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

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

1 Le théorème de Lagrange

1 $f : H \mapsto aH$ définie par $f(h) = ah$ est trivialement surjective (on rappelle que $aH = \{ah, h \in H\}$). De plus, elle est injective car $f(h_1) = f(h_2) \Leftrightarrow ah_1 = ah_2 \Leftrightarrow h_1 = h_2$.

2 Supposons que $aH \cap bH \neq \emptyset$. Il existe h et h' tels que $ah = bh'$ donc $b^{-1}a \in H$. Soit $ah \in aH$. $ah = bb^{-1}ah = b(b^{-1}a)h \in bH$. Donc $aH \subset bH$. De la même manière, $bH \subset aH$.

3 $G \subset \underset{g\in G}{\cup} gH$ car $g \in gH$. L'autre inclusion est aussi facile car $gH \subset G$ pour tout $g \in G$.

4 On a recouvert G avec $(gH)_{g\in G}$. Mais dans cet ensemble il peut-y avoir de la redondance. En effet, si deux éléments g_1H et g_2H ont une intersection non vide, ils sont égaux. On a donc éventuellement plusieurs copies d'un même ensemble. En ne prenant qu'un représentant, on aboutit à une partition de G. On a donc $G = \underset{g\in\omega}{\cup} gH$ avec les différents éléments de $(gH)_{g\in\omega}$ qui ont une intersection vide. Ainsi on a $|G| = \sum\limits_{g\in\omega} |gH| = |\omega||H|$ et donc $|H|$ divise $|G|$.

5 Simple application de la propriété ci-dessus.

2 Le théorème de Cayley

1 τ_x est une bijection en effet. $\tau_x(x^{-1}g) = xx^{-1}g = g$ donc τ_x est surjective. De plus elle est injective car $\tau_x(g_1) = \tau_x(g_2) \Leftrightarrow xg_1 = xg_2 \Leftrightarrow g_1 = g_2$.

2 La loi à considérer est la composition. L'élément neutre est la fonction identité, l'associativité découle de l'associativité des fonctions, le symétrique d'une fonction est la fonction réciproque. Bien évidemment la loi est interne.

3 $\tau_x \circ \tau_y = \tau_{xy}$ (vérification immédiate). Ainsi on a bien un morphisme de groupe. Pour vérifier l'injectivité on doit montrer que le noyau de ce morphisme est l'élément neutre de G. Soit $\tau_x = \mathrm{id}$. Dans ce cas $\tau_x(e) = xe = x = \mathrm{id}(e) = e$ donc $x = e$ et le seul élément du noyau est e.

4 Donc ϕ est un isomorphisme de G dans $\mathrm{Im}(\phi)$. Mais $\mathrm{Im}(\phi)$ est un sous-groupe de $\mathfrak{S}_G$ d'où la conclusion.

3 Nombres réels et sous groupes

⚠il faut supposer que le groupe n'est pas réduit à $\{0\}$ pour la suite, j'aurais dû le rajouter dans l'énoncé.

1 G_+ non vide, inclus dans $\mathbb{R}$ et minoré (par 0) donc x_0 bien défini.

2 Soit $x \in \mathbb{R}_+$. Soit $\epsilon \in \mathbb{R}_+^*$. Puisque $x_0 = 0$, $\exists g \in G_+$, $g \leq \epsilon$. Mais alors $\lfloor \frac{x}{g} \rfloor \leq \frac{x}{g} < \lfloor \frac{x}{g} \rfloor + 1$. Donc $\lfloor \frac{x}{g} \rfloor g \leq x < \lfloor \frac{x}{g} \rfloor g + g$. Mais les termes $\lfloor \frac{x}{g} \rfloor g$ et $\lfloor \frac{x}{g} \rfloor g + g$ sont des éléments de G et ne peuvent être tous les deux à distance plus grande de ϵ de x car ils sont à distance $g \leq \epsilon$ l'un de l'autre. Donc G_+ dense dans $\mathbb{R}_+$ et donc par symétrie, G dense dans $\mathbb{R}$.

3 Montrons que x_0 est atteint. Dans le cas contraire, tout suite d'éléments de G_+ qui tend vers x_0 ne stationne pas à x_0. Quitte à extraire, on peut considérer que tous les termes de la suite sont différents. On la note g_n. A partir d'un certain rang les éléments sont aussi proches que l'on veut, c'est-à-dire $\forall \epsilon \in \mathbb{R}_+^*,\ \exists N \in \mathbb{N},\ \forall (n,p) \in \mathbb{N}^2, n \geq N \Rightarrow\ |g_n - g_{n+p}| \leq \epsilon$. Donc pour un certain N $|g_N - g_{N+1}| < x_0$. On suppose que $g_N - g_{N+1} \geq 0$ (sinon on prend son opposé). De plus $g_N \neq g_{N+1}$ donc $0 < g_N - g_{N+1} < x_0$ et $g_N - g_{N+1} \in G_+$. C'est absurde car la borne inférieure de G_+ est x_0. Donc x_0 est atteint.

4 Soit $g \in G_+$ et $g \neq x_0$. Alors $g = qx_0 + r$ avec $0 \leq r < x_0$ (division euclidienne). Mais $r \in G$. La seule possibilité est donc $r = 0$ (sinon on a un élément plus petit que le minimum...). Donc $x_0\mathbb{Z} \subset G$. Trivialement on vérifie que $x_0\mathbb{Z} \subset G$ et on a l'égalité des deux ensembles.

5 Les sous-groupes du groupe additif $(\mathbb{R}, +)$ sont donc de la forme $a\mathbb{Z}$ avec $a \in \mathbb{R}_+$ ou bien ils sont denses dans $\mathbb{R}$ (comme $\mathbb{Q}$ ou le corps des nombres constructibles à la règle et au compas).

4 Carrés parfaits

1 On regarde n modulo 8 et on montre que n^2 ne peut jamais être congru à 7 modulo 8.

2 5 divise $(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2 = 5n^2 + 10$. Donc si ce nombre est un carré parfait il est divisible par 25. Donc $n^2 + 2$ est congru à 3 modulo 5. Ceci n'est pas possible en étudiant chaque congruence de n modulo 5.

5 Implication et primalité

1 Si p est congru à 1 ou 2 modulo 3 alors $8p^2 + 1$ est congru à 0 modulo 3 et n'est pas premier. Si p est congru à 0 modulo 3 alors $p = 3$ car p est premier. $8 \times 3^2 + 1 = 73$ est premier, 71 aussi.

6 Puissance et nombres premiers entre eux

1 On procède par récurrence. C'est trivial au rang 1. On a ensuite :

$$\begin{aligned}(1+\sqrt{2})^{n+1} &= (1+\sqrt{2})(1+\sqrt{2})^n \\ &= (1+\sqrt{2})(a_n + b_n\sqrt{2}) \\ &= a_n + 2b_n + (b_n + a_n)\sqrt{2}\end{aligned} \tag{1}$$

Donc $a_{n+1} = a_n + 2b_n$ et $b_{n+1} = b_n + a_n$ et donc ce sont également deux entiers.

2 On va également procéder par récurrence. La proposition est triviale au rang 1. On a ensuite :

$$\begin{aligned}a_{n+1} \vee b_{n+1} &= (a_n + 2b_n) \vee (a_n + b_n) \\ &= b_n \vee a_n + b_n \\ &= a_n \vee b_n \\ &= 1\end{aligned} \tag{2}$$

7 Équations et arithmétiques

⚠On suppose toujours x plus grand que y et on raisonne par symétrie...

1 $105 = 5 \times 3 \times 7$ donc les seules possibilités sont $x = 105, 35, 21, 15, 7, 5, 3$. 105 est trop grand. On vérifie que $(35,21)$ est solution. Ensuite si $x = 21$ alors $y > x$ c'est absurde. Donc $(35,21)$ et $(21,35)$ solutions. On aurait aussi pu utiliser le fait que $x \vee y = (x+y) \vee (w \wedge y)$ (c'est un bon exercice que de démontrer cette propriété).

2 On raisonne de la même manière et on trouve : $(8,9)(9,8)$.

3 On raisonne de la même manière et on trouve :{$(61,4), (244,1), (123,6), (246,3), (63,36)$
$(252,9), (135,54), (270,27), (486,243), (324,81)$}.

8 Équations et arithmétique

9 Nombres de Fermat

1 Supposons que m n'est pas une puissance de 2. $m = 2^l q$ avec q qui ne contient pas de facteurs 2 dans sa décomposition en produit de facteurs premiers. En particulier q est impair. On a alors $N = 1-(-2^{2^l})^q$. Donc $N = \left(1+2^{2^l}\right)\left(\sum_{k=0}^{q-1}(-2^{2^l})^k\right)$. Or $1+2^{2^l} \neq 1$ et $1+2^{2^l} \neq N$ donc on a N non premier.

2 Soit p un facteur premier commun à F_n et F_m avec $m > n$. On a alors $2^{2^n} = -1[p]$ et $2^{2^m} = -1[p]$. Mais en maintenant l'équation de gauche au carré $m-n$ fois on obtient $1 = -1[p]$. La seule possibilité est alors $p = 2$ mais $p \neq 2$ car tous les nombres de Fermat sont impairs.

10 Nombres de Mersenne

1 Même astuce que pour les nombres de Fermat. Si $a \neq 2$ alors $N = (a-1)\left(\sum_{k=0}^{m-1} a^k\right)$. Puisque $1 < a-1 < a^m$ alors on a N non premier. Si maintenant on a $m = pq$ avec $1 < p < m$. $N = (2^p)^q - 1 = (2^p-1)\left(\sum_{k=0}^{q-1}(2^p)^k\right)$. $1 < 2^p - 1 < 2^m$ donc on a N non premier.

2 Soit q un diviseur de $2^{p_m}-1$ et de $2^{p_n}-1$. On suppose $m > n$. $p_m = qp_n + r$ (division euclidienne). On a alors $(2^{p_n})^q \times 2^r = 1[p]$. Donc p divise $2^r - 1$. Inversement grâce à la même égalité si p divise 2^r-1 et 2^{p_n} p divise $2^{p_m}-1$. Donc $2^{p_m}-1 \vee 2^{p_n}-1 = 2^{p_n}-1 \vee 2^r - 1$. Donc on peut appliquer l'algorithme d'Euclide et conclure puisque $p_n \vee p_m = 1$.

11 Triplets pythagoriciens

⚠Il ne faut pas confondre premiers dans leur ensemble et premiers deux à deux. $(6,10,15)$ sont premiers entre eux dans leur ensemble mais pas premiers entre eux deux à deux.

1 $(3,4,5)$ fonctionne.

2 On divise par le pgcd de ces trois nombres et on obtient un nouveau triplet qui vérifie également une équation du type $x^2+y^2=z^2$ et les éléments de ce triplet sont premiers entre eux dans leur ensemble.

3 Soit p premier qui divise x et y alors il divise x^2+y^2 donc p divise z^2 donc z (lemme d'Euclide). C'est absurde donc $x \vee y = 1$. On raisonne exactement de la même manière pour les autres couples.

4 Ces trois nombres ne peuvent être pairs tous à la fois sinon ils ne sont pas premiers entre eux dans leur ensemble. De plus si un seul est impair alors il peut s'écrire comme somme (ou soustraction) de deux entiers pairs au carré donc il est pair et c'est absurde. De plus on ne peut pas avoir tous les nombres impairs car alors puisque x et y sont impairs leur carré également et donc z^2 est pair (et donc z également). Donc exactement deux éléments sont impairs. La seule possibilité est que z soit pair et les deux autres impairs.

5 On a :

$$\begin{aligned} X \vee Z &= \frac{1}{2}(x+z \vee x-z) \\ &= \frac{1}{2}(2z \vee x+z) \\ &= x \vee z \\ &= 1 \end{aligned} \tag{3}$$

De plus $XZ = y'^2$ donc XZ est un carré parfait. Donc tous les exposants dans la décomposition en produit de facteurs premiers de XZ sont pairs. Mais puisque X et Z sont premiers entre eux les décompositions en produit de facteurs premiers de X et Z sont distinctes et donc les exposants dans la décomposition en produit de facteurs premiers de X et Z sont pairs. Donc X et Z sont carrés.

6 Ainsi l'ensemble des triplets pythagoriciens est (à inversion près des coefficients x et y) :

$$S = \{(c(u^2 - v^2), 2cuv, c(u^2 + v^2)),\ u \vee v = 1\} \tag{4}$$

12 Factorielle et arithmétique

1 Par récurrence, via la formule de Pascal.

2 On utilise le fait que $k\binom{n}{k} = n\binom{n-1}{k-1}$. Donc n divise $k\binom{n}{k}$. On conclut via le lemme de Gauss.

3 Simple application du théorème précédent.

13 Suite de Fibonacci et arithmétique

1 On procède par récurrence. C'est trivial au rang 1. On a :

$$\begin{aligned} u_{n+1}u_{n-1} - u_n^2 &= u_n u_{n-1} + u_{n-1}^2 - u_n^2 \\ &= u_n u_{n-1} + u_{n-1}^2 - u_n u_{n-1} - u_n u_{n-2} \\ &= u_{n-1}^2 - u_n u_{n-2} \\ &= -(-1)^{n-1} \\ &= (-1)^n \end{aligned} \tag{5}$$

On a donc le théorème de Bézout qui s'applique et u_n et u_{n+1} sont premiers entre eux.

2 On raisonne par récurrence. C'est vrai si $m = 1$ ou $m = 2$ (simple vérification). On a :

$$\begin{aligned} u_{m+1+n} &= u_{m-1}u_{n+1} + u_m u_{n+2} \\ &= u_{m-1}u_{n+1} + u_m u_{n+1} + u_m u_n \\ &= -u_m u_{n+1} + u_{m+1}u_{n+1} + u_m u_{n+1} + u_m u_n \\ &= u_m u_{n+1} + u_{m+1}u_{n+1} \end{aligned} \tag{6}$$

3 Comme dans l'exercice sur les nombres de Mersenne on va montrer qu'on peut construire un algorithme d'Euclide. $m = qn + r$ avec r le reste. $u_m = u_{n-1}u_r + bu_n$. Donc si p divise u_m et u_n il divise $u_{n-1}u_r$ mais la question 1 assure alors qu'il divise u_r. Si on a un diviseur de u_n et u_r c'est automatiquement un diviseur de u_m. Donc $u_m \vee u_n = u_n \vee u_r$. On peut donc appliquer l'algorithme d'Euclide et on a $u_m \vee u_n = u_{m \vee n}$.