exercice 8

Soit p un nombre premier strictement supérieur à 3.

a) Etudier les restes possibles dans la division euclidienne de p par 12.

b) En déduire que $p^2 + 11$ n'est jamais un nombre premier.

Un exercice de bac…

Pour tout entier naturel n , on note F_n le n-ième nombre de Fermat. Il est défini par

$$F_n = 2^{2^n} + 1.$$

Partie A :

Pierre de Fermat, leur inventeur, a conjecturé que :

« Tous les nombres de Fermat sont premiers »,

L'objectif est de tester cette conjecture.

1. **a.** Calculer F_0, F_1, F_2 et F_3.
   b. Peut-on en déduire que tous les nombres de Fermat sont premiers ?
2. On considère l'algorithme ci-dessous :

```
F ← 2^(2^5) + 1
N ← 2
Tant que F%N ≠ 0
    N ← N + 1
Fin Tant que
Afficher N
```

$F\%N$ désigne le reste de la division euclidienne de F par N.

La valeur affichée à la fin de l'exécution est 641.
Que peut-on en déduire ?

Partie B :

L'objectif est de prouver que deux nombres de Fermat distincts sont toujours premiers entre eux.

1. Démontrer que pour tout entier naturel n non nul on a $F_n = (F_{n-1} - 1)^2 + 1$.
2. Pour tout entier naturel n on note :

$$\prod_{i=0}^{n} F_i = F_0 \times F_1 \times F_2 \times \ldots \times F_{n-1} \times F_n.$$

On a donc $\prod_{i=0}^{n} F_i = \left(\prod_{i=0}^{n-1} F_i\right) \times F_n$.
Montrer par récurrence et en utilisant le résultat de la question précédente que pour tout entier naturel n non nul on a :

$$\prod_{i=0}^{n-1} F_i = F_n - 2.$$

3. Justifier que, pour tous entiers naturels n et m tels que $n > m$, il existe un entier naturel q tel que $F_n - qF_m = 2$.
4. En déduire que deux nombres de Fermat sont toujours premiers entre eux.

III-Le petit théorème de Fermat

1) *Introduction :* Pourquoi « petit » ?

Voici le grand théorème de Fermat :

« Pour tout entier naturel n, il n'existe pas de nombres entiers non nuls x, y et z tels que $x^n + y^n = z^n$ dès que n est un entier strictement supérieur à 2 ».

Pierre de Fermat (1601-1665) l'énonça dans la marge d'un livre et écrit : « j'ai trouvé une merveilleuse démonstration de cette proposition, mais la marge est trop étroite pour la contenir ». Ce théorème ne fût démontré qu'en 1995 (plus de 300 ans plus tard) par Andrew Wiles. Cette démonstration tient en plusieurs centaines de pages.

Dans le cas où n=1 l'équation diophantienne $x^n + y^n = z^n$ admet clairement une infinité de solutions.

Qu'en est-il lorsque n=2 ?

Plimpton 322 :

On appelle triplet pythagoricien un triplet (a, b, c) d'entiers strictement positifs tels que $a^2 + b^2 = c^2$ donc solution de l'équation $x^n + y^n = z^n$ pour n=2.

La tablette babylonienne Plimpton 322 (du nom du collectionneur Georges Plimpton) date des années −1800 environ. C'est l'un des plus anciens textes mathématiques connus. Cette tablette donne une liste de 15 triplets pythagoriciens comme celui de la question h) de l'exercice suivant. Une recherche au hasard de tels triplets est exclue et les premiers commentateurs de la tablette pensaient que les babyloniens connaissaient déjà le résultat du a), 1300 ans avant Pythagore et 1500 ans avant Euclide. Un débat autour des méthodes employées est toujours en cours.

Découverte du petit théorème de Fermat

Soit a un entier relatif.

a) On considère l'entier p=5. Compléter le tableau ci-dessous :

a modulo 5	0	1	2	3	4
a^4 modulo 5					

b) On considère l'entier p=7. Compléter le tableau ci-dessous :

a modulo 7	0	1	2	3	4	5	6
a^6 modulo 7							

c) On considère l'entier p=11. Compléter le tableau ci-dessous :

a modulo 11	0	1	2	3	4	5	6	7	8	9	10
a^{10} modulo11											

d) Quelle condition suffisante sur p et sur a peut-on conjecturer pour que : $a^{p-1} \equiv \ldots [p]$?

Le petit théorème de Fermat

Théorème

- Soit p un nombre premier et a un entier naturel quelconque, alors $a^p \equiv a\ [p]$.
- (Corollaire crucial) Soit p un nombre premier et a un entier naturel non multiple de p, alors : $a^{p-1} \equiv 1\ [p]$.

Démonstration : Celle de MPSI avec coefficient binomiaux et par récurrence.

Exercice 9

Montrer que pour tout $n \in \mathbb{N}$, $3^{6n} - 1$ est divisible par 7.

Exercice 10

Soit p un nombre premier différent de 3.

Démontrer que pour tout $n \in \mathbb{N}$, $3^{n+p} - 3^{n+1}$ est divisible par p.

Exercice 11

Soit $n \in \mathbb{N}$ et $a = n^5 - n$.

1) Montrer que a est divisible par 5.

2) Montrer que $a = n(n^2 - 1)(n^2 + 1)$

3) Montrer que a est divisible par 2 et par 3.

4) a est-il divisible par 30 ?

Compléments :

Exercice 4 d'arithmétique du bac Marocain 2023, excellent.

EXERCICE4 :(3 points)

Soit p **un nombre premier impair**. On considère dans $\mathbb{Z}$ l'équation $(E): x^2 \equiv 2\ [p]$

0.25 1- a) Montrer que : $2^{p-1} \equiv 1\ [p]$

0.25 b) En déduire que : $2^{\frac{p-1}{2}} \equiv 1\ [p]$ ou $2^{\frac{p-1}{2}} \equiv -1\ [p]$

(On remarque que : $(2^{\frac{p-1}{2}} - 1)(2^{\frac{p-1}{2}} + 1) = 2^{p-1} - 1$)

2- Soit x une solution de l'équation (E)

0.5 a) Montrer que p et x sont premiers entre eux.

0.5 b) En déduire que : $2^{\frac{p-1}{2}} \equiv 1\ [p]$ (On pourra utiliser le théorème de Fermat)

0.25 3- Montrer que pour tout $k \in \{1,2,...,p-1\}$, p divise C_p^k

(On rappelle que : $(\forall k \in \{1,2,...,p-1\})$ $C_p^k = \dfrac{p!}{k!(p-k)!}$ et que : $kC_p^k = pC_{p-1}^{k-1}$)

0.25 4-a) En utilisant la formule de Moivre, montrer que :

$$(1+i)^p = 2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) + i2^{\frac{p}{2}} \sin\left(p\frac{\pi}{4}\right)$$

(i étant le nombre complexe tel que : $i^2 = -1$)

0.5 b) On admet que : $(1+i)^p = \sum_{k=0}^{k=\frac{p-1}{2}} (-1)^k C_p^{2k} + i \sum_{k=0}^{k=\frac{p-1}{2}} (-1)^k C_p^{2k+1}$

Montrer que : $2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) \in \mathbb{Z}$ et $2^{\frac{p}{2}} \cos\left(p\frac{\pi}{4}\right) \equiv 1\ [p]$ (on pourra utiliser la question3-)

0.5 5- En déduire que si $p \equiv 5\ [8]$ alors l'équation (E) n'admet pas de solution dans $\mathbb{Z}$

Démontrer la propriété suivante :

Soit n un entier naturel, $\sqrt{n}$ est rationnel si, et seulement si n est un carré d'entier.