Problème FERMAT

1 Introduction

En 1637 (si, si), Pierre de Fermat énonce en marge de son traité d'arithmétique ce qui est maintenant connu comme le célèbre théorème de Fermat, l'une des questions les plus fameuses de l'histoire des mathématiques. Il aura fallu pas moins de 350 ans pour qu'enfin cet énoncé soit démontré par Andrew Wiles en 1994. Il vous faudra quelques heures pour en démontrer une partie : « Il n'y a pas d'entier x, y, et z tels que $x^3+y^3=z^3$. »

(Le théorème de Fermat dit qu'il n'y a pas d'entiers x, y et z tels que $x^n+y^n=z^n$, ceci pour tout entier $n>2$.)

$\mathbb{N}$ désigne l'ensemble des engtiers naturels $\{0;1;2;\cdots\}$

$\mathbb{Z}$ désigne l'ensemble des entiers relatifs $\{\cdots;-2;-1;0;1;2;\cdots\}$

$\mathbb{R}$ désigne l'ensemble des nombres réels. $\mathbb{C}$ désigne l'ensemble des nombres complexes.

Les questions 11 ; 12 ; 13 ; 14 ; 17 et 18 sont très faciles

On note c le complexe défini par $\boxed{c=e^{i\frac{2\pi}{3}}=-\frac{1}{2}+i\frac{\sqrt{3}}{2}}$

On note $\mathbb{Z}[c]$ l'ensemble des complexes de la forme $a+cb$ où a et b sont dans $\mathbb{Z}$.

On définit sur $\mathbb{C}$ l'application N par $N(z)=|z|^2=x^2+y^2$ lorsque $z=x+iy$.

On note enfin le complexe $\boxed{f=1-c}$

11. Vérifier que $N(f)=3$.

12. Montrer que si $z=a+cb$, alors $N(z)=a^2-ab+b^2$.

En déduire que si $z\in\mathbb{Z}[c]$, alors $N(z)\in\mathbb{N}$.

13. Vérifier que $N(zz')=N(z)N(z')$ pour tout z et z' appartenant à $\mathbb{C}$.

14. Montrer que $c^2=-1-c$.

En déduire que $\mathbb{Z}[c]$ est stable pour la multiplication, c'est à dire que :

Si z et z' sont deux complexes de $\mathbb{Z}[c]$, alors le produit z.z' est encore dans $\mathbb{Z}[c]$.

15. Montrer que si $z=a+cb\in\mathbb{Z}[c]$, alors $N(z)$ n'est jamais égal à 2.

Indication : Lorsque a et b ont le même signe, on peut utiliser la formule $a^2-ab+b^2=(a-b)^2+ab$.

16. On dit que $z\in\mathbb{Z}[c]$ est **inversible** lorsqu'il existe $z'\in\mathbb{Z}[c]$ tel que $z.z'=1$.

z' s'appelle alors l'**inverse** de z.

Montrer que : si $z\in\mathbb{Z}[c]$ est inversible, alors N(z)=1

En déduire que 3 n'est pas inversible. (eh bien, eh bien, il suffit de calculer $N(3)$!)

17. Montrer que c est inversible. (on pourra calculer $c.c^2$) Quel est l'inverse de c ?

18. Montrer que f n'est pas inversible. (eh bien, eh bien, hein ?)

19. Prouver que $\mathbb{Z}[c]$ n'a que six éléments inversibles qui sont : ±1 ; $\pm c$; $\pm(1+c)$.

(Pour cela, on pourra commencer par résoudre l'équation $N(z)=1$)

En déduire que : $\boxed{\text{si } z\in\mathbb{Z}[c] \text{ , alors « z est inversible } \Longleftrightarrow N(z)=1 \text{ »}}$

2 Construction d'une division euclidienne dans $\mathbb{Z}[c]$.

21. a et b sont des entiers relatifs fixés. c est toujours le même ! $c = e^{i\frac{2\pi}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$

Vérifier que les quatre points A ; B ; D ; G d'affixes respectifs a+cb ; a+1+cb ; a+c(b+1) ; (a+1)+c(b+1) forment un parallélogramme. (on pourra calculer l'affixe de $\overrightarrow{AB}$ et de $\overrightarrow{DG}$)

Faites un beau dessin lorsque a=5 et b=1.

22. Montrer que le cercle de centre B de rayon 1 passe par A et G.

Idem avec le cercle de centre D et de rayon 1.

23. Pour x réel, on note **E(x)** la partie entière de x. C'est le plus grand entier inférieur ou égal à x.

Ainsi, par exemple, $E(1,7) = 1$; $E(3) = 3$ et $E(-8,6) = -9$.

Soit z et z' appartenant à $\mathbb{Z}[c]$, z et z' étant non nuls.

On cherche à prouver l'existence de q et r appartenant à $\mathbb{Z}[c]$ tels que $\begin{cases} z = z'q + r \\ N(r) < N(z') \end{cases}$.

Dans $\mathbb{C}$, $\frac{z}{z'} = x + iy = \alpha + c\beta$ où α et β sont des réels.

Avec $a = E(\alpha)$ et $b = E(\beta)$, on récupère les quatre points de la question 21.

En utilisant le fait que l'image du complexe $\frac{z}{z'}$ est à l'intérieur du parallélogramme ABGD, montrer qu'il existe $q \in \mathbb{Z}[c]$ tel que $|\frac{z}{z'} - q| < 1$.

24. On pose $r = z - z'q$. Vérifier que $r \in \mathbb{Z}[c]$ et que $N(r) < N(z')$. Conclure.

3 Décomposition en produits de facteurs irréductibles.

Les questions 31 à 33 sont très faciles.

31. Quelques exemples :

Dans $\mathbb{N}$, $48 = 2^4.3$. Les entiers 2 et 3 sont dits irréductibles ou premiers dans $\mathbb{N}$.

On dit qu'on a décomposé 48 en produit de facteurs irréductibles.

Les nombres premiers dans $\mathbb{N}$ sont 2 ; 3 ; 5 ; 7 ; 11 ; 13 ; $\cdots$

Décomposer dans $\mathbb{N}$ le nombre 15120.

32. On dit que $z \in \mathbb{Z}[c]$ est **irréductible** dans $\mathbb{Z}[c]$ lorsque :

« $z = z_1.z_2 \Longrightarrow z_1$ ou z_2 est l'un des six inversibles de $\mathbb{Z}[c]$ (trouvés dans la question 19) »

Par exemple, montrons que 2 est irréductible dans $\mathbb{Z}[c]$:

Si $2 = z_1.z_2$, alors $4 = N(z_1.z_2) = N(z_1).N(z_2)$.

Il y a trois possibilités :

$N(z_1) = 2$ et $N(z_2) = 2$. Ceci est impossible d'après la question 15.

$N(z_1) = 1$ et $N(z_2) = 4$. z_1 est inversible.

$N(z_1) = 4$ et $N(z_2) = 1$. z_2 est inversible.

Donc 2 est irréductible dans $\mathbb{Z}[c]$.

Montrer que f est irréductible dans $\mathbb{Z}[c]$. (on a déja calculé N(f))

33. Décomposer dans $\mathbb{Z}[c]$ le complexe 2-2c en produit de fateurs irréductibles.

34. Décomposer dans $\mathbb{Z}[c]$ le complexe 3 en produit de facteurs irréductibles.

(pensez à f et à son conjugué)

4 Une particularité des cubes de $\mathbb{Z}[c]$.

Les questions 45 et 46 sont faciles.

Bien que longues, les questions 41 à 43 sont uniquement calculatoires.

Désormais, on note ε l'un des six inversibles de $\mathbb{Z}[c]$.

41. Remplir le tableau suivant dans lequel on exprimera les carrés, les cubes et les inverses des six inversibles **de la forme a+cb** où a et b sont des entiers. On justifiera les résultats obtenus.

On pourra utiliser les formules : $c^2 = -1 - c$ et $c^3 = 1$.

ε	1	-1	c	-c	$-c^2 = 1 + c$	$c^2 = -(1 + c)$
ε^2						
ε^3					-1	
$\frac{1}{\varepsilon}$						

42. Remplir le tableau suivant dans lequel on exprimera le complexe $(\varepsilon')^2 - c^2\varepsilon^2$ de la forme a+cb.

N'oubliez pas de justifier.

	$\varepsilon^2 = 1$	$\varepsilon^2 = c$	$\varepsilon^2 = -1 - c$
$(\varepsilon')^2 = 1$	$2 + c$		
$(\varepsilon')^2 = c$			
$(\varepsilon')^2 = -1 - c$	0		

43. Remplir le même tableau en écrivant les résultats de la forme $f.z$ où $z \in \mathbb{Z}[c]$.

Justifiez, bien sûr !

	$\varepsilon^2 = 1$	$\varepsilon^2 = c$	$\varepsilon^2 = -1 - c$
$(\varepsilon')^2 = 1$	$f.(1 + c)$		
$(\varepsilon')^2 = c$			
$(\varepsilon')^2 = -1 - c$	$f.0$		

En conclure que tous les $(\varepsilon')^2 - c^2\varepsilon^2$ sont divisibles par f.

44. Montrer que si $p \in \mathbb{Z}[c]$ et n'est pas divisible par f, alors le reste de la division de p par f est l'un des six inversibles. (on étudiera $N(r)$ où r est le reste de la division euclidienne de p par f)

Désormais, on suppose que $p \in \mathbb{Z}[c]$ et que p n'est pas divisible par f.

En vertu de la question 44, on peut donc écrire $p = fq + \varepsilon$ où $q \in \mathbb{Z}[c]$

45. Développer $p^3 = (fq + \varepsilon)^3$ grâce à la formule du binôme. Vérifier que $3 = -f^2c^2$

46. En déduire que $p^3 - \varepsilon^3 = f^3q(q^2 - c^2\varepsilon^2 - fc^2q\varepsilon)$

47. Si q n'est pas divisible par f, alors on peut l'écrire $q = fq' + \varepsilon'$ où $q' \in \mathbb{Z}[c]$ d'après la question 44.

Développer $q^2 = (fq' + \varepsilon')^2$ et en déduire que $q^2 - c^2\varepsilon^2$ est divisible par f.

48. En déduire que $p^3 - \varepsilon^3$ est divisible par f^4.

49. En déduire la propriété suivante :

Si $p \epsilon \mathbb{Z}[c]$ n'est pas divisible par f, alors $p^3 + 1$ ou $p^3 - 1$ est divisible par f^4

5 Démonstration de « $x^3 + y^3 + \varepsilon z^3 = 0$ n'a pas de solution dans $\mathbb{Z}[c]$ »

En particulier, lorsque $\varepsilon = -1$, on aura montré le théorème de Fermat quand n = 3.

51. Première simplification du problème :

On dit que z_1 et z_2 sont premiers entre eux dans $\mathbb{Z}[c]$ lorsqu'ils n'ont pas de diviseurs irréductibles communs.

Dans cette question, on veut montrer que l'existence de x ; y et z non nuls tels que $x^3 + y^3 + \varepsilon z^3 = 0$ peut se ramener au cas où x ; y et z sont premiers entre eux deux à deux.

Expliquez en moins de 37 mots que si p est irréductible de $\mathbb{Z}[c]$, divise deux des x ; y et z, alors il divise le troisième.

Ainsi on peut désormais supposer que x ; y et z sont premiers entre eux deux à deux.

52. Montrer que $N(\pm 1 \pm 1 \pm \varepsilon) \leq 9$. (on pourra utiliser l(inégalité triangulaire)

Montrer que si $k \in \mathbb{Z}[c]$, et $k \neq 0$, alors $N(kf^4) \geq 81$.

Montrer que $\pm 1 \pm 1 \pm \varepsilon$ ne peut pas être nul.

En déduire qu'au moins un des trois x ; y et z est divisible par f. (on utilise la question 49)

FIN POUR AUJOURD'HUI

La suite n'est pas à faire aujourd'hui. C'est la fin de la démonstration de ce petit théorème de Fermat.

Un petit cadeau pour ceux que ça intéresse.

53. Deuxième simplification :

Dans cette question, on veut montrer que l'existence de x ; y et z non nuls tels que $x^3 + y^3 + \varepsilon z^3 = 0$ peut se ramener au cas où x ; y et z sont premiers entre eux deux à deux et où f divise z (et z seulement)

Si f divise deux des x ; y et z, alors il divise clairement le troisième.

Supposons que f divise x (et x seulement)

Alors, $\frac{1}{\varepsilon}x^3 + \frac{1}{\varepsilon}y^3 + z^3 = 0$; c'est à dire $\varepsilon' x^3 + \varepsilon' y^3 + z^3 = 0$ où ε' est l'un des six inversibles.

Montrer qu'il existe $k \in \mathbb{Z}[c]$ tel que $kf^3 = \pm\varepsilon' \pm 1$. Montrer que $k = 0$. En déduire que $\varepsilon' = \pm 1$.

Si $\varepsilon' = 1$, on est ramené à l'équation $x^3 + y^3 + z^3 = 0$.

Si $\varepsilon' = -1$, en posant $X = z$; $Y = -y$ et $Z = x$, on est ramené à $X^3 + Y^3 + \varepsilon Z^3 = 0$ et f divise Z .

Conclure.

On suppose dorénavant que $x^3 + y^3 + \varepsilon z^3 = 0$; que x, y et z sont premiers entre eux deux à deux dans $\mathbb{Z}[c]$; et que f divise z et z seulement.

54. Montrer que $\varepsilon z^3 = kf^4$. En déduire que f^2 divise z.

On définit n en supposant que f^n divise z, mais que f^{n+1} ne divise pas z.

On a donc $n \geq 2$ d'aprés 54.

55. Vérifier que $(x+y)(x+cy)(x+c^2y) = -\varepsilon z^3$.

On note $\alpha = x + y$; $\beta = x + cy$ et $\gamma = x + c^2y$.

Comme f divise z, f divise α, β ou γ. On suppose que f divise α. Montrer que f divise β et γ.

(on remplace c par sa valeur en fonction de f dans β et γ)

Ainsi, f divise α, β et γ.

56. On suppose que f^2 divise α et β. En déduire que f divise y.

On aboutit ainsi à une contradiction.

Montrer plus généralement que f^2 divise un seul des termes α, β et γ.

57. Montrer que si p irréductible dans $\mathbb{Z}[c]$ divise α, β et γ, alors $p = \varepsilon' f$ où ε' est l'un des six irréductibles

indication : p divise $\alpha + \beta + \gamma$.

58. Quitte à remplacer y par cy ou par c^2y dans la formule $\alpha\beta\gamma = -\varepsilon z^3$, on peut supposer que f^2 divise c.

Montrer qu'il existe des éléments x' ; y' et z' de $\mathbb{Z}[c]$, premiers entre eux deux à deux , non divisibles par f, et des éléments inversibles ε_1 ; ε_2 et ε_3 tels que l'on ait $\alpha = \varepsilon_1 f x'^3$; $\beta = \varepsilon_2 f y'^3$ et $\gamma = \varepsilon_3 f^{3n-2} z'^3$

59. Vérifier que $\alpha + c\beta + c^2\gamma = 0$.

En déduire qu'il existe des inversibles ε'_1 et ε'_2 tels que $x'^3 + \varepsilon'_1 y'^3 + \varepsilon'_2 f^{3n-3} z'^3 = 0$.

Montrer que $\varepsilon'_1 = \pm 1$. (on procède comme dans la question 53)

Expliquer en moins de 37 mots comment on aboutit à une contradiction.

Conclure.