Arithmétique

1 $a\mathbb{N} + b\mathbb{N}$

Soit $a \geq 1$ et $b \geq 1$ deux entiers naturels premiers entre eux.

1- Que dire de $a\mathbb{N} + b\mathbb{N}$?

2- Montrer que $a\mathbb{N} + b\mathbb{N}$ ne contient pas $(a-1)(b-1) - 1$.

3- Montrer que $a\mathbb{N} + b\mathbb{N}$ contient tous les entiers à partir de $(a-1)(b-1)$.

Indications

2- supposons
$$(a-1)(b-1) - 1 = au + bv$$
avec $u, v \in \mathbb{N}^*$. Alors
$$a(b-1-u) = b(v+1)$$
Avec le théorème de Gauss : b divise $b-1-u$, donc b divise $1+u$.

Ensuite, $1+u \geq b$, $u \geq b-1$, $au \geq a(b-1)$, donc
$$(a-1)(b-1) - 1 = au + bv \geq a(b-1)$$
Contradiction.

3- On suppose $n \geq (a-1)(b-1)$. On peut écrire
$$n = au + bv$$
avec $u, v \in \mathbb{Z}$. Alors
$$\forall q \in \mathbb{Z},\ n = a(u - qb) + b(v + qa)$$
Il reste à choisir q ; on utilise la division euclidienne :
$$u = qb + r$$
D'où
$$n = ar + b(v + qa)$$
Il reste à montrer que $v + qa \geq 0$.

2 Nombres de diviseurs, de multiples

Soit $n \in \mathbb{N}^*$.

1- Soit d un entier, $1 \leq d \leq n$. Montrer que le nombre m de multiples de d dans $[\![1, n]\!]$ est
$$\left\lfloor \frac{n}{d} \right\rfloor$$

2- On note d_k le nombre de diviseurs de k. Montrer que
$$\sum_{k=1}^{n} d_k = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor$$

3- On note s_k la somme des diviseurs de k. Montrer que
$$\sum_{k=1}^{n} s_k = \sum_{d=1}^{n} d \left\lfloor \frac{n}{d} \right\rfloor$$

4- Donner un équivalent de $A_n = \sum_{k=1}^{n} d_k$.

Indications

1- $md \leq n < (m+1)\,d$
2- Notons $a_{p,q} = 1$ si p divise q, 0 sinon.

$$\sum_{k=1}^{n} d_k = \sum_{k=1}^{n}\sum_{d=1}^{n} a_{d,k} = \sum_{d=1}^{n}\sum_{k=1}^{n} a_{d,k} = \sum_{d=1}^{n} \left\lfloor \frac{n}{d} \right\rfloor$$

Plus clairement, on compte le nombre de 1 dans une matrice carrée de deux manières différentes.
3-

$$\sum_{k=1}^{n} s_k = \sum_{k=1}^{n}\sum_{d=1}^{n} d.a_{d,k} = \sum_{d=1}^{n}\sum_{k=1}^{n} d.a_{d,k} = \sum_{d=1}^{n} d \left\lfloor \frac{n}{d} \right\rfloor$$

4-

$$A_n \sim n.\ln(n)$$

3 24 divise $p^2 - 1$

Soit $p \geq 5$ un nombre premier ; montrer que 24 divise $p^2 - 1$.

Indications

$3 \wedge 8 = 1$; il suffit donc de montrer que 3 et 8 divisent $p^2 - 1$.
3 divise l'un des nombres $p-1, p, p+1$; il ne divise pas p, donc il divise $p-1$ ou $p+1$.
$p-1$ et $p+1$ sont pairs, et l'un des deux est multiple de 4 ; pourquoi ? Donc 8 divise $p^2 - 1$.

4 247^{349} modulo 7

Trouver avec et sans ordinateur le reste de la division euclidienne de $n = 247^{349}$ par 7.

Indications

Dans $\mathbb{Z}/7\mathbb{Z}$, $\overline{247} = \overline{2}$; on doit donc chercher $\overline{2}^{349}$; or $\overline{2}^3 = \overline{1}$; on étudie donc 349 modulo 3 ; on trouve que

$$349 = 3k + 1$$

Donc $\overline{2}^{349} = \overline{2}^{3k+1} = \left(\overline{2}^3\right)^k.\overline{2} = \overline{2}$; le résultat cherché est 2.

Avec Python

```
u = 1
for k in range(349):
    u = (u * 247) % 7
print(u)
```

Mieux

Utiliser l'algorithme d'exponentiation rapide.

5 $n = 1010...10101$

Soit $n = 1010...10101$, comportant 2020 zéros. Montrer que n n'est pas premier.

Indications

Après calcul : $99n = 100^{2021} - 1 = \left(10^{2021} - 1\right)\left(10^{2021} + 1\right)$.
En déduire une contradiction si n est premier.

6 $a^r - 1$ premier

Soit $a \geq 2$, $r \geq 2$ tels que $a^r - 1$ soit premier. Montrer que $a = 2$ et que r est premier.

Indications

Soit $P = X^r - 1$; on sait que $P = (X-1).Q$ avec $Q = 1 + X + ... + X^{r-1}$; d'où :

$$a^r - 1 = (a-1).Q(a)$$

Donc $a - 1$ divise $a^r - 1$; de plus $1 \leq a - 1 < a^r - 1$; $a^r - 1$ étant premier : $a = 2$.

Ensuite, supposons que r n'est pas premier : $r = s.t$ avec $s \geq 2$ et $t \geq 2$. De manière analogue :

$$P = X^r - 1 = X^{s.t} - 1 = (X^s)^t - 1 = (X^s - 1)R(X)$$

Donc que $a^r - 1$ est divisible par $a^s - 1$, $1 < a^s - 1 < a^r - 1$ et donc $a^r - 1$ non premier.

7 $2^p + 1$

Soit p un entier naturel non nul tel que $n = 2^p + 1$ soit premier. Que dire de p ?

Indications

On calcule les premiers ; une condition nécessaire semble être que p est une puissance de 2 ; montrons le.

Supposons que p n'est pas une puissance de 2 : $p = 2^q.(2r+1)$ avec $r \geq 1$; soit $P = X^{2r+1} + 1$; P se factorise :

$$P = X^{2r+1} + 1 = (X+1).Q(X)$$

Donc $n = \left(2^{2^q} + 1\right) Q\left(2^{2^q}\right)$; n est donc divisible par $n' = 2^{2^q} + 1$, et $1 < n' < n$; dans ce cas, on a bien montré que n n'est pas premier.

8 Diviseurs de $2^p - 1$

Soit $p \geq 3$ premier et k un diviseur premier de $2^p - 1$; montrer que $k \equiv 1\,[2p]$.

Indications

$2^p - 1$ est impair, donc k est impair, donc 2 divise $k - 1$.

Soit G le groupe des inversibles de $\mathbb{Z}/k\mathbb{Z}$, dont le cardinal est $k - 1$.

$$\overline{2}^p \equiv 1\,[k]$$

donc l'ordre de $\overline{2}$ dans G divise p, et n'est pas 1 ; p étant premier, $\overline{2}$ est d'ordre p ; donc p divise $k - 1 = |G|$.

Pour finir, 2 et p sont deux diviseurs de $k - 1$ premiers entre eux, donc $2p$ divise $k - 1$.

9 Inversibles de $\mathbb{Z}/2^n\mathbb{Z}$

Soit $n \geq 3$ un entier ; soit $k = 2^{n-2}$; soit G le groupe des inversibles de $\mathbb{Z}/2^n\mathbb{Z}$: $G = (\mathbb{Z}/2^n\mathbb{Z})^\times$.

1) Quel est le cardinal de G ?

2) Soit a un entier impair ; montrer que $a^k \equiv 1\,[2^n]$.

3) G est-il cyclique ?

Indications

1) Le cardinal de G est $\varphi(2^n) = 2^{n-1}$.
2) Procédons par récurrence sur n : pour $n = 3$,

$$a^k - 1 = a^2 - 1 = (a-1)(a+1)$$

C'est le produit de deux nombres pairs, et l'un des deux est multiple de 4 ; c'est donc un multiple de 8 ; donc

$$a^k \equiv 1\,[8]$$

Soit $n \geq 3$ et supposons la propriété vérifiée pour n ; montrons la pour $n+1$.
On sait que $a^k \equiv 1\,[2^n]$; on peut donc écrire

$$a^k = 1 + p.2^n$$

où p est un entier ; on élève au carré, et on obtient :

$$a^{2k} = 1 + p.2^{n+1} + p^2.2^{2n} = 1 + q.2^{n+1}$$

où q est un entier ; donc

$$a^{2k} \equiv 1\left[2^{n+1}\right]$$

Ce qui termine la démonstration.
3) Soit $\overline{a}$ un élément de G ; a est impair, donc $a^k \equiv 1\,[2^n]$; ou encore :

$$\overline{a}^k = \overline{1}$$

Ce qui prouve que l'ordre de tout élément de G est un diviseur de k ; donc aucun élément de G n'est d'ordre 2^{n-1} ; donc G n'est pas cyclique.

10 Det $(i \wedge j)$

Pour $1 \leq i, j \leq n$, on note

$$a_{i,j} = i \wedge j$$

Montrer que

$$\mathrm{Det}(A) = \prod_{k=1}^{n} \varphi(k)$$

Indications

$$i \wedge j = \sum_{d=1}^{n} \varphi(d).b_{d,i}.b_{d,j}$$

où $b_{i,j} = 1$ si i divise j, 0 sinon.

11 La fonction de Möbius

On note E l'ensemble des suites de complexes $(a_n)_{n\in\mathbb{N}^*}$:

$$E = \mathbb{C}^{\mathbb{N}^*}$$

On définit sur $\mathbb{N}^*$ la fonction μ ainsi :
- $\mu(1) = 1$.
- si n est le produit de r nombres premiers distincts, $\mu(n) = (-1)^r$.
- sinon, $\mu(n) = 0$.

Questions

1- Montrer que si $a \wedge b = 1$, alors $\mu(ab) = \mu(a)\mu(b)$.
2- Montrer que si $n \geq 2$:

$$\sum_{d|n} \mu(d) = 0$$

Une loi de composition interne sur E :
Soit a et b deux éléments de E. On définit $c = a * b$ par

$$c_n = \sum_{d|n} a_d.b_{\frac{n}{d}}$$

3- Montrer que $*$ est commutative.
4- Trouver un élément neutre e.
5- Montrer que $*$ est associative.
6- Trouver l'inverse de μ.
7- Quels sont les éléments de E inversibles ?
8- Une formule d'inversion : soit $(a_n)_{n\geq 1}$ une suite de complexes.
On définit (b_n) par

$$b_n = \sum_{d|n} a_d$$

Montrer que

$$\forall n \geq 1,\ a_n = \sum_{d|n} \mu(d).b_{\frac{n}{d}}$$

9- On note φ l'indicateur d'Euler ; montrer que

$$\forall n \geq 1,\ \varphi(n) = \sum_{d|n} \mu(d).\frac{n}{d}$$

10- Pour ceux qui connaissent les polynômes cyclotomiques : montrer que

$$\forall n \in \mathbb{N}^*,\ \Phi_n(X) = \prod_{d|n} \left(X^d - 1\right)^{\mu\left(\frac{n}{d}\right)}$$

Indications

1- Supposons $\mu(a)$ et $\mu(b)$ non nuls. $a = p_1...p_r$ et $b = q_1...q_s$; dans ce cas :

$$\mu(ab) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(a)\mu(b)$$

2- Soit $n = p_1^{\alpha_1}...p_r^{\alpha_r}$ et $m = p_1...p_r$; on constate que

$$\sum_{d|n} \mu(d) = \sum_{d|m} \mu(d) = \sum_{k=0}^{r} \binom{r}{k}(-1)^k = (1-1)^r = 0$$

3-

$$d \to \frac{n}{d}$$

est une involution de l'ensemble des diviseurs de n.
4- $e_1 = 1$ et $e_n = 0$ si $n \geq 2$.
5- D'abord une remarque : soit $n \in \mathbb{N}^*$, k et d deux diviseurs de n.

$$k|\frac{n}{d} \iff kd|n \iff d|\frac{n}{k}$$

Soit a, b, c trois éléments de E.

$$[a*(b*c)]_n = \sum_{d|n} a_d.\sum_{k|\frac{n}{d}} b_{\frac{n}{kd}}c_k = \sum_{k|n}\left(\sum_{d|\frac{n}{k}} a_d b_{\frac{n}{kd}}\right)c_k = [(a*b)*c]_n$$

6- L'inverse de μ est la suite constante (1) d'après 2.
7- Les (a_n) tels que $a_1 \neq 0$.
8- $b = 1 * a$, donc

$$\mu * b = \mu * (1 * a) = (\mu * 1) * a = a$$

9- On sait que

$$\forall n \in \mathbb{N}^*,\ n = \sum_{d|n} \varphi(d)$$

Autrement dit :

$$(n) = (1) * \varphi$$

10- La question 8 se généralise à tout groupe commutatif, en particulier

$$G = (\mathbb{C}(X) \setminus \{0\}, \times)$$

et on sait que

$$\forall n \in \mathbb{N}^*,\ X^n - 1 = \prod_{d|n} \Phi_d$$

12 Probabilité que $a \wedge b = 1$

On utilise l'exercice précédent, et on admet que

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

1- Montrer que

$$\sum_{i=1}^{\infty} \frac{\mu(i)}{i^2} = \frac{1}{\zeta(2)}$$

2- Soit $x > 1$; montrer que

$$\sum_{1 \leq n \leq x} \varphi(n) = \frac{1}{2} \sum_{1 \leq i \leq x} \mu(i) \left(\left\lfloor \frac{x}{i} \right\rfloor + \left\lfloor \frac{x}{i} \right\rfloor^2 \right)$$

3- Montrer que

$$\sum_{1 \leq n \leq x} \varphi(n) \sim \frac{3x^2}{\pi^2}$$

4- Pour $n \in \mathbb{N}^*$, X_n et Y_n suivent la loi uniforme sur $[\![1, n]\!]$ et sont indépendantes. On note

$$p_n = \mathbb{P}(X_n \wedge Y_n = 1)$$

Trouver la limite de (p_n).
5- Ecrire une fonction Python 'pgcd(a,b)' et l'utiliser pour confirmer le résultat précédent.

Indications

1-

$$\sum_{i=1}^{\infty} \frac{\mu(i)}{i^2} . \zeta(2) = \sum_{i=1}^{\infty} \frac{\mu(i)}{i^2} . \sum_{j=1}^{\infty} \frac{1}{j^2}$$

On note

$$a_{i,j} = \frac{\mu(i)}{i^2} . \frac{1}{j^2}$$

et on utilise le théorème de sommation par paquets avec

$$I_n = \{(i,j) \,/\, ij = n\}$$

et on utilise l'exercice précédent : si $n \geq 2$,

$$s_n = \sum_{(i,j) \in I_n} \frac{\mu(i)}{i^2} . \frac{1}{j^2} = \sum_{(i,j) \in I_n} \frac{\mu(i)}{n^2} = \frac{1}{n^2} . \sum_{i|n} \mu(i) = 0$$

et pour $n = 1$,

$$s_1 = 1$$

2- On montre que pour $i \geq 1$, $\left\lfloor \frac{x}{i} \right\rfloor$ est le nombre de multiples de i inférieurs ou égaux à x.
Et la somme des multiples de i inférieurs ou égaux à x est

$$\frac{i}{2}\left(\left\lfloor \frac{x}{i} \right\rfloor + \left\lfloor \frac{x}{i} \right\rfloor^2\right)$$

3-

$$0 \leq \left(\frac{x}{i}\right)^2 - \left\lfloor \frac{x}{i} \right\rfloor^2 \leq \frac{x}{i} + \left\lfloor \frac{x}{i} \right\rfloor \leq 2.\frac{x}{i}$$

D'où

$$\left| \sum_{1 \leq i \leq x} \mu(i) \left(\left(\frac{x}{i}\right)^2 - \left\lfloor \frac{x}{i} \right\rfloor^2\right) \right| \leq 2x. \sum_{1 \leq i \leq x} \frac{1}{i} = O(x.\ln x)$$

4-

$$\lim_n p_n = \frac{6}{\pi^2}$$

13 Somme des racines primitives de l'unité

Calculer μ_n, somme des éléments de $\mathbb{P}_n$, ensemble des générateurs de $\mathbb{U}_n$.

14 Répartition des nombres premiers

Notations :
$\pi(x)$ est le nombre de nombres premiers inférieurs ou égaux à x.
Pour $n \in \mathbb{N}$:

$$I_n = \int_0^1 t^n (1-t)^n \, \mathrm{d}t$$

1- Montrer que pour $n \geq 3$:

$$I_n \leq \frac{1}{2^{2n+1}}$$

Soit $x_1, ..., x_m$ des entiers naturels et P leur ppcm. On note

$$P = p_1^{\alpha_1} ... p_r^{\alpha_r}$$

où $p_1, ..., p_r$ sont r nombres premiers distincts.
2- Montrer que

$$\forall i,\ p_i^{\alpha_i} \leq \max(x_1, ..., x_m)$$

3- Soit $N = 2n + 1$. Montrer que

$$\pi(N) \geq \ln 2.\frac{N}{\ln N}$$

Indications

1- $I_{n+1} \leq \frac{1}{4}.I_n$ car $\frac{1}{4}$ est le maximum de $t \to t(1-t)$ sur $[0, 1]$.
2- $p_i^{\alpha_i}$ divise l'un des x_j.
3- Vérifier que $I_n.M_n \in \mathbb{N}^*$, avec $M_n = \mathrm{PPCM}(1, 2, ..., N)$.

15 $\ln 2$ est irrationnel

On suppose $\ln 2$ rationnel :

$$\ln 2 = \frac{a}{b}$$

avec a et b dans $\mathbb{N}^*$. Notation :

$$M_n = \text{PPCM}\,(1, 2, ..., n)$$

1- On note

$$I_n = \int_0^1 \frac{x^n}{x+1}\mathrm{d}x$$

Montrer que

$$I_n = (-1)^n \ln 2 + \frac{A_n}{M_n}$$

avec $A_n \in \mathbb{Z}$.

2- Pour $n \geq 1$, on note

$$Q_n = X^n\,(1-X)^n\,,\ P_n = \frac{1}{n!}Q_n^{(n)}$$

Montrer que $P_n \in \mathbb{Z}\,[\mathbb{X}]$.

3- On note

$$J_n = \int_0^1 \frac{P_n\,(x)}{x+1}\mathrm{d}x$$

Montrer que pour tout $n \geq 1$:

$$J_n = \frac{B_n}{b.M_n}$$

avec $B_n \in \mathbb{N}^*$.

4- On note $\pi\,(n)$ le nombre de nombres premiers inférieurs ou égaux à n. On admet que

$$\pi\,(n) \sim \frac{n}{\ln n}$$

Montrer que $M_n \leq 3^n$ à partir d'un certain rang.

5- Conclure.

Indications

1- $x^n = x^n - (-1)^n + (-1)^n$ et $x^n - a^n = ?$

2- Développer avec la formule du binôme.

3- Utiliser 1 pour montrer que B_n est entier et des intégrations par parties pour montrer que $B_n > 0$.

4- On écrit

$$M_n = p_1^{\alpha_1}...p_r^{\alpha_r}$$

où $r = \pi\,(n)$ et on vérifie que pour tout j, $p_j^{\alpha_j} \leq n$; d'où

$$M_n \leq n^r$$

ensuite on remarque que

$$n^r \leq 3^n \Longleftrightarrow \pi\,(n) \leq \ln 3.\frac{n}{\ln n}$$

5- Q2 on a trouvé que

$$J_n = \int_0^1 \frac{Q_n\,(x)}{(x+1)^{n+1}}\mathrm{d}x$$

et

$$\forall x \in [0,1]\,,\ 0 \leq Q_n\,(x) \leq \frac{1}{4^n}$$

Donc :

$$\forall n \geq 1,\ J_n \leq \frac{1}{4^n}$$