Semaine 11 - Arithmétique dans $\mathbb{Z}$

Valentin De Bortoli
email : valentin.debortoli@gmail.com

1 Le théorème de Lagrange

Soit G un groupe fini. Soit H un sous groupe de G.

1 Soit $a \in G$. Montrer que le cardinal de aH est le même que celui de H.

2 Montrer que $aH \cap bH \neq \emptyset \Rightarrow aH = bH$.

3 Montrer que $G = \underset{g \in G}{\cup} gH$.

4 En déduire que le cardinal d'un sous groupe divise toujours le cardinal du groupe.

5 Soit $H_x = \{x^n, n \in \mathbb{N}\}$. On appelle **ordre** de x le cardinal de ce sous-groupe. Montrer que l'ordre de x divise le cardinal du groupe.

2 Le théorème de Cayley

Soit G un groupe fini. On note $\mathfrak{S}_G$ l'ensemble des bijections de G dans G. On note τ_x ($x \in G$) la fonction qui va de G dans G et qui est définie par $\forall g \in G,\ \tau_x(g) = xg$.

1 Vérifier que τ_x est un élément de $\mathfrak{S}_G$.

2 Vérifier que $\mathfrak{S}_G$ est un groupe.

3 Montrer que ϕ qui va de G dans $\mathfrak{S}_G$ définie par $\phi(x) = \tau_x$ est un morphisme de groupe injectif.

4 En déduire que G est isomorphe à un sous groupe de $\mathfrak{S}_G$.

3 Nombres réels et sous groupes

Soit G un sous groupe de $(\mathbb{R}, +)$ non réduit à un élément. On note $G_+ = G \cap \mathbb{R}_+^*$. On note $x_0 = \inf G_+$.

1 Vérifier que x_0 est bien défini.

2 Montrer que si $x_0 = 0$ alors G est dense dans $\mathbb{R}$.

3 Montrer que si $x_0 \neq 0$ alors $x_0 = \min G_+$, c'est-à-dire $x_0 \in G_+$.

4 Montrer alors que $G = x_0\mathbb{Z}$.

5 Conclure sur la forme des sous-groupes du groupe additif $(\mathbb{R}, +)$

4 Carrés parfaits

Soit $n \in \mathbb{N}$ si il existe $m \in \mathbb{N}$ tel que $n = m^2$. On dit que n est un carré parfait.

1 Montrer que $\forall n \in \mathbb{N}$, $8n + 7$ n'est pas un carré parfait.

2 Montrer que la somme de cinq nombres consécutifs au carré n'est pas un carré parfait.

5 Implication et primalité

Soit p un nombre premier.

1 Montrer que $8p^2 + 1$ premier $\Rightarrow 8p^2 - 1$ premier.

Remarque : on pourra différencier les cas selon la valeur de p modulo 3.

6 Puissance et nombres premiers entre eux

1 Montrer que $\forall n \in \mathbb{N},\ (1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$ avec a_n et b_n deux entiers.

2 Montrer que $a_n \wedge b_n = 1$.

7 Équations et arithmétique

Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

1

$$\begin{cases} x + y = 56 \\ x \vee y = 105 \end{cases}$$

2

$$\begin{cases} x \wedge y = x - y \\ x \vee y = 72 \end{cases}$$

3 $x \vee y - x \wedge y = 243$

8 Nombres de Fermat

1 Soit $N = 2^m + 1$. Montrer que si N est premier alors m est une puissance de 2.

2 On note $F_n = 2^{2^n} + 1$ le n-ième nombre de Fermat. Montrer que deux nombres de Fermat distincts sont premiers entre eux.

3 A votre avis, ces nombres sont-ils premiers ?

9 Nombres de Mersenne

1 Soit $N = a^m - 1$. Montrer que si N est premier alors $a = 2$ et m est un nombre premier

2 On note $M_n = 2^{p_n} - 1$ le n-ième nombre de Mersenne (où p_n est une énumération des nombres premiers). Montrer que deux nombres de Mersenne distincts sont premiers entre eux.

Remarque : les plus grands nombres premiers trouvés à ce jour sont des nombres de Mersenne. En cette fin de décembre 2016 le plus grand nombre premier identifié est un nombre de Mersenne. Il comporte 22 338 618 chiffres (projet GIMPS).

10 Triplets pythagoriciens

On appelle triplet pythagoricien tout triplet $(x, y, z) \in \mathbb{Z}^3$ tel que $x^2 + y^2 = z^2$.

1 Exhiber un tel triplet.

2 Montrer que l'on peut se restreindre au cas où x, y et z sont premiers entre eux dans leur ensemble.

3 Montrer qu'alors ils sont premiers entre eux deux à deux.

4 Dans ce cas, montrer que deux sont impairs et que z est impair. On suppose alors que $y = 2y'$ et x et z impairs.

5 On pose $X = \frac{x+z}{2}$ et $Z = \frac{z-x}{2}$. Montrer que $X \wedge Z = 1$ et que X et Z sont des carrés parfaits.

6 En déduire l'ensemble des triplets pythagoriciens.

Remarque : il n'existe pas de solutions si l'exposant est strictement supérieur à 2. Il s'agit du grand théorème de Fermat que celui-ci pensait avoir montré. Une démonstration rigoureuse a été donnée par Wiles en 1995 après de nombreuses années de recherche.

11 Factorielle et arithmétique

1 Soit $k \in [\![0, n]\!]$, montrer que $\begin{pmatrix} n \\ k \end{pmatrix}$ est un entier.

2 Soit $k \wedge n = 1$ montrer que n divise $\begin{pmatrix} n \\ k \end{pmatrix}$.

3 Soit p un nombre premier. Montrer que $\forall k \in [\![0, p-1]\!]$, p divise $\begin{pmatrix} p \\ k \end{pmatrix}$.

12 Suite de Fibonacci et arithmétique

On considère la suite de Fibonacci définie par $u_0 = 0$, $u_1 = 1$ et $u_{n+2} = u_{n+1} + u_n$.

1 Montrer que $u_{n+1}u_{n-1} - u_n^2 = (-1)^n$. En déduire que $u_{n+1} \wedge u_n = 1$ si $n \in \mathbb{N}^*$.

2 Montrer que $\forall (m, n) \in \mathbb{N}^* \times \mathbb{N},\ u_{m+n} = u_{m-1}u_n + u_m u_{n+1}$. On pourra commencer par le cas $m = 1$ et le cas $m = 2$ puis raisonner par récurrence.

3 En déduire que $u_n \wedge u_m = u_{n \wedge m}$.