



EXERCICES DE
THÉORIE DES NOMBRES

EXERCICE 1.

Niveau : Collège

Auteur : Ruben Ricchiuto (30.12.04)

Mots Clés : Nombres premiers

Énoncé : Démontrer que tout nombre entier positif n se décompose en produit de nombres premiers. [Indication: procéder par récurrence sur n].

Solution :

Par récurrence sur n . Si $n = 1$ il n'y a rien à démontrer. Supposons la proposition vérifiée pour tout $k \leq n$. Si $n + 1$ est premier c'est fini, sinon il existe deux nombres $a, b > 1$ tels que $n + 1 = a \cdot b$. Etant donné que $a, b < n + 1$ on peut appliquer l'hypothèse de récurrence qui nous dit que a et b sont produit de nombres premiers, par conséquent $n + 1$ l'est aussi.

EXERCICE 2.

Niveau : Collège

Auteur : Ruben Ricchiuto (30.12.04)

Mots Clés: Nombres premiers

Énoncé :

Démontrer qu'il y a une infinité de nombres premiers.

Solution :

On va montrer que pour tout entier n il existe un nombre premier $p > n$, ce qui prouvera l'infinité des nombres premiers. Soit donc n un entier. Posons $m := n! + 1$. Soit p un premier qui divise m alors $p > n$ (car sinon p divise $n!$ et par conséquent il divise aussi 1 car $m - n! = 1$).

Autre preuve: supposons que $\{p_1, \dots, p_n\}$ soit l'ensemble des nombres premiers. On pose

$m := \prod_{j=1}^n p_j + 1$. Soit p un premier qui divise m . p n'appartient pas à $\{p_1, \dots, p_n\}$ car sinon p

divise 1 ($m - \prod_{j=1}^n p_j = 1$). Contradiction.

EXERCICE 3.

Niveau : Collège

Auteur : Ruben Ricchiuto (30.12.04)

Mots Clés : irrationalité

Énoncé :

Démontrer que $\sqrt{2}$ est irrationnel. [Indication: supposer que $\sqrt{2} = \frac{p}{q}$ avec $\frac{p}{q}$ irréductible et en déduire que p et q sont pairs ce qui est une contradiction].

Solution :

Si $\sqrt{2} = \frac{p}{q}$ avec $\frac{p}{q}$ irréductible alors $2 \cdot q^2 = p^2$ et p^2 est pair. Ceci entraîne que p est pair et donc $p = 2 \cdot n$. En remplaçant on trouve $2 \cdot q^2 = 4 \cdot n^2$ c'est-à-dire $q^2 = 2 \cdot n^2$. Par le même raisonnement qu'avant ceci implique que q est pair, la fraction $\frac{p}{q}$ n'est donc pas irréductible ce qui est en contradiction avec l'hypothèse de départ.

EXERCICE 4.

Niveau : Premier Cycle

Auteur : Ruben Ricchiuto (30.12.04)

Mots Clés : Nombres irrationnels

Énoncé : Prouver que si $n \in \mathbb{N}$ n'est pas un carré alors \sqrt{n} est irrationnel.

Solution :

Supposons $\sqrt{n} = \frac{p}{q}$ avec p et q premiers entre eux (positifs). Alors $q^2 n = p^2$ et par conséquent q^2 divise p^2 ce qui entraîne $q = 1$. Pour finir $n = p^2$ ce qui est une contradiction.

EXERCICE 5.

Niveau : Premier Cycle

Auteur : Ruben Ricchiuto (30.12.04)

Mots Clés : Nombres premiers

Énoncé :

Démontrer qu'il existe une infinité de nombres premiers congrus à 3 (mod 4).

[Indication: si $\{p_1, \dots, p_n\}$ sont des premiers congrus à 3 (mod 4) considérer l'entier

$$n = 4 \cdot \prod_{j=1}^n p_j - 1].$$

Solution : On suppose qu'il n'existe qu'un nombre fini de premiers congrus à 3 (mod 4)

$\{p_1, \dots, p_n\}$. On considère l'entier $n = 4 \cdot \prod_{j=1}^n p_j - 1$. n est congru à 3 (mod 4) par conséquent il

existe au moins un nombre premier congru à 3 (mod 4) qui divise n et ce nombre n'appartient pas à $\{p_1, \dots, p_n\}$ ce qui est absurde.

EXERCICE 6.*Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Nombres de Liouville, nombres transcendants**Énoncé:**

1. Soit $x \in \mathbb{R}$ un nombre algébrique sur \mathbb{Q} de degré $n > 1$ et $P(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$ irréductible sur \mathbb{Q} tel que $P(x) = 0$. Montrer qu'il existe $C > 0$ tel que pour tout $(p, q) \in \mathbb{Z}^2$ ($q > 0$), $|x - p/q| > \frac{C}{q^n}$. [Indication: distinguer les cas $|x - p/q| > 1$ et $|x - p/q| \leq 1$. Pour ce dernier utiliser le théorème des accroissements finis.]
2. Soit E l'ensemble des suites $(\alpha_i)_{\mathbb{N}^*}$ telles que $\alpha_k \in \{0, 1, \dots, 9\}$ et $\{k \in \mathbb{N}^*, \alpha_k \neq 0\}$ est infini. On appelle nombre de Liouville tout nombre de la forme $\sum_{k=1}^{+\infty} \alpha_k 10^{-k!}$ avec $(\alpha_i)_{\mathbb{N}^*} \in E$. Montrer en utilisant 1. que les nombres de Liouville sont transcendants.
3. Montrer que l'ensemble L des nombres de Liouville n'est pas dénombrable. [Indication: montrer que les applications $f : E \rightarrow L, (\alpha_i)_{\mathbb{N}^*} \mapsto \sum_{k=1}^{+\infty} \alpha_k 10^{-k!}$ et $g : E \rightarrow]0, 1], (\alpha_i)_{\mathbb{N}^*} \mapsto \sum_{k=1}^{+\infty} \alpha_k 10^{-k}$ sont bijectives.]

Solution :

1. Si $|x - p/q| > 1$, $|x - p/q| > \frac{1}{q^n}$. Si $|x - p/q| \leq 1$, par le théorème des accroissements finis on a: $\frac{|P(p/q)|}{|x - p/q|} = |P'(\xi)|$ avec $\xi \in [x-1, x+1]$, d'où $\frac{|P(p/q)|}{|x - p/q|} \leq m$ avec $m = \max_{[x-1, x+1]} |P'(y)|$. Or $|P(p/q)| = \left| \sum_{i=0}^n a_i \frac{p^i}{q^i} \right| = \frac{1}{q^n} \left| \sum_{i=0}^n a_i p^i q^{n-i} \right| \geq \frac{1}{q^n}$ car $P(p/q) \neq 0$ et $\left| \sum_{i=0}^n a_i p^i q^{n-i} \right|$ est entier. Donc, $|x - p/q| \geq \frac{1}{mq^n}$. Dans tous les cas si $C = \frac{1}{m+1}$, $|x - p/q| > \frac{C}{q^n}$.
2. Soit $x = \sum_{k=1}^{+\infty} \alpha_k 10^{-k!}$ un nombre de Liouville. x est irrationnel car il n'a pas de développement décimal périodique. Supposons que x est algébrique. Soit d le degré de

x , on a $d > 1$. Soit $x_n = \sum_{k=1}^n \alpha_k 10^{-k!} = \frac{\sum_{k=1}^n \alpha_k 10^{n!-k!}}{10^{n!}}$ avec $n \geq 1$.

$|x - x_n| = \left| \sum_{k=n+1}^{+\infty} \alpha_k 10^{-k!} \right| \leq 9 \sum_{k=n+1}^{+\infty} 10^{-k!} < \frac{1}{10^{(n+1)!-1}}$. Il existe par 1. une constante $C > 0$

telle que pour tout $n \geq 1$, $\frac{C}{10^{n!d}} < |x - x_n|$. Mais dans ce cas pour tout $n \geq 1$,

$\frac{C}{10^{n!d}} < \frac{1}{10^{(n+1)!-1}}$ c'est-à-dire $C < 10^{n!(d-n-1)+1}$. Or $\lim_{n \rightarrow \infty} 10^{n!(d-n-1)+1} = 0$ et donc $C = 0$,

ce qui contredit l'hypothèse $C > 0$. Par suite, x est transcendant.

3. $f : E \rightarrow L, (\alpha_i)_{\mathbb{N}^*} \mapsto \sum_{k=1}^{+\infty} \alpha_k 10^{-k!}$ est surjective par définition de L . Si $(\alpha_i)_{\mathbb{N}^*}$,

$(\beta_i)_{\mathbb{N}^*} \in E$ et que $\sum_{k=1}^{+\infty} \alpha_k 10^{-k!} = \sum_{k=1}^{+\infty} \beta_k 10^{-k!}$ alors en multipliant par $10^{1!}$ on a

$\alpha_1 + \sum_{k=2}^{+\infty} \alpha_k 10^{-k!+1} = \beta_1 + \sum_{k=2}^{+\infty} \beta_k 10^{-k!+1}$ c'est-à-dire

$\alpha_1 - \beta_1 = \sum_{k=2}^{+\infty} \beta_k 10^{-k!+1} - \sum_{k=2}^{+\infty} \alpha_k 10^{-k!+1} \in]-1, 1[$ d'autre par $\alpha_1 - \beta_1 \in \{-9, \dots, 9\}$ donc

$\alpha_1 = \beta_1$. Une récurrence immédiate montre que $\alpha_n = \beta_n$ pour tout entier $n \geq 1$. f est par conséquent injective et donc bijective. Le même raisonnement montre que

$g : E \rightarrow]0, 1], (\alpha_i)_{\mathbb{N}^*} \mapsto \sum_{k=1}^{+\infty} \alpha_k 10^{-k}$ est injective. La surjectivité de g découle du fait

que tout nombre $\in]0, 1]$ possède un développement décimal infini. Ainsi L n'est pas dénombrable car équipotent à $]0, 1]$.

EXERCICE 7.*Niveau* : Deuxième Cycle*Auteur* : Ruben Ricchiuto (30.12.04)*Mots Clés* : Nombres premiers**Énoncé** : Soit p un nombre premier impair.

1. Montrer que: \mathbb{F}_p^* contient un sous-groupe d'ordre quatre $\Leftrightarrow (-1)$ est un carré dans \mathbb{F}_p .
2. Dédire de 1. que $p \equiv 1 \pmod{4} \Leftrightarrow (-1)$ est un carré dans \mathbb{F}_p .
3. Dédire de 2. qu'il existe une infinité de nombres premiers $\equiv 1 \pmod{4}$.

Solution :

1. Si \mathbb{F}_p^* contient un sous-groupe d'ordre quatre alors il existe $x \in \mathbb{F}_p^*$ d'ordre quatre (nous rappelons que \mathbb{F}_p^* est cyclique) et donc $(x^2)^2 = 1$ ce qui entraîne $x^2 = -1$.
Réciproquement si (-1) est un carré dans \mathbb{F}_p alors il existe $x \in \mathbb{F}_p^*$ tel que $x^2 = -1$ et par suite $x^4 = 1$, x est donc d'ordre quatre.
2. (-1) est un carré dans $\mathbb{F}_p \Leftrightarrow \mathbb{F}_p^*$ contient un sous-groupe d'ordre quatre
 $\Leftrightarrow 4 \mid p-1 \Leftrightarrow p \equiv 1 \pmod{4}$.
3. Supposons que $\{p_1, \dots, p_n\}$ soit l'ensemble des nombres premiers $\equiv 1 \pmod{4}$.

Considérons l'entier $x = (2 \cdot p_1 \cdot \dots \cdot p_n)^2 + 1$. On remarque que les p_i ne divisent pas x .
 $x \equiv 1 \pmod{4}$ et par suite x ne peut pas être premier. Soit p un premier qui divise x .

Alors $x = (2 \cdot p_1 \cdot \dots \cdot p_n)^2 + 1 = 0$ dans \mathbb{F}_p c'est-à-dire $(2 \cdot p_1 \cdot \dots \cdot p_n)^2 = -1$ dans \mathbb{F}_p et par 2. ceci entraîne $p \equiv 1 \pmod{4}$. Etant donné que $p \notin \{p_1, \dots, p_n\}$ il y a contradiction.