Feuille $n^0 1$
Jeudi 10 janvier 2019
un peu d'arithmétique

Exercice 1 Relation de Bézout

a) Montrer que 105 et 88 sont premiers entre eux. Trouver une relation de Bézout ! *en utilisant l'algorithme d'Euclide.*

b) Résoudre $49x + 5y = 2$, $x, y \in \mathbb{Z}$.

Exercice 2 Le théorème des restes chinois

a) Montrer que l'application :

$$\mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$k \bmod mn \mapsto (k \bmod m,\ k \bmod n)$$

est un isomorphisme si m, n sont premiers entre eux. En déduire que si m, n sont premiers entre eux, $(\mathbb{Z}/mn\mathbb{Z})^\times \simeq (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$.

b) Déterminer explicitement l'isomorphisme réciproque de $\mathbb{Z}/245\mathbb{Z} \to \mathbb{Z}/49\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Exercice 3 À propos de la fonction indicatrice d'Euler

a) (Théorème d'Euler) : Montrer que $a^{\phi(n)} = 1 \bmod n$ si a, n sont des entiers premiers entre eux.

b) (Petit théorème de Fermat) : Montrer que si p est premier et a non divisible par p, alors $a^{p-1} = 1 \bmod p$.

c) (Théorème de Wilson) Montrer que $(a-1)! = -1 \bmod a \Leftrightarrow a$ premier.

d) (Théorème RSA) : soient $p \neq q$ des nombres premiers. Soit $n = pq$. Montrer que $^\forall d, e \in \mathbb{Z}$, $de = 1 \bmod \phi(n) \Rightarrow m^{de} = m \bmod n$ pour tout $m \in \mathbb{Z}$.

Exercice 4 *Soit $p > 3$ un nombre premier. Soient $s_1, ..., s_p$ les entiers tels que*

$$P := (X-1)...(X-p+1) = X^{p-1} - s_1 X^{p-2} + ... - s_{p-2}X + s_{p-1}\ .$$

a) Montrer que $P = X^{p-1} - 1 \bmod p$ et en déduire les relations :

$$s_{p-1} = -1 \bmod p,\ s_i = 0 \bmod p \text{ si } 1 \leq i < p-1$$

b) *Montrer* $s_{p-2} = 0 \bmod p^2$ *(indication : calculer* $P(p)$*) et en déduire :*

$$1^{-1} + 2^{-1} + ... + (p-1)^{-1} = 0 \bmod p^2 \ .$$

Exercice 5 Symbole de Legendre *Soit* p *un nombre premier impair. Si* $x \in \mathbb{Z}$ *st premier à* p*, on pose* $\binom{x}{p} = 1$ *si* x *est un carré* $\bmod p$*,* -1 *sinon.*

a) *en considérant le morphisme de groupes :*

$$\mathbb{F}_p^* \to \mathbb{F}_p^*, \, x \mapsto x^2 \, ,$$

déterminer le nombre de carrés dans $\mathbb{F}_p^*$ *et en déduire que* $\binom{x}{p} = x^{\frac{p-1}{2}} \bmod p$

b) *Montrer que* $\binom{-1}{p} = (-1)^{\frac{p-1}{2}}$.

c) *Montrer que* $\binom{2}{p} = (-1)^{\frac{p^2-1}{8}}$ *Indication : notons* $\mathcal{P}$ *l'ensemble des entiers pairs* $2 \leq n \leq p-1$ *et* $\mathcal{R} = \{(-1)^i i \ : \ 1 \leq i \leq \frac{p-1}{2}\}$*. Vérifier que* $\overline{\mathcal{P}} = \overline{\mathcal{R}}$ *(on prend les classes* $\bmod p$*) et faire le produit ...*

d) *Loi de réciprocité quadratique : si* p, q *premiers impairs distincts , alors*

$$\binom{p}{q}\binom{q}{p} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

par exemple : p *est un carré* $\bmod 5 \Leftrightarrow 5$ *est un carré* $\bmod p$*.*

Exercice 6 Structure de $(\mathbb{Z}/n\mathbb{Z})^\times$

a) *Montrer que* $\mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/(\mathrm{pgcd}(n,m))\mathbb{Z}$

b) *Montrer que* $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$*. Quel est l'ordre des groupes suivants :* $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}, +)$ *(p premier),* $\mathrm{Aut}(\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z}))$ *et* $\mathrm{Aut}(\mathrm{Aut}(\mathrm{Aut}(\mathbb{Z}/9\mathbb{Z})))$ *?*

c) *Soit* p *un nombre premier (*$p \neq 2$*), montrer que pour tout entier* $k \geq 1$*, il existe un entier* $\lambda \geq 1$*, premier avec* p*, et tel que*

$$(1+p)^{p^k} = 1 + \lambda p^{k+1}$$

En déduire que pour tout $n \geq 1$ *on a* $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathbb{Z}/p^{n-1}(p-1)\mathbb{Z}$.

d) *En montrant que pour tout* $k \geq 1$*,* $5^{2^k} = 1 + \lambda 2^{k+2}$ *avec* λ *un entier impair, en déduire pour* $n \geq 2$ *l'isomorphisme*

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-2}\mathbb{Z}$$

e) *Donner la structure de* $(\mathbb{Z}/n\mathbb{Z})^\times$*. Pour quelles valeurs de* n *est-il cyclique ?*

Exercice 7 *Soit p un nombre premier.*

a) *Déterminer l'ordre du groupe $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$.*

b) *Montrer que $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, $(a_{i,j}) \mapsto (a_{i,j} \bmod p)$ est un morphisme surjectif. En déduire l'ordre du groupe $\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})$.*

c) *Montrer que pour tout entier $n > 0$, le groupe $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ est d'ordre*

$$n^4 \prod_{p|n} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^2}\right)$$

Exercice 8 Le groupe $\mathbb{Z}^{\mathbb{N}}$ n'est pas un groupe abélien libre

a) *Soit M un $\mathbb{Z}-$module libre. Soit $N \leq M$. Alors N aussi est un $\mathbb{Z}-$module libre. Indication : soit $(e_i)_{i\in I}$ une base de M. Soit $(J, \mathscr{B})$ un élément maximal de l'ensemble des couples tels que $J \subseteq I$ et $\mathscr{B}$ est une base de $N_J := M \cap \langle e_j \ : \ j \in J\rangle$ (ça existe par le lemme de Zorn ...) ; montrer que $J = I$.*

b) *Supposons par l'absurde que $A := \mathbb{Z}^{\mathbb{N}}$ a une base $(e_i)_{i\in I}$. Justifier que I n'est pas dénombrable.*

c) *On note $B = \{(x_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \ : \ \lim_n v_2(x_n) = +\infty\}$ où $v_2(x)$ est le plus grand exposant k tel que $2^k|x$. Vérifier que $A \to B$, $(x_n) \mapsto (2^n x_n)_n$ est injective et en déduire que B est libre avec une base non dénombrable.*

d) *Montrer que $B/2B$ est engendré par une famille dénombrable ... et conclure !*

Exercice 9 À propos du dual de $\mathbb{Z}^{\mathbb{N}}$

a) *Montrer que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{(\mathbb{N})}, \mathbb{Z}) \simeq \mathbb{Z}^{\mathbb{N}}$, $\phi \mapsto \phi(n)_{n\in\mathbb{N}}$.*

b) *Montrer que $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}^{(\mathbb{N})}, \mathbb{Z})$ est injective. Indication : soit ϕ dans le noyau. Montrer que $\phi((2^n a_n)_n) = 0$ pour toute suite (a_n). Puis montrer que si (x_n) est une suite quelconque, alors $x_n = 2^n a_n + 3^n b_n$ pour tout n et pour certains entiers a_n b_n ...*

c) *Montrer que si a est un entier, si $k \geq 0$, alors il existe un unique $(a_n)_{0\leq n\leq k} \in \{0,1\}^{k+1}$ tel que $a = a_0 + ... + a_k 2^k \bmod 2^{k+1}$. On appelle $(a_n)_{n\in\mathbb{N}}$ la décomposition de a en base binaire. Par exemple donner la décomposition de -1.*

d) *Montrer que la décomposition en base binaire d'un entier se termine par que des 1 ou par que des 0.*

e) *Soit $\phi \in \mathrm{Hom}(\mathbb{Z}^{\mathbb{N}}, \mathbb{Z})$. On note ϵ_n la suite qui vaut 1 en position n et 0 ailleurs. On pose $\lambda_n = \phi(\epsilon_n)$. On choisit une suite $a = (\pm 2^{s_n})_n$ où la suite s_n est strictement croissante (d'entiers) $\pm 2^{s_n}\lambda_n \geq 0$ et $2^{s_n} > 2^{1+s_{n-1}}|\lambda_n|$ pour tout n.*

Montrer que $f(a) = 2^{s_0}|\lambda_0| + ... + 2^{s_n}|\lambda_n| \bmod 2^{s_{n+1}}$ *pour tout* n*. En déduire une contradiction à propos de la décomposition binaire de l'entier* $f(a)$*.*

f) *Pour un groupe abélien* G*, on pose* $G^\vee := \mathrm{Hom}(G, \mathbb{Z})$*. Montrer que* $(\mathbb{Z}^{\mathbb{N}})^\vee \simeq \mathbb{Z}^{(\mathbb{N})}$ *et* $(\mathbb{Z}^{(\mathbb{N})})^\vee \simeq \mathbb{Z}^{\mathbb{N}}$*. En particulier :*

$$(\mathbb{Z}^{\mathbb{N}})^{\vee\vee} \simeq \mathbb{Z}^{\mathbb{N}} \text{ et } (\mathbb{Z}^{(\mathbb{N})})^{\vee\vee} \simeq \mathbb{Z}^{(\mathbb{N})}$$

les duaux ne sont pas isomorphes mais l'isomorphisme avec le bidual est respecté.