Nombres premiers

Cours et exercices

Définition

Un nombre premier est un nombre qui n'a que deux diviseurs positifs.
On note $\mathcal{P}$, l'ensemble des nombres premiers.

Ainsi un nombre premier est un nombre qui n'est divisible que par 1 et par lui-même sauf 1.
Par exemple 2, 13, 101.

Proposition Lemme d'Euclide

Soient a, b des entiers et $p \in \mathcal{P}$.

$$p|ab \Longrightarrow (p|a) \vee (p|b)$$

Démonstration. Supposons que p ne divise pas a. Les seuls diviseurs de p et donc du $\text{PGCD}(p, a)$ sont 1 et p et puisque p ne divise pas a on a nécessairement $\text{PGCD}(p, a) = 1$. Le lemme de Gauss permet de conclure que $p|b$. □

Les nombres premiers sont au cœur de l'arithmétique. Ils forment les atomes de tous les nombres.

Théorème Théorème fondamental de l'arithmétique - Gauss

Tout nombre entier non nul se décompose de manière unique, à l'ordre des facteur près, en produit fini de nombre premier.

Démonstration. Montrons l'existence par récurrence sur n. Le nombre 1 est produit d'un nombre fini de nombre premier : aucun (produit sur l'ensemble vide) ce qui prouve le cas initial.

Supposons que tout entier $n < N$ s'écrit comme produit fini de nombre premier et montrons qu'il en est de même pour N. Considérons le plus petit $p \in D(N)$ strictement supérieur à 1 qui existe car cet ensemble est une partie non vide de $\mathbb{N}$ et admet donc un plus petit élément.

Nécessairement p est un nombre premier par minimalité. Mais $N = N'p$ et puisque $N' < N$ il s'écrit comme produit de nombre premier et il en va donc de même pour N.

L'unicité se déduit du lemme d'Euclide. □

Théorème

$$\text{Card}(\mathcal{P}) = +\infty$$

Démonstration. Raisonnons par l'absurde et supposons que $p_1 < p_2 < \cdots < p_n$ sont les seuls premier. Considérons $N = 1 + p_1 \cdot p_2 \cdots p_n$. Le nombre N n'est pas un nombre premier (puisque strictement plus grand que le plus grand des nombres premiers). D'après le théorème fondamental de l'arithmétique, N est divisible par un nombre premier, p_k. Mais puisque $p_1 \cdot p_2 \cdots p_n$ est également divisible par p_k on en déduit que $1 = N - p_1 \cdot p_2 \cdots p_n$ est divisible par p_k et nécessairement $p_k = 1$ qui n'est pas un nombre premier. Absurde. □

Exercice 1

Parmi les nombres suivants identifier ceux qui sont des nombres premiers.

1. 103	5. 587	9. 701	13. 989	17. 1211
2. 247	6. 597	10. 787	14. 991	18. 1311
3. 367	7. 683	11. 809	15. 997	19. 1319
4. 539	8. 693	12. 909	16. 1009	20. 1321

Exercice 2

Soit $p \in \mathcal{P}$ tel que $p > 2$. Montrer qu'il existe $k \in \mathbb{N}$ tel que soit $p = 4k+1$ soit $p = 4k-1$.

Exercice 3

Trouver tous les nombres premiers p tel que $4p+1$ et $7p-4$ soient également premiers. On pourra regarder modulo 3.

Définition

Soit $p \in \mathcal{P}$ et $n \in \mathbb{N}_{>0}$. On appelle **valuation p-adique** de n la plus graphe puissance de p qui apparait dans la décomposition en facteur premier de n. On la note $\nu_p(n)$.

Par exemple $\nu_2(12) = 2$, $\nu_3(12) = 1$ et $\nu_5(12) = 0$.

Corollaire

Soit $n \in \mathbb{N}_{>0}$. La famille $\{\nu_p(n)\}_{p\in\mathcal{P}}$ est une famille d'entier presque tous nul et

$$n = \prod_{p\in\mathcal{P}} p^{\nu_p(n)}$$

Démonstration. Cela se déduit du théorème fondamental de l'arithmétique. □

Proposition

Soient a et b des éléments de $\mathbb{N}_{>0}$ et $p \in \mathcal{P}$.

(i). $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.

(ii). $a|b \iff \left(\forall p \in \mathcal{P},\ \nu_p(a) \leqslant \nu_p(b)\right)$.

(iii). $\nu_p(a^b) = b\nu_p(a)$.

(iv). $\nu_p(\mathrm{PGCD}(a,b)) = \min(\nu_p(a), \nu_p(b))$.

Démonstration.

(i). On a $a = \prod_{p\in\mathcal{P}} p^{\nu_p(a)}$ et $b = \prod_{p\in\mathcal{P}} p^{\nu_p(b)}$ d'où $ab = \prod_{p\in\mathcal{P}} p^{\nu_p(a)+\nu_p(b)}$.

(ii). Si $a|b$ alors il existe $k \neq 0$ tel que $b = ka$ ce qui implique d'après le premier point que $\nu_p(b) = \nu_p(k) + \nu_p(a)$ pour tout $p \in \mathcal{P}$. En particulier $\nu_p(b) \geqslant \nu_p(a)$. Réciproquement : posons $k = \prod_{p\in\mathcal{P}} p^{\nu_p(b)-\nu_p(a)}$.

Alors $b = ka$.

(iii). Beaucoup trop triviale.

(iv). C'est une conséquence de la construction du PGCD.

□

Exercice 4

Calculer.

1. $\nu_3(15)$
2. $\nu_7(120)$
3. $\nu_5(625)$
4. $\nu_2(18)$
5. $\nu_{11}(121)$
6. $\nu_3(18^{2017})$

Exercice 5

Calculer $\nu_2(2^{100} + 2^{200})$.

Théorème Formule de Legendre

Soient $n \in \mathbb{N}_{>0}$ et $p \in \mathcal{P}$.

$$\nu_p(n!) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right]$$

où $[x]$ désigne la partie entière du réel x.

Démonstration. Soit $\alpha_i \in \mathbb{N}$ le plus grand entier tel que $\alpha_i p^i \leqslant n$. Dans ce cas le nombre d'entier inférieur ou égaux à n et divisible par p^i est $\alpha_i = \left[\frac{n}{p^i}\right]$.

Soit n_i le nombre d'entier entre 1 et n de valuation p-adique exactement égale à i. Naturellement $\nu_p(n!) = n_1 + 2n_2 + 3n_3$ etc...

Pour finir on observe que $\left[\frac{n}{p^i}\right] = n_i + n_{i+1}. \cdots$. □

Exercice 6

Calculer $\nu_7(100!)$.

Exercice 7

Déterminer le nombre de 0 à droite dans l'écriture décimale de $10!$. Même question avec $100!$

Exercice 8

Montrer que pour tout entier $n \in \mathbb{N}_{>0}$, $\nu_2(n!) \leqslant n$.

Exercice 9

Soient 111 nombres relatifs de somme nulle. Montrer que la somme de leur puissance 37-ième est divisible par 399.

Les nombres premiers bien que centraux en arithmétiques sont très peu connu. Voici une petite brochette de conjecture lié aux nombres premiers.

Goldbach. Tout nombre paire strictement supérieur à 2 s'écrit comme la somme de deux nombres premiers.

Legendre. Pour tout entier $n > 1$, il existe toujours un nombre premier entre n^2 et $(n+1)^2$.

Sophie Germain. Il existe une infinité de nombre premier p tel que $2p + 1$ est également premier [1].

Mersenne. Il existe une infinité de nombre premier de la forme $2^n - 1$.

Fermat. Il existe une infinité de nombre premier de la forme $2^{2^n} + 1$

Fibonacci. Il existe une infinité de nombre premier qui apparaissent dans la suite de Fibonacci.

Riemann. ...

Malgré les mystères qui entourent ces nombres nous disposons de puissant résultat.

1. Monsieur Le Blanc

Proposition

Soit $p \in \mathcal{P}$ et $0 < k < p$ $\begin{pmatrix} p \\ k \end{pmatrix} = \dfrac{p!}{k!(p-k)!}$ est divisible par p

Démonstration. On observe que $k\begin{pmatrix} p \\ k \end{pmatrix} = p\begin{pmatrix} p-1 \\ k-1 \end{pmatrix}$. Ainsi $p|k\begin{pmatrix} p \\ k \end{pmatrix}$ et puisque k est premier à p le lemme de Gauss prouve que $p|\begin{pmatrix} p \\ k \end{pmatrix}$. □

Théorème Petit théorème de Fermat

Soit $p \in \mathcal{P}$ et $x \in \mathbb{N}$, $x^p \equiv_p x$

Démonstration. On raisonne par récurrence sur x le cas initial étant trivial.
Supposons que pour un x quelconque fixé, $x^p \equiv_p x$. En developpant par le binôme de Newton on a

$$(x+1)^p = \sum_{k=0}^{p} \begin{pmatrix} p \\ k \end{pmatrix} x^k = 1 + x^p + \sum_{k=1}^{p-1} \begin{pmatrix} p \\ k \end{pmatrix}$$

Or entre 1 et $p-1$ tous les coefficients binomiaux sont multiples de p c'est à dire nuls modulo p. En conclusion $(x+1)^p \equiv_p x^p + 1$. Par hypothèse de récurrence, $(x+1)^p \equiv_p x + 1$. □

Corollaire

Soit $p \in \mathcal{P}$ et $x \in \mathbb{N}$ non multiple de p alors $x^{p-1} \equiv_p 1$

Démonstration. Le petit théorème de Fermat affirme que $x^p \equiv_p x$ c'est à dire qu'il existe $k \in \mathbb{Z}$ tel que $x^p - x = kp$ soit encore $x(x^{p-1} - 1) = kp$. Cette dernière égalité implique que $p|(x(x^{p-1} - x))$ or p et x sont premiers entre eux puisque p est premier et x non multiple de p. Le lemme de Gauss permet de conclure que $x^{p-1} - 1$ est multiple de p. □

Exercice 10

1. Montrer que 13 divise $2^{70} + 3^{70}$.
2. Montrer que 11 divise $2^{129} + 3^{118}$.
3. Montrer que $2^{281} + 3^{193}$ est un multiple de 7.

Exercice 11

Pour quelle valeur de n, $5^{6n} + 5^n + 2$ est-il divisible par 7.

Exercice 12

Déterminer les entiers n tel que $72n^5 - 95n^3 + 3n$ est divisible par 5.

Exercice 13

Soit $p \in \mathcal{P}$ tel que $p > 2$. Montrer que s'il existe $k \in \mathbb{N}$ tel que $k^2 \equiv_p -1$ alors $p \equiv_4 1$.