Devoir Maison n° 6

Exercice (facultatif) - Grand théorème de Fermat pour $n = 4$

Le but de cet exercice est de prouver qu'il n'existe pas de solutions dans $\mathbb{Z}$ non triviales (i.e. avec $XYZ \neq 0$) à l'équation $X^4 + Y^4 = Z^4$. On se place dans un premier temps dans $\mathbb{N}$: on raisonne par l'absurde et on suppose qu'il existe trois entiers naturels X, Y, Z tous non nuls solutions de cette équation, et on veut arriver à une absurdité.

1. Justifier qu'il existe x, y, z dans $\mathbb{N}^*$ avec x et y premiers entre eux tels que $x^4 + y^4 = z^2$. On pourra utiliser et généraliser l'exercice 15 du poly.
2. D'après l'exercice 49, il existe u et v dans $\mathbb{N}^*$ premiers entre eux tels que
$$x^2 = u^2 - v^2, y^2 = 2uv, z = u^2 + v^2 \qquad \text{ou} \qquad x^2 = 2uv, y^2 = u^2 - v^2, z = u^2 + v^2$$
On supposera dans la suite qu'on est dans le premier cas. Justifier que u et v sont de parité différente. En étudiant la congruence de x^2 modulo 4, prouver que u est impair et v pair : il existe donc $w \in \mathbb{N}^*$ tel que $v = 2w$.
3. En exprimant y^2 en fonction de u et de w, prouver que u et w sont des carrés (on pourra utiliser l'exercice 15 du poly).
4. Justifier que x et v sont premiers entre eux. Calculer $x^2 + v^2$, et en déduire qu'il existe b et c premiers entre eux tels que $v = 2bc$ et $u = b^2 + c^2$.
5. Justifier qu'il existe x_1 et y_1 dans $\mathbb{N}^*$ premiers entre eux tels que $b = {x_1}^2$ et $c = {y_1}^2$.
6. Exhiber une solution (x_1, y_1, z_1) avec $x_1 y_1 z_1 \neq 0$, à l'équation $x^4 + y^4 = z^2$, avec $0 < z_1 < z$, et aboutir à une absurdité.
7. Justifier que l'équation de Fermat n'admet aucune solution non triviale dans $\mathbb{Z}$.

Problème - Presque le théorème des nombres premiers

Si $n \in \mathbb{N}$, $\pi(n)$ désigne le nombre de nombres premiers inférieurs ou égaux à n. Le but de ce problème est de donner une version faible du théorème des nombres premiers. Le théorème des nombres premiers est un résultat difficile stipulant que $\pi(n) \sim \dfrac{n}{\ln(n)}$ (nous verrons les équivalents au second semestre) c'est-à-dire que
$$\pi(n) \times \frac{\ln(n)}{n} \xrightarrow[n \to +\infty]{} 1$$
Nous nous contenterons dans ce devoir d'un résultat plus faible : le but de ce devoir est de prouver que, pour tout $n \geq 9$,
$$\ln(2) \times \frac{n}{\ln(n)} \leq \pi(n) \leq e \times \frac{n}{\ln(n)}$$
Commençons par quelques notations :

- Comme en classe, on note $\mathbb{P}$ l'ensemble des nombres premiers.
- Dans tous le sujet, la lettre p désignera exclusivement un nombre premier, y compris lorsque la lettre p est utilisée comme indice d'une somme ou d'un produit. Par exemple, si x est un réel quelconque, la notation $\displaystyle\sum_{p \leq x} \frac{1}{p}$ désigne la somme des inverses des nombres premiers p inférieurs ou égaux à x. Par conséquent, on fera bien attention à ne jamais appeler un indice p sauf lorsque cela désignera un nombre premier.
- Pour tout entier $n \geq 0$, on note $\pi(n)$ le nombre de nombres premiers inférieurs ou égaux à n. Par exemple, $\pi(0) = \pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = \pi(4) = 2$ etc. Cela va sans dire mais je le dis quand même : $\pi(n)$ n'a absolument aucun rapport avec le nombre π !
- Pour tout $n \geq 1$, on note $\Delta_n = \text{PPCM}(1, 2, \ldots, n)$.
- Étant donnés un entier $n \geq 1$ et un nombre premier p, on rappelle que la valuation p-adique de n, notée $v_p(n)$, est l'exposant de p dans la décomposition en produit de facteurs premiers de n. Par exemple, si on prend $n = 350 = 2 \times 5^2 \times 7$, on a $v_2(n) = v_7(n) = 1$, $v_5(n) = 2$ et $v_p(350) = 0$ pour tout nombre premier $p \neq 2, 5, 7$.
- On rappelle les propriétés suivantes :

- ⋆ Pour tout $n \geq 1$, la suite $(v_p(n))_{p\in\mathbb{P}}$ ne contient qu'un nombre fini de termes non nuls, de sorte que l'on peut écrire
$$n = \prod_{p\in\mathbb{P}} p^{v_p(n)}$$
ce produit pouvant être alors considéré comme un produit fini. Cette écriture n'est alors rien d'autre que la décomposition en produit de facteurs premiers de n.
- ⋆ Pour tous n, m entiers naturels non nuls et $p \in \mathbb{P}$, on a : $v_p(nm) = v_p(n) + v_p(m)$.
- ⋆ Enfin, pour tous a et b entiers naturels non nuls, $v_p(a \vee b) = \max(v_p(a), v_p(b))$.

Les deux dernières propriétés se généralisent aisément à un plus grand nombre d'entiers.

Partie I - Minoration de la fonction π

1. On se donne dans cette question et la suivante deux entiers naturels a et b vérifiant $1 \leq b \leq a$ et on pose
$$I(b,a) = \int_0^1 x^{b-1}(1-x)^{a-b}\,\mathrm{d}x$$
   (a) Expliciter $I(1,a)$ en fonction de a.
   (b) Soit $y \in [\,0\,;1\,[$. À l'aide du binôme de Newton, montrer que :
$$\int_0^1 (1-x+xy)^{a-1}\,\mathrm{d}x = \sum_{k=1}^{a} \binom{a-1}{k-1} y^{k-1} I(k,a)$$
   (c) En calculant maintenant directement l'intégrale, prouver que
$$\int_0^1 (1-x+xy)^{a-1}\,\mathrm{d}x = \frac{1}{a}\sum_{k=1}^{a} y^{k-1}$$
   (d) En admettant que deux fonctions polynomiales qui coïncident en une infinité de points ont les mêmes coefficients, prouver que :
$$I(b,a) = \frac{1}{a\binom{a-1}{b-1}} = \frac{1}{b\binom{a}{b}}$$
2. (a) Montrer que
$$I(b,a) = \sum_{k=0}^{a-b} (-1)^k \binom{a-b}{k} \frac{1}{k+b}$$
   (b) En déduire que $I(b,a) \times \Delta_a \in \mathbb{N}$. On rappelle que Δ_a est le PPCM des entiers $1, 2, \dots, a$.
   (c) Prouver finalement que l'entier $b\dbinom{a}{b}$ divise l'entier Δ_a.

   On se donne dans la suite un entier $n \geq 9$.

3. (a) Justifier que Δ_{2n} divise Δ_{2n+1}. En déduire que les entiers $n\dbinom{2n}{n}$ et $(2n+1)\dbinom{2n}{n}$ divisent l'entier Δ_{2n+1}.
   (b) Justifier que n et $2n+1$ sont premiers entre eux. En déduire que $n(2n+1)\dbinom{2n}{n}$ divise Δ_{2n+1}.
4. (a) On rappelle (cf. exercice 44 du chapitre 3) que, pour tout $k \in [\![0\,;\,2n]\!]$,
$$\binom{2n}{k} \leq \binom{2n}{n}$$
   Montrer que $(2n+1)\dbinom{2n}{n} \geq 4^n$. On pourra développer l'égalité $4^n = (1+1)^{2n}$.
   (b) En déduire que $\Delta_{2n+1} \geq n4^n$.
   (c) Montrer que $\Delta_n \geq 2^n$ (on rappelle que $n \geq 9$). Cette inégalité est-elle encore vraie pour $n = 7$ et $n = 8$?
5. (a) Justifier que
$$\Delta_n = \prod_{p\leq n} p^{v_p(\Delta_n)}$$

(b) Soit $p \in \mathbb{P}$. En utilisant le fait que $v_p(\Delta_n) = \max(v_p(1), \dots, v_p(n))$, montrer que $p^{v_p(\Delta_n)} \leq n$.

(c) En déduire que $\Delta_n \leq n^{\pi(n)}$.

6. Montrer que pour tout $n \geq 7$, on a :

$$\pi(n) \geq \ln(2) \times \frac{n}{\ln(n)}$$

Pour quels entiers $n \in \{2; 3; 4; 5; 6\}$ cette inégalité est-elle encore vraie ? On pourra utiliser la calculatrice dans cette question.

Partie II - Majoration de la fonction π

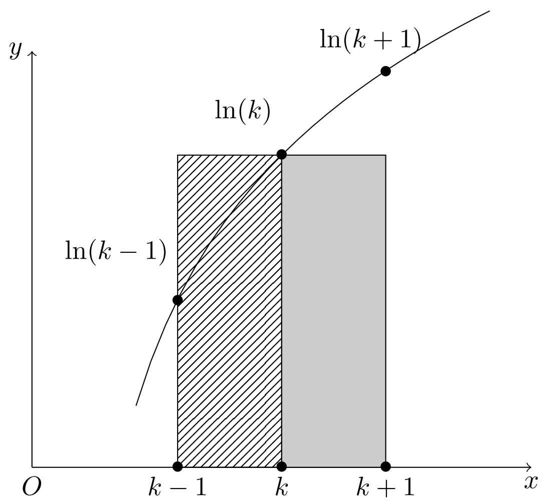
1. (a) Montrer que pour tout $m \in \mathbb{N}$, $\binom{2m+1}{m} \leq 4^m$.

(b) Soit p un nombre premier vérifiant $m+1 < p \leq 2m+1$. Montrer que p divise $\binom{2m+1}{m}$. En déduire que

$$\prod_{m+1<p\leq 2m+1} p \leq 4^m$$

(c) Montrer par récurrence que pour tout $n \geq 2$, $\prod_{p \leq n} p \leq 4^n$.

2. (a) Soit $k \geq 2$. Montrer que $\int_{k-1}^{k} \ln(t)\,\mathrm{d}t \leq \ln(k) \leq \int_{k}^{k+1} \ln(t)\,\mathrm{d}t$. On s'inspirera du dessin :



(b) En déduire que $\ln(k-1) \leq \int_{k-1}^{k} \ln(t)\,\mathrm{d}t \leq \ln(k)$.

(c) Montrer que pour tout $m \geq 2$ on a $\ln((m-1)!) \leq m\ln(m) - m + 1 \leq \ln(m!)$ (on pourra utiliser librement le fait que $x \mapsto x\ln(x) - x$ est une primitive de la fonction ln). En déduire que

$$e\left(\frac{m}{e}\right)^m \leq m! \leq me\left(\frac{m}{e}\right)^m$$

3. Déduire de ce qui précède que, pour tout $n \geq 2$, on a $\pi(n)! \leq 4^n$ puis que :

$$\pi(n) \times \ln(\pi(n)) - \pi(n) \leq n\ln(4)$$

4. On souhaite montrer, à partir du résultat précédent, que pour tout entier $n \geq 3$, on a :

$$\pi(n) \leq e \times \frac{n}{\ln(n)}$$

Pour cela, on raisonne par l'absurder et on suppose qu'il existe un entier $n_0 \geq 3$ tel que $\pi(n_0) > e \times \frac{n_0}{\ln(n_0)}$.

(a) Donner le tableau de variations de $f : x \mapsto x\ln(x) - x$ sur $[\,1\,;+\infty\,[$. En déduire que :

$$\frac{e - \ln(4)}{e} < \frac{\ln(\ln(n_0))}{\ln(n_0)}$$

(b) Montrer que la fonction $x \mapsto \frac{\ln(x)}{x}$ est majorée par e^{-1} sur $\mathbb{R}_+^*$ et conclure.