Concours Agrégation, Mathématiques générales

Leçon 20- Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

Commentaires du jury 2015 :

Cette leçon, souvent choisie par les candidats, demande toutefois une préparation minutieuse. Tout d'abord n n'est pas forcément un nombre premier. Il serait bon de connaître les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ et les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Il est nécessaire de bien maîtriser le lemme chinois et sa réciproque. Et pour les candidats plus étoffés, connaître une généralisation du lemme chinois lorsque deux éléments ne sont pas premiers entre eux, faisant apparaître le pgcd et le ppcm de ces éléments. Il faut bien sûr savoir appliquer le lemme chinois à l'étude du groupe des inversibles, et ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du lemme chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux, de connaître les automorphismes, les nilpotents, les idempotents... Enfin, les candidats sont invités à rendre hommage à Gauss en présentant quelques applications arithmétiques des anneaux $\mathbb{Z}/n\mathbb{Z}$, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon.

Commentaires du jury 2016 :

Dans cette leçon, l'entier n n'est pas forcément un nombre premier. Il serait bon de connaître les idéaux de $\mathbb{Z}/n\mathbb{Z}$ et, plus généralement, les morphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Il est nécessaire de bien maîtriser le lemme chinois et sa réciproque. S'ils le désirent, les candidats peuvent poursuivre en donnant une généralisation du lemme chinois lorsque deux éléments ne sont pas premiers entre eux, ceci en faisant apparaître le pgcd et le ppcm de ces éléments. Il faut bien sûr savoir appliquer le lemme chinois à l'étude du groupe des inversibles, et ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du lemme chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux, de connaître les automorphismes, les nilpotents et les idempotents. Enfin, il est indispensable de présenter quelques applications arithmétiques des propriétés des anneaux $\mathbb{Z}/n\mathbb{Z}$, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon. S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$.

Remarque : Le crypto-système RSA a sa place dans cette leçon puisqu'il est basé sur la relation d'Euler. On pourra consulter `http://fr.wikipedia.org/wiki/Chiffrement_RSA`

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
Errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
Compléments et errata, https://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A.] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. F.] Fresnel J. *Anneaux* (Hermann 2001)

Développements conseillés :

(1) Les inversibles de $\mathbb{Z}/n\mathbb{Z}$, [Fr. F.] p 33
(2) Générateurs de $SL_n(\mathbb{Z}/N\mathbb{Z})$, [Fr. A.] ex 2.3. 19 et 20 p. 136-137
(3) Polynôme dans $\mathbb{Z}[X]$ sans racine dans $\mathbb{Q}$ ayant une racine modulo $m\mathbb{Z}$ pour tout $m > 1$ cf. [F. M. 1] $n°101$ p. 276

Exercice 0 Exercice de pratique des congruences. Les généralisations figurent dans les exercices qui suivent.

(1) *Les idempotents de* $\mathbb{Z}/100\mathbb{Z}$

(a) Déterminer les idempotents de l'anneau $\mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$.
Preuve. Il faut rappeler que si p est premier et $a > 0$ et si $p^a|uv$ avec $PGCD(u,v) = 1$ alors $p^a|u$ ou $p^a|v$: on a $v_p(p^a) = a \leq v_p(u) + v_p(v)$ et $v_p(u)$ et $v_p(v)$ ne sont pas simultanément non nuls. Le couple $E := (e_1 \mod 2^2, e_2 \mod 5^2)$ avec $e_i \in \mathbb{Z}$ est un idempotent ssi $E^2 = E$ et donc ssi $e_1^2 = e_1 \mod 2^2$ et $e_2^2 = e_2 \mod 5^2$ i.e. $e_1(1-e_1) = 0 \mod 2^2$ et $e_2(1-e_2) = 0 \mod 5^2$. Puisque e_i et $1-e_i$ sont premiers entre eux il suit que $E \in \{(0,0),(1,0),(0,1),(1,1)\}$. ///

(b) Résoudre le système de congruences $x \in \mathbb{Z}$, $x = x_1 \mod 2^2$ et $x = x_2 \mod 5^2$.
Preuve. On a la relation de Bezout $-6.2^2 + 5^2 = 1$; ainsi si $e_1 := 5^2$ et $e_2 := -6.2^2$, on a $e_1e_2 = 0 \mod 100$ et $e_1 + e_2 = 1 \mod 100$. Ainsi $x_0 := x_1e_1 + x_2e_2$ est solution du système et l'ensemble des solutions est $x = x_0 + 100\mathbb{Z}$. ///

(c) Déterminer les idempotents de $\mathbb{Z}/100\mathbb{Z}$.
Preuve. Puisque l'homomorphisme d'anneaux $x \in \mathbb{Z} \to (x \mod 2^2, x \mod 5^2)$ induit un isomorphisme de $\mathbb{Z}/100\mathbb{Z} \to \mathbb{Z}/2^2\mathbb{Z} \times \mathbb{Z}/5^2\mathbb{Z}$, il suit que les idempotents de $\mathbb{Z}/100\mathbb{Z}$ sont $\{0 \mod 100, e_1 \mod 100, e_2 \mod 100, 1 \mod 100\}$. ///

(2) le groupe $(\mathbb{Z}/5^3\mathbb{Z})^\times$

(a) Montrer que $6 = 1+5$ est d'ordre 5^2 dans le groupe $(\mathbb{Z}/5^3\mathbb{Z})^\times$ (on calculera $(1+5)^{5^2} \mod 5^3$ avec le binôme de Newton).
Preuve. On a $(1+5)^{5^2} = 1 + 5^2.5 \mod 5^3$; ainsi l'ordre de $6 \mod 5^3$ divise 5^2 et puisque $(1+5)^5 = 1 + 5.5 + \frac{5.(5-1)}{2}5^2 \mod 5^3 \neq 1 \mod 5^3$ il suit que 6 est d'ordre 5^2. ///

(b) Montrer que pour tout $n \geq 1$, 4 divise l'ordre du groupe $(\mathbb{Z}/5^n\mathbb{Z})^\times$ et en déduire que l'équation $a_n \in \mathbb{Z} \cap [-\frac{5^n-1}{2}, \frac{5^n-1}{2}]$, $a_n^2 = -1 \mod 5^n$ a deux solutions et qu'elles sont opposées.
Preuve. On peut utiliser le fait que le groupe $(\mathbb{Z}/5^n\mathbb{Z})^\times$ est cyclique d'ordre $\varphi(5^n) = 4(5^{n-1}-1)$ ainsi il contient $\varphi(4) = 2$ éléments $x_n, -x_n$ d'ordre 4 ou plus simplement que $\mathbb{F}_5^\times$ est cyclique et donc si $x \in z$ est d'ordre 4 modulo 5 alors son ordre modulo 5^n est multiple de 4 par le théorème de Lagrange). Ainsi l'équation $x \in \mathbb{Z}$, $x^2 = -1 \mod 5^n$ a deux solutions dans $\mathbb{Z}/5^n\mathbb{Z}$ et donc deux solutions dans le système de représentants $[-\frac{5^n-1}{2}, \frac{5^n-1}{2}]$ et puisque ce système est centré en 0 les solutions sont opposées . ///

(c) Résoudre l'équation $a_1 \in \mathbb{Z}$, $0 \leq a_1 \leq 2$, $a_1^2 = -1 \mod 5$.
Preuve. On calcule les carrés a_1^2 pour $0 \leq a_1 \leq 2$. Les solutions sont $a_1 \in \{\pm 2\}$. ///

(d) En déduire une solution de $a_2 \in \mathbb{Z}$, $0 \leq a_2 \leq 12$, $a_2^2 = -1 \mod 5^2$ (on pourra écrire $a_2 = 5q_1 + r_1$ avec $-2 \leq r_1 \leq 2$).
Preuve. Puisque l'intervalle entier $[-2,2]$ est un système de représentants modulo 5, il suit que si a_2 est comme dans l'énoncé on peut l'écrire $a_2 = 5q_1 + r_1$ avec $-2 \leq r_1 \leq 2$. Alors $r_1^2 = -1 \mod 5$ et pour $r_1 = 2$ on a $a_2^2 = 25q_1^2 + 20q_1 + 4 = -1 \mod 5^2$ qui équivaut à $4q_1 = -1 \mod 5$ et puisque $0 \leq a_2 \leq 12$ il suit que $q_1 = 1$ et donc $a_2 = 7$ est solution. ///

(e) En déduire une solution de $a_3 \in \mathbb{Z}$, $0 \leq a_3 \leq \frac{5^3-1}{2}$, $a_3^2 = -1 \mod 5^3$.
Preuve. Puisque l'intervalle entier $[-12,12]$ est un système de représentants modulo 5^2, il suit que si a_3 est comme dans l'énoncé on peut l'écrire $a_3 = 5^2q_2 + r_2$ avec $-12 \leq r_2 \leq 12$. Alors $r_2^2 = -1 \mod 5^2$ et pour $r_2 = 7$ on a $a_3^2 = 5^4q_2^2 + 2.5^2.7q_2 + 7^2 = -1 \mod 5^3$ qui équivaut à $q_2 = 2 \mod 5$ ainsi $a_3 = 57$ convient. ///

(f) Construire un entier a avec $0 < a < 5^3$ et d'ordre $\varphi(5^3)$ dans $(\mathbb{Z}/5^3\mathbb{Z})^\times$.
Preuve. On a vu que 6 (resp. 57) était d'ordre 5^2 (resp. 4) modulo 5^3. Soit $a := 6.57$ et $d > 0$, alors $a^d = 1 \mod 5^3$ implique $a^{5^2d} = 1 \mod 5^3$ et donc $57^{5^2d} = 1 \mod 5^3$ et donc $4|d$. De même $a^{4d} = 1 \mod 5^3$ et donc $6^{4d} = 1 \mod 5^3$ et donc $5^2|d$ d'où finalement $\varphi(5^3) = 4.5^2|d$ et l'ordre de a est donc $\varphi(5^3)$. ///

Exercice 1 Sous-groupes de $\mathbb{Z}/n\mathbb{Z}$: Si G est un tel sous-groupe alors le théorème de Lagrange montre que $d := |G|$ divise n ainsi $a + n\mathbb{Z} \in G$ implique $da = 0 \mod n$ et donc $a \in \frac{n}{d}\mathbb{Z}$ et donc $G \subset \frac{n}{d}\mathbb{Z}/n\mathbb{Z} = \{\frac{n}{d} + n\mathbb{Z}, ..., d\frac{n}{d} + n\mathbb{Z}\}$ et donc $G = \frac{n}{d}\mathbb{Z}/n\mathbb{Z}$. Il suit que les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont en bijection avec les diviseurs de n dans $\mathbb{N}$.

Rappelons que si $H \subset G$ sont 2 groupes avec H distingué dans G alors la surjection canonique $\pi : G \to \frac{G}{H}$, induit une bijection entre l'ensemble des sous groupes de G qui contiennent H et l'ensemble des sous-groupes de $\frac{G}{H}$. Dans le cas où $G = \mathbb{Z}$ on connait les sous-groupes d'où une preuve "classique".

Exercice 2 Déterminer les entiers n tels que $\frac{\mathbb{Z}}{n\mathbb{Z}}$ a 24 idéaux (les idéaux de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ coïncident avec les sous-groupes du groupe additif $\frac{\mathbb{Z}}{n\mathbb{Z}}$).

Exercice 3 Soit $n, m \in \mathbb{N}^\star$. On se propose de déterminer les homomorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Pour $k \in \mathbb{N}^\star$, on note π_k la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/k\mathbb{Z}$.

(1) Soit f un homomorphisme de groupe de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$. Soit $a \in \mathbb{Z}$ avec $f \circ \pi_n(1) = \pi_m(a)$. Montrer que $\frac{m}{(m,n)}$ divise a.

Preuve. Par construction si $x \in \mathbb{Z}$ alors $f_a \circ \pi_n(x) = xf_a \circ \pi_n(1) = x\pi_m(a)$ et pour $x = n$ puisque $\pi_n(x) = 0 \mod n$ on obtient $0 \mod m$. Ainsi $na = dm$ avec $d \in \mathbb{Z}$ ce qui équivaut à $\frac{n}{(m,n)}a = \frac{m}{(m,n)}d$ et qui par le lemme de Gauss implique que $\frac{m}{(m,n)}$ divise a. ///

(2) Réciproquement soit $a \in \frac{m}{(m,n)}$, montrer qu'il existe un unique homomorphisme de groupes $f_a : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ avec $f_a \circ \pi_n(1) = \pi_m(a)$.

Preuve. Soit $a = d\frac{m}{(m,n)}\mathbb{Z}$ avec $d \in \mathbb{Z}$ et $h_a : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ l'homomorphisme $h_a(x) = ax \mod m$ alors $h_a = f_a \circ \pi_n$. Puisque $h_a(n) = d\frac{nm}{(m,n)} \mod m = 0 \mod m$, on a $\operatorname{Ker}\pi_n \subset \operatorname{Ker} h_a$ et on conclut avec le théorème de factorisation des homomorphismes de groupes. ///

(3) A quelle condition sur m, n y a-t-il un seul homomorphisme de groupe de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$?

Preuve. Puisque l'on dispose toujours de l'homomorphisme $h_0(x) = 0 \mod m$ la condition est que $\frac{m}{(m,n)} \in m\mathbb{Z}$ i.e. $(m, n) = 1$. ///

(4) Calculer en fonction de m, n le nombre d'homomorphismes de groupes de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/m\mathbb{Z}$.

Preuve. On cherche donc le nombre de restes modulo m des entiers $a = d\frac{m}{(m,n)}$ avec $d \in \mathbb{Z}$. Si r est le reste de d modulo (m, n) alors le reste de $d\frac{m}{(m,n)}$ modulo m est $r\frac{m}{(m,n)}$, ainsi le nombre de classes modulo m des entiers multiples de $\frac{m}{(m,n)}$ est (m, n). ///

Exercice 4 Soit $m > 1$ et $\rho : \mathbb{Z} \to \frac{\mathbb{Z}}{m\mathbb{Z}}$ la surjection canonique. Les automorphismes du groupe additif $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les $\sigma_{\rho(a)}$ pour $a \in \mathbb{Z}$ et $(a, m) = 1$ et définis par $\sigma_{\rho(a)}(z) = \rho(az)$. Ainsi le groupe des automorphismes du groupe additif $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est isomorphe au groupe multiplicatif $(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$ des inversibles de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$. Le seul automorphisme de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est l'identité.

Preuve. Les homomorphismes du groupe $\frac{\mathbb{Z}}{m\mathbb{Z}}$ dans lui-même sont caractérisés par l'image de 1, ce sont donc les $\sigma_{\rho(a)}$ avec $a \in \mathbb{Z}$ et $\sigma_{\rho(a)}(\rho(z)) = \rho(az)$. Les automorphismes du groupe $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les homomorphismes surjectifs et donc les $\sigma_{\rho(a)}$ avec $\rho(a)$ un générateur du groupe $\frac{\mathbb{Z}}{m\mathbb{Z}}$. Mais $\rho(a)$ un générateur si et seulement si il existe $b \in \mathbb{Z}$ avec $b\rho(a) = \rho(1)$ i.e. $ba - 1 \in m\mathbb{Z}$ autrement dit $(a, m) = 1$. Par définition de la multiplication dans l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$ on a $\rho(b)\rho(a) = \rho(1)$ i.e. $\rho(a)$ est inversible de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$. Puisque $\sigma_{\rho(a)} \circ \sigma_{\rho(a')} = \sigma_{\rho(aa')}$ l'application $\rho(a) \in (\frac{\mathbb{Z}}{m\mathbb{Z}})^\times \to \sigma_{\rho(a)}$ est donc un isomorphisme du groupe des inversibles de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$ dans le groupe des automorphismes du groupe additif $\frac{\mathbb{Z}}{m\mathbb{Z}}$. Enfin si un tel automorphisme est un automorphisme d'anneau il doit en particulier vérifier $\sigma_{\rho(a)}(\rho(1)) = \rho(1)$ i.e. $a = 1 \mod m\mathbb{Z}$. ///

Exercice 5 Le théorème des restes chinois et sa réciproque. Voir [F. M. 1] 93 p. 257 pour une généralisation à des anneaux quotients

Soient $r > 1$, $m_1, m_2, ..., m_r \in \mathbb{Z}$ et $m = m_1 m_2 ... m_r$. Alors les propriétés suivantes sont équivalentes.

(1) Le groupe additif $\frac{\mathbb{Z}}{m\mathbb{Z}}$ est isomorphe au produit des groupes additifs $\frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$.

(2) On a $1 = (m_i, m_j)$ pour $i \neq j$.

Preuve. On peut en fait remplacer "groupe" par "anneau" dans l'énoncer. Voyons ii) implique i). C'est le théorème des restes chinois. Il est important dans les applications de connaître un isomorphisme et la bijection réciproque de façon explicite .

L'homomorphisme d'anneaux naturel à considérer est $\rho : \mathbb{Z} \to \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ *défini par* $\rho(x) = (x \mod m_1, x \mod m_2, ..., x \mod m_r)$. *Alors* $\operatorname{Ker}\rho = m_1 m_2 ... m_r\mathbb{Z}$; *ainsi* ρ *induit un homomorphisme d'anneaux injectif* $\overline{\rho} : \frac{\mathbb{Z}}{m\mathbb{Z}} \to \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ *qui est surjectif pour des raisons de cardinal. L'explicitation de l'application réciproque est liée à la recherche des idempotents de l'anneau* $\frac{\mathbb{Z}}{m\mathbb{Z}}$. *En effet notons* $e_i := (0, 0, ..., 1, ..., 0)$ *où le* 1 *est à la* i*-ième position. Alors* $\overline{\rho}^{-1}(\sum_{1\leq i\leq r} x_i e_i) = \sum_{1\leq i\leq r} x_i \overline{\rho}^{-1}(e_i)$ *pour* $x_i \in \mathbb{Z}$. *Ainsi il suffit de déterminer* $\overline{\rho}^{-1}(e_i)$. *Pour cela on remarque que si* $p \in \mathbb{Z}$ *est premier et divise les* $q_i := \prod_{1\leq j\leq r,\ j\neq i} m_j = 1$ *pour* $1 \leq i \leq r$ *alors il existe* i_0 *avec* $p | m_{i_0}$ *mais alors* $p | (p_{i_0}, m_{i_0}) = 1$; *ainsi l'idéal* $\sum_{1\leq i\leq r} \mathbb{Z} q_i = \mathbb{Z}$ *et il existe donc* $u_i \in \mathbb{Z}$ *avec* $\sum_{1\leq i\leq r} u_i q_i = 1$. *On a donc* $\rho(u_i q_i) = e_i$ *et plus généralement* $\rho(\sum_{1\leq i\leq r} x_i u_i q_i) = \sum_{1\leq i\leq r} x_i e_i = (x_1 \mod m_1, x_2 \mod m_2, ..., x_r \mod m_r)$.

Montrons que non ii) implique non i). On suppose par exemple qu'un premier p *divise* m_1 *et* m_2. *Alors pour tout élément* $(a_1, a_2, ..., a_r) \in \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$, *on a* $\frac{m}{p}(a_1, a_2, ..., a_r) = (0, 0, ..., 0)$, *donc tout élément du groupe additif* $\frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ *est divisible par* $\frac{m}{p}$. *Par ailleurs si* $\pi : \mathbb{Z} \to \frac{\mathbb{Z}}{m\mathbb{Z}}$ *est la surjection canonique alors* $\pi(1)$ *est d'ordre* m. *Ce qui contredit l'isomorphisme. ///*

Exercice 6 Les idempotents de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$, voir [F. M. 1] 93 p. 257 pour une généralisation à des anneaux quotients.

Rappelons que si A est un anneau unitaire, un idempotent est un élément $e \in A$ avec $e(e-1) = 0$. Ainsi l'anneau A est isomorphe à la somme directe des anneaux unitaires Ae et $A(e-1)$.

Soit $m = \prod_{1\leq i\leq r} p_i^{\alpha_i}$ avec $p_i \in \mathbb{N}$ premiers et $\alpha_i \geq 1$ et $\overline{\rho} : \frac{\mathbb{Z}}{m\mathbb{Z}} \to \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ où $m_i = p_i^{\alpha_i}$. Alors les idempotents de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$ sont les $\overline{\rho}^{-1}(\epsilon_1, \epsilon_2, ..., \epsilon_r)$ avec $\epsilon_i \in \{0, 1\} \in \frac{\mathbb{Z}}{m_i\mathbb{Z}}$; ils sont donc en bijection avec les parties de l'ensemble $\{1, 2, ..., r\}$.

Preuve. Soit $e = (\epsilon_1, \epsilon_2, ..., \epsilon_r) \in \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ *est un idempotent si et seulement si* ϵ_i *est un idempotent de l'anneau* $\frac{\mathbb{Z}}{m_i\mathbb{Z}}$ *pour* $1 \leq i \leq r$. *Dans cet exercice* m_i *est puissance d'un nombre premier et si* $\rho_i : \mathbb{Z} \to \frac{\mathbb{Z}}{m_i\mathbb{Z}}$ *est la surjection canonique et si* $\rho(x_i) = \epsilon_i$ *alors* $x_i(x_i - 1) = 0 \mod p_i^{\alpha_i}$ *et donc* $x_i(x_i - 1) = 0 \mod p_i$. *Si donc* $p_i | x_i$, *il suit de l'égalité* $1 = x_i + (1 - x_i)$ *que* $(p_i, x_i - 1) = 1$ *et donc que* $p_i^{\alpha_i} | x_i$; *ainsi* $\epsilon_i = 0$. *Si* $p_i | (1 - x_i)$, *il suit de même que* $\epsilon_i = 1$. *L'application qui à la partie* I *de* $\{1, 2, ..., r\}$ *associe* $e_I := \sum_{i\in I} e_i$ *et* $e_i := (0, 0, ..., 1, ..., 0)$ *où le* 1 *est à la* i*-ième position (avec* $e_\emptyset = 0$*) est une bijection avec les idempotents de l'anneau* $\frac{\mathbb{Z}}{m\mathbb{Z}}$. *Notez que dans la preuve du théorème des restes chinois à l'exercice précédent on a vu que* $\rho(u_i q_i) = e_i$. ///

Exercice 7 Les nilpotents de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$.

Rappelons que si A est un anneau un élément $a \in A$ est nilpotent si il existe $r > 0$ avec $a^r = 0$. Si A est commutatif l'ensemble des nilpotents est un idéal.

Soit $m = \prod_{1\leq i\leq r} p_i^{\alpha_i}$ avec $p_i \in \mathbb{N}$ premiers et $\alpha_i \geq 1$ et $\overline{\rho} : \frac{\mathbb{Z}}{m\mathbb{Z}} \to \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \frac{\mathbb{Z}}{m_2\mathbb{Z}} \times ... \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}$ où $m_i = p_i^{\alpha_i}$. Alors $(\prod_{1\leq i\leq r} p_i)\frac{\mathbb{Z}}{m\mathbb{Z}}$, est l'ensemble des nilpotents de l'anneau $\frac{\mathbb{Z}}{m\mathbb{Z}}$. C'est le sous-groupe d'indice $\prod_{1\leq i\leq r} p_i$ du groupe additif $\frac{\mathbb{Z}}{m\mathbb{Z}}$.

Exercice 8 Le théorème des restes chinois généralisé, [F. M. 2] p. 189.

Exercice 9

(1) L'équation diophantienne $(x,y,z)\in\mathbb{Z}^3,\ x^2+y^2=7z^2$ implique $x=y=z=0$.

Preuve : On suppose que $xyz\neq 0$. On note δ le PGCD de x,y,z et on pose $(x',y',z'):=(\frac{x}{\delta},\frac{y}{\delta},\frac{y}{\delta})$ il suit que $x'^2+y'^2=0$ *mod* 7. Puisque $(-1)^{\frac{7-1}{2}}=-1$ il suit que -1 n'est pas un carré modulo 7 et ainsi 7 divise x' et y' et donc 7^2 divise $7z^2$ d'où 7 divise z' ce qui est une contradiction. Si $z=0$ il suit de la positivité de x^2+y^2 que $x=y=0$. Et si $z\neq 0$ et $xy=0$ on peut supposer par symétrie que $y=0$ et ainsi $x^2=7z^2$, ainsi $2v_7(x)=1+2v_7(z)$, ce qui est une contradiction. ///

(2) L'équation diophantienne $(x,y,z)\in\mathbb{Z}^3,\ x^2+y^2=pz^2$ avec p premier.

Preuve. 1ère méthode. Si $p=3 \mod 4$ *comme dans le cas de* $p=7$ *on trouve seulement la solution triviale* $(0,0,0)$. *Par contre si* $p=1 \mod 4$ *il y a une infinité de solutions. Traitons le cas* $p=5$, *le cas général se traite de façon similaire. Soit donc* $(x,y,z)\in\mathbb{Z}^3,\ x^2+y^2=5z^2$. *On remarque que* $(1,2,1)$ *est une solution non triviale. On peut écrire* $|x+iy|^2=|1+2i|^2z^2$ *ainsi* $|(x+2y)+i(y-2x)|^2=(5z)^2$ *ce qui en posant* $5X=x+2y$ *et* $5Y=-2x+y$ *et* $Z=z$, *donne* $X^2+Y^2=Z^2$. *De plus* $x^2+y^2=(x+2y)(x-2y)$ *mod* 5, *ainsi quitte à changer* y *en* $-y$ *on peut supposer que* $5|(x+2y)$ *et donc* $5|(-2x+y)=-2(x+2y)$ *mod* 5 *et alors* $(X,Y,Z)\in\mathbb{Z}^3$ *et donc à permutation près de* X,Y, $X=\epsilon_1 d(u^2-v^2)$, $Y=\epsilon_2 2duv$ *et* $Z=\epsilon_3 d(u^2+v^2)$ *avec* $u,v\in\mathbb{Z}$, $(u,v)=1$ *et* $\epsilon_i\in\{1,-1\}$. *Puisque* $x=X-2Y$ *et* $y=2X+Y$, *on en déduit que* $x=\epsilon_1 d(u^2-v^2)-2\epsilon_2(2duv)$, $y=2\epsilon_1 d(u^2-v^2)+\epsilon_2 2duv$, $z=\epsilon_3 d(u^2+v^2)$ *ou* (y,x,z). *Réciproquement on vérifie que ces formules donnent des solutions.*

2ième méthode. Une autre solution est de remarquer que X^2+Y^2-5 *définit une conique sur* $\mathbb{Q}$ *et que* $(1,2)$ *est une solution. Si* $(X,Y)\in\mathbb{Q}^2$ *est solution soit* $X=1$, *auquel cas* $Y=2$ *ou* $Y=-2$ *soit* $X-1\neq 0$ *auquel cas on pose* $T:=\frac{Y-2}{X-1}$ *et alors* $Y=2+T(X-1)$ *d'où* $X^2+Y^2-5=(X-1)[(T^2+1)X-(1+4T-T^2)]$ *et donc* $X=\frac{T^2-4T+1}{T^2+1}$ *et* $Y=\frac{-2T^2-2T+2}{T^2+1}$. *Ainsi les solutions de* $X^2+Y^2=5$ *avec* $(X,Y)\in\mathbb{Q}$ *sont* $(1,2)$, $(1,-2)$ *et* $(X=\frac{T^2-4T+1}{T^2+1},Y=\frac{-2T^2-2T+2}{T^2+1})$ *avec* $T\in\mathbb{Q}$.

Les solutions de $(x,y,z)\in\mathbb{Z}^3,\ x^2+y^2=5z^2$. *sont pour* $z=0$ *le triplet* $(0,0,0)$ *et pour* $z\neq 0$ *vérifient les conditions au-dessus en posant* $X:=\frac{x}{z}$ *et* $Y=\frac{y}{z}$. *Posant* $T=\frac{u}{v}$ *avec* $u,v\in\mathbb{Z}$, $(u,v)=1$ *et* $v\neq 0$ *on retrouve les solutions entières précédentes... ///*

Exercice 10 L'équation $x^2=1$ dans $\frac{\mathbb{Z}}{m\mathbb{Z}}$.

(1) Soit $p>2$, premier et $n\geq 1$. Montrer que l'équation $x^2=1$ a 2 solutions dans $\frac{\mathbb{Z}}{p^n\mathbb{Z}}$.

Preuve.

1-ère méthode. *Soit* $x\in\mathbb{Z}$ *avec* $x^2=1 \mod p^n\mathbb{Z}$; *en particulier* $(x-1)(x+1)=0 \mod p\mathbb{Z}$ *et donc* $x=1+pa$ *ou* $x=-1+pa$ *avec* $a\in\mathbb{Z}$.*Si* $n=1$, *on a donc les 2 solutions* $-1,1$. *Supposons donc que* $n>1$ *et que* $x=1+pa$, *alors* $1=x^2=1+2pa+p^2a^2 \mod p^n\mathbb{Z}$, *ainsi* $2a=0 \mod p^{n-1}\mathbb{Z}$ *et* $p>2$ *il suit que* $a=0 \mod p^{n-1}\mathbb{Z}$ *et ainsi* $x=1 \mod p^n\mathbb{Z}$. *De même si* $x=-1+pa$ *on montre que* $x=-1 \mod p^n\mathbb{Z}$. ///

2-ième méthode. *On retrouve dans cette preuve la méthode utilisée pour prouver la cyclicité du groupe multiplicatif* $(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ *(cf. [Fr. F.] p 33). De fait plus généralement si* $d>1$ *alors* $x\in\frac{\mathbb{Z}}{p^n\mathbb{Z}}$ *est tel que* $x^d=1$ *si et seulement si* $x\in(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ *et l'ordre de* x *dans le groupe cyclique* $(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ *divise* d. *Soit* $d':=(d,\varphi(p^n))$ *alors (Bézout),* $x^d=1$ *si et seulement si* $x^{d'}=1$. *Puisque* d' *divise l'ordre de* $(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ *les solutions de* $x^d=1$ *sont les élements du sous-groupe d'indice* d' *de* $(\frac{\mathbb{Z}}{p^n\mathbb{Z}})^\times$ *et il y en a* $d'=(d,\varphi(p^n))$. *En particulier si* $d=2$ *alors* $d'=d=2$, *il y a 2 solutions qui sont celles que l'on connait à savoir* $-1,1$. ///

(2) Toujours $n\geq 1$. Montrer que l'équation $x^2=1,\ x\in\frac{\mathbb{Z}}{2^n\mathbb{Z}}$ a respectivement 1, 2, 4 solutions suivant que $n=1,2$ ou $n\geq 3$.

Preuve.

1-ère méthode. *On traite directement les cas $n = 1, 2$. On suppose alors que $n \geq 3$. Soit donc $x \in \mathbb{Z}$ avec $x^2 = 1 \mod 2^n\mathbb{Z}$. En particulier $(x-1)(x+1) = 0 \mod 2$ et donc $x = 1 + 2a$; ainsi $1 = x^2 = 1 + 4a + 4a^2 \mod 2^n\mathbb{Z}$ et donc $a(1+a) = 0 \mod 2^{n-2}\mathbb{Z}$. Ainsi $a = b2^{n-2}$ ou $a = -1 + b2^{n-2}$ avec $b \in \mathbb{Z}$. Dans le premier cas $x = 1 \mod 2^n\mathbb{Z}$ ou $x = 1 + 2^{n-1} \mod 2^n\mathbb{Z}$ et dans le second cas $x = -1 \mod 2^n\mathbb{Z}$ ou $x = -1 + 2^{n-1} \mod 2^n\mathbb{Z}$. Réciproquement on vérifie que ce sont bien des solutions de l'équation $x \in \mathbb{Z}$ avec $x^2 = 1 \mod 2^n\mathbb{Z}$.*

2-ième méthode. *On rappelle que le groupe multiplicatif de l'anneau $\frac{\mathbb{Z}}{2^n\mathbb{Z}}$ est respectivement isomorphe via Ψ, au groupe additif 0, $\frac{\mathbb{Z}}{2\mathbb{Z}}$, $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2^{n-1}\mathbb{Z}}$ suivant que $n = 1$, $n = 2$ ou $n \geq 3$ où Ψ est donné explicitement (cf. [Fr. F.] p 33). Il suffit alors de résoudre l'équation $2z = 0$ dans chacun de ces groupes en tenant compte de Ψ. Ainsi les solutions sont respectivement 1, ± 1, $\pm 1, \pm(1 + 2^{n-1})$ suivant que $n = 1$, $n = 2$ ou $n \geq 3$. Comme dans la question précédente cette méthode permet de résoudre plus généralement l'équation $x \in \mathbb{Z}$ avec $x^d = 1 \mod 2^n\mathbb{Z}$ où $d \geq 1$. ///*

(3) Soit $m > 1$, résoudre l'équation $x^2 = 1 \mod m\mathbb{Z}$.

Preuve. On utilise la décomposition en nombre premiers de m. Ecrivons $m = p_0^{n_0} p_1^{n_1} p_2^{n_2} ... p_r^{n_r}$ avec $n_0 \geq 0$, $p_0 = 2 < p_1 < p_2 < ... < p_r$ et $n_i > 0$ pour $1 \leq i \leq r$. Ainsi par le théorème des restes chinois l'homomorphisme d'anneau $\rho : \mathbb{Z} \to \prod_{0 \leq i \leq r} \frac{\mathbb{Z}}{p_i^{n_i}\mathbb{Z}}$ avec $\rho(x) = (x \mod p_0\mathbb{Z}, x \mod p_1\mathbb{Z}, ..., x \mod p_r\mathbb{Z})$ induit un isomorphisme des groupes multiplicatifs $(\frac{\mathbb{Z}}{m\mathbb{Z}})^\times$ et $\prod_{0 \leq i \leq r}(\frac{\mathbb{Z}}{p_i^{n_i}\mathbb{Z})^\times}$. Ainsi avec les questions précédentes les solutions sont données par les $x \mod m\mathbb{Z}$, $x \in \mathbb{Z}$ avec $x = \pm 1 \mod p_i^{n_i}$ pour $1 \leq i \leq r$ si $n_0 = 0$; $x = \pm 1 \mod p_i^{n_i}$ pour $1 \leq i \leq r$ et $x = 1 \mod 2\mathbb{Z}$ si $n_0 = 1$; $x = \pm 1 \mod p_i^{n_i}$ pour $1 \leq i \leq r$ et $x = \pm 1 \mod 2^2\mathbb{Z}$ si $n_0 = 2$ et $x = \pm 1 \mod p_i^{n_i}$ pour $1 \leq i \leq r$ et $x = \pm(1 + 2^{n-1}) \mod 2^n\mathbb{Z}$ si $n_0 \geq 3$. Ce qui donne avec le théorème des restes chinois respectivement 2^r, 2^r, 2^{r+1} et 2^{r+2} solutions suivant que $n_0 = 0, 1, 2$ ou $n_0 \geq 3$. ///

Exercice 11 Soit $n > 1$ on veut caractériser les entiers n tels que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique. On considère pour cela la décomposition en irréductibles $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$.

(1) Soit $G = \prod_{1 \leq i \leq s} \mathbb{Z}/m_i\mathbb{Z}$ avec $1 < m_i$ et $m = \prod_{1 \leq i \leq s} m_i$. Montrer que $\{a \in \mathbb{Z} \mid aG = 0\} = PPCM(m_1, ..., m_s)\mathbb{Z}$.
(2) Montrer que $G = \prod_{1 \leq i \leq s} \mathbb{Z}/m_i\mathbb{Z}$ avec $1 < m_i$ est cyclique si et seulement $(m_i, m_j) = 1$ pour $1 \leq i < j \leq s$ (on appelle cet énoncé la "réciproque du théorème des restes chinois",cf. exercice 5).
(3) On suppose que n est impair. Montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n = p^\alpha$ avec $p > 2$ et $\alpha > 0$.
(4) On suppose que n est pair. Montrer que $(\mathbb{Z}/n\mathbb{Z})^\times$ est cyclique si et seulement si $n \in \{2, 2^2, 2p^\alpha\}$ avec $p > 2$ et $\alpha > 0$.

Exercice 12 La fonction totient d'Euler.

A. La minoration $(*)$ $\varphi(n) \geq (n/2)^{1/2}$.

(1) Soit $m \in \mathbb{N}$, impair avec $\varphi(m) \geq m^{\frac{1}{2}}$ et p un nombre premier impair. Montrer que $\varphi(pm) \geq (pm)^{\frac{1}{2}}$.

Preuve. On suppose d'abord que $(p, m) = 1$ alors $\varphi(pm) = (p-1)\varphi(m) \geq (p-1)m^{\frac{1}{2}}$. Il suffit alors de montrer que $(**)$ $p - 1 \geq p^{\frac{1}{2}}$.

Si maintenant $p|m$, alors $m = p^a m'$ avec $(p, m') = 1$; ainsi $\varphi(pm) = \varphi(p^{a+1})\varphi(m') = p\varphi(m) \geq pm^{\frac{1}{2}} \geq (pm)^{\frac{1}{2}}$. ///

(2) En déduire $(*)$ lorsque m est impair.

Preuve. On utilise la décomposition de m en nombre premiers (donc impairs) $m = p_1 p_2 ... p_r$ avec $2 < p_1 \leq p_1 \leq ... \leq p_r$. Le résultat vient par récurrence sur r (notez que si $r = 1$, c'est $(**)$). ///

(3) Montrer $(*)$.

Preuve. On écrit $m = 2^a m'$ avec m' impair. Si $a = 0$ on a démontré $(*)$ précédemment. On suppose $a \geq 1$; alors $\varphi(m) = 2^{a-1}\varphi(m') \geq 2^{a-1}(m')^{\frac{1}{2}}$ puisque m' est impair. Et puisque $2^{a-1} \geq 2^{\frac{a-1}{2}}$ l'inégalité $(*)$ suit. ///

Exercice 13 Une propriété de divisibilité, [F. M. 2] p.56.

Soient a, n des entiers > 1 et $m := a^n - 1$. Montrer que $n|\varphi(m)$.

Preuve. On a donc $a^n = 1 + m$. Soit $\rho : \mathbb{Z} \to \frac{\mathbb{Z}}{\mathfrak{m}\mathbb{Z}}$ la surjection canonique, on a donc $\rho(a)^n = \rho(1)$; il suit donc que $k := o(\rho(a))|n$. Montrons que $k = n$. En effet si $1 \leq k < n$, on a $1 \leq a^k - 1 < a^n - 1$, or $\rho(a)^k = \rho(1)$ veut dire que $a^k - 1 = \lambda m$; $1 \leq \lambda m < m$, ce qui est impossible. On a bien $o(\rho(a)) = n$ et par le théorème de Lagrange, il suit que $n = o(\rho(a))|o((\frac{\mathbb{Z}}{\mathfrak{m}\mathbb{Z}})^\times) = \varphi(m)$. ///

Exercice 14 Montrer que la période du développement décimal de 1/n divise $\varphi(n)$ (indicatrice d'Euler), [F. M. 1] $n°85$ p. 241

Exercice 15 *Valuation p-adique de n! et reste modulo p de $\frac{p^n!}{p^{v_p(p^n!)}}$*

Dans cet exercice p désigne un nombre premier > 2 et $v_p(.)$ désigne la valuation p-adique.

(1) Soit $M \in \mathbb{N}^*$. Si $k \in \mathbb{N}$, on note $E_k(M) := \{x \in \mathbb{N}^*,\ x \leq M \mid v_p(x) = k\}$. Montrer que $|E_k(M)| = \lfloor \frac{M}{p^k} \rfloor - \lfloor \frac{M}{p^{k-1}} \rfloor$.

Preuve. Les $x \in \mathbb{N}^*,\ x \leq M$ qui sont multiples de p^k s'écrivent $p^k y$ avec $\frac{1}{p^k} \leq y \leq \frac{M}{p^k}$, il y a $\lfloor \frac{M}{p^k} \rfloor$ solutions entières y. ///

(2) En déduire que $v_p(M!) = \sum_{k \geq 1} \lfloor \frac{M}{p^k} \rfloor$.

Preuve. Il y a donc $\lfloor \frac{M}{p^k} \rfloor - \lfloor \frac{M}{p^{k-1}} \rfloor$ entiers x avec $x \leq M$ et $v_p(x) = k$ et chacun contribue pour k dans la valuation p-adique de $M!$. Ainsi $v_p(M!) = \sum_{k \geq 1} k(\lfloor \frac{M}{p^k} \rfloor - \lfloor \frac{M}{p^{k-1}} \rfloor)$ qui après simplification donne la formule annoncée. ///

(3) En déduire que $v_p(p^n!) = \frac{p^n - 1}{p-1}$.

Preuve. On applique la formule à $M = p^n!$, ainsi $v_p(p^n!) = \sum_{k \geq 1} p^{n-k} = \frac{p^n - 1}{p-1}$. ///

(4) Résoudre lorsque $k > 0$ l'équation $x \in \mathbb{Z}/p^k Z,\ x^2 = 1$. Voir l'exercice 10 pour une généralisation.

Preuve. On cherche donc les entiers x avec $p^k|(x-1)(x+1)$. Puisque $k > 0$ on a donc $p|(x-1)(x+1)$, ainsi $p|(x-1)$ ou $p|(x+1)$. Dans le cas où $p|(x-1)$ on remarque que $p \nmid (x-1)$ car sinon $p|((x+1) - (x-1))$; ainsi par le lemme de Gauss $p^k|(x-1)$ et on trouve la solution $x = 1 \mod p^k\mathbb{Z}$. Dans le cas $p|(x+1)$ le même raisonnement donne $x = -1 \mod p^k\mathbb{Z}$. ///

(5) En déduire que $\prod_{i \leq p^k,\ (i,p)=1} i = -1 \mod p^k$ pour $k > 0$.

Preuve. On note que $\prod_{i \leq p^k,\ (i,p)=1} i \mod p^k$ est le produit des éléments du groupe $(\mathbb{Z}/p^k Z)^\times$ et c'est après simplifications égal au produit des éléments égaux à leur inverse. ///

(6) Soit $q := \frac{p^n!}{p^{v_p(p^n!)}}$. Montrer que $q = (-1)^n \mod p$ (on pourra considérer le produit $\prod_{x \in E_k(p^n!)} \frac{x}{p^k} \mod p$ pour $0 \leq k \leq n$).

Preuve. Si $0 \leq k \leq n$ les $\lfloor \frac{p^n!}{p^k} \rfloor - \lfloor \frac{p^n!}{p^{k-1}} \rfloor$ entiers x avec $1 \leq x \leq p^n!$ et $v_p(x) = k$ sont les $p^k i$ avec $1 \leq i \leq p^{n-k}$ et $(i,p) = 1$. Par la question précédente pour $0 < n-k$ on a $\prod_{1 \leq i \leq p^{n-k},\ (i,p)=1} i = -1 \mod p^{n-k}$ et donc $\prod_{1 \leq i \leq p^{n-k},\ (i,p)=1} i = -1 \mod p$. Enfin si $k = n$ on a $\prod_{1 \leq i \leq p^{n-k},\ (i,p)=1} i = 1$, ainsi $q = (-1)^n \mod p$. ///

Remarque. *Pour une généralisation on pourra consulter l'exercice 83 p. 239 de [F. M. 1] et plus particulièrement la question 2.*

Exercice 16 Sur la suite de Fibonacci, [Fr. F] Ex. 1.9.30 p. 57.