Université Lille 1 Algèbre
2010/11 M51.MIMP

Fiche n° 5: Congruences, anneaux, idéaux

Exercice 1 (a) Trouver $999{\cdot}1998 \mod 1999$, $136^7 \mod 137$, $1997{\cdot}1998{\cdot}1999{\cdot}2000 \mod 2001$.
(b) Trouver $2792^{217} \mod 5$ et $10^{1000} \mod 13$.

Exercice 2 (a) Examiner les carrés $a^2 \mod n$ pour $n = 3,\ 4,\ 8$.
(b) Examiner $a^3 \mod 9$ et $a^4 \mod 16$.

Exercice 3 Passer $\mod n$ avec un module approprié et montrer que chacune des équations suivantes n'a aucune solution dans $\mathbb{Z}$:
(a) $3x^2 + 2 = y^2$,
(b) $x^2 + y^2 = n$ pour $n = 2003, 2004$,
(c) $x^2 + y^2 + z^2 = 1999$,
(d) $x^3 + y^3 + z^3 = 5$.

Exercice 4 On dit que $a \mod n$ est inversible s'il existe $b \mod n$ tel que $ab \equiv 1 \mod n$.
(a) Trouver tous les éléments inversibles modulo 5, 6, 9, 11.
(b) Trouver $\mathrm{pgcd}(107, 281)$ et sa représentation linéaire en utilisant **l'algorithme d'Euclide**.
(c) Trouver l'inverse de $107 \mod 281$ et l'inverse de $281 \mod 107$.
(d) Montrer que $a \mod n$ est inversible ssi a et n sont premiers entre eux.

Exercice 5 Trouver toutes les solutions dans $\mathbb{Z}$ de
(a) $2x + 3 \equiv 10 \mod 13$,
(b) $\begin{cases} 2x + 3y \equiv 5 \mod 7 \\ 5x + 2y \equiv 2 \mod 7, \end{cases}$
(c) $x^2 + 2x + 14 \equiv 0 \mod 17$.

Exercice 6 (le petit théorème de Fermat)
Soit p un nombre premier et a un nombre premier à p. Montrer que
(a) $am \equiv an \mod p$ ssi $m \equiv n \mod p$,
(b) La suite $a,\ 2a,\ 3a, \dots, (p-1)a \mod p$ est une permutation de la suite $1,\ 2,\ 3, \dots, (p-1) \mod p$,
(c) $a^{p-1} \equiv 1 \mod p$.

Exercice 7 (a) Examiner $7^n + 11^n \mod 19$.
(b) Montrer que 13 divise $2^{70} + 3^{70}$ et 11 divise $2^{129} + 3^{118}$.

Exercice 8 (théorème de Wilson)
Soit $p = 2m + 1$ un nombre premier. Montrer que
(a) $(p-1)! \equiv -1 \mod p$,
(b) $(m!)^2 \equiv (-1)^{m+1} \mod p$.

Exercice 9 Soit $p > 2$ un nombre premier.
(a) Soit a premier à p. Supposons que la congruence $x^2 \equiv a \mod p$ possède une solution dans $\mathbb{Z}$. Montrer que $a^{(p-1)/2} \equiv 1 \mod p$.
(b) Montrer que la congruence $x^2 \equiv -1 \mod p$ a une solution dans $\mathbb{Z}$ si et seulement si $p \equiv 1 \mod 4$.

Exercice 10 Donner la définition d'un corps. Les opérations binaires $+$ et $\cdot$ sont-elles équivalentes dans la définition ?

Exercice 11 Trouver toutes les solutions des équations :
(a) $ax + b = c \quad (a, b, c \in K,\ K$ est un corps),
(b) $2x \equiv 3 \mod 10$ et $2x \equiv 6 \mod 10$ dans l'anneau $\mathbb{Z}/10\mathbb{Z}$.

Exercice 12 Soit A un anneau. Démontrer que
(a) $\forall a \in A \quad 0_A \cdot a = 0_A$,
(b) $(-1_A) \cdot a = -a$,
(c) $|A| \geqslant 2$ si et seulement si $1_A \neq 0_A$ dans A ($|A|$ désigne le cardinal de A).

Exercice 13 Montrer que
(a) Si $x \cdot y$ est inversible dans un anneau A, alors x et y sont inversibles.
(b) Dans un anneau, un élément inversible n'est pas diviseur de zéro et un diviseur de zéro n'est pas inversible.

Exercice 14 Démontrer que tout anneau intègre fini est un corps.

Exercice 15 Lesquels de ces sous-ensembles donnés de $\mathbb{C}$ sont des anneaux ? Lesquels sont des corps ?
(a) $\mathbb{Z}_{10^\infty} = \bigcup_{n \in \mathbb{N}} 10^{-n}\mathbb{Z}$,
(b) $\mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid \exists\, m \in \mathbb{Z}, n \in \mathbb{N}^*,\ x = \frac{m}{n},$ avec $\operatorname{pgcd}(m, n) = 1$ et $p \nmid n\ \}$ (p est un nombre premier fixé),
(c) $\mathbb{Z}[i] = \mathbb{Z} + i\mathbb{Z}, \quad \mathbb{Z}[\sqrt{2}] = \mathbb{Z} + \mathbb{Z}\sqrt{2}$,
(d) $\mathbb{Q}[i] = \mathbb{Q} + i\mathbb{Q}$, $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\sqrt{2}$.

Exercice 16 Les éléments inversibles d'un anneau A forment le groupe multiplicatif $(A^\times, \cdot)$.
(a) Trouver $A^\times$ pour les anneaux (a) et (b) de l'exercice 15.
(b) Trouver le groupe $\mathbb{Z}[i]^\times$ en utilisant la norme complexe.
(c) Montrer que le groupe $\mathbb{Z}[\sqrt{2}]^\times$ est infini.

Exercice 17 Un élément a d'un anneau A s'appelle nilpotent s'il existe $n \in \mathbb{N}^*$ tel que $a^n = 0$.
(a) Trouver tous les éléments inversibles, les diviseurs de zéro, les nilpotents de l'anneau $\mathbb{Z}/360\mathbb{Z}$, et plus généralement de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
(b) Démontrer que, pour tout nilpotent x de A, l'élément $1 + x$ est inversible.

Exercice 18 Soit I un idéal d'un anneau A. On note par $(a) = a \cdot A$ l'idéal principal engendré par a. Montrer que
(a) $I = A$ ssi $1 \in I$ ssi I contient un inversible,
(b) $(a) = A$ ssi a est inversible,
(c) Un anneau A est un corps ssi (0) est le seul idéal propre de A.

Exercice 19 Montrer que les éléments nilpotents d'un anneau forment un idéal.

Exercice 20 (sommes et produits d'idéaux)
(a) Soient I, J deux idéaux d'un anneau A. Montrer que
$$I \cap J, \quad I + J = \{x + y \,|\, x \in I, y \in J\},$$
sont des idéaux de A.

(b) Montrer que $I + J$ est le plus petit idéal de A contenant I et J.

(c) Soit $n, m \in \mathbb{Z}$, $I = (n) = n\mathbb{Z}$, $J = (m) = m\mathbb{Z}$. Trouver $I \cap J$ et $I + J$.

(d) Montrer que

$$I \cdot J = \{x_1y_1 + x_2y_2 + \dots x_ny_n \,|\, n \in \mathbb{N},\ x_k \in I,\ y_k \in J \text{ pour } \ 1 \leqslant k \leqslant n\}$$

est un idéal. Il s'appelle **produit des idéaux** I et J.

(e) On considère les idéaux $I = (x_1, \dots x_n) = Ax_1 + \dots + Ax_n$ et $J = (y_1, \dots y_m) = Ay_1 + \dots + Ay_m$. Décrire les idéaux $I + J$, $I \cdot J$, I^2 en fonction de x_k, y_l.

Exercice 21 (idéaux étrangers)
(a) Montrer que $I \cdot J \subset I \cap J$ et $(I + J) \cdot (I \cap J) \subset I \cdot J$

(b) On dit que deux idéaux I et J de A sont **étrangers** si $I + J = A$.
Montrer que $I \cap J$=$I \cdot J$ si I, J sont étrangers.

Exercice 22 Soit I un idéal d'un anneau A. On définit le radical d'un idéal par

$$\sqrt{I} = \{x \in A \ \mid \ \exists n \in \mathbb{N}^*, x^n \in I\}$$

(a) Montrer que $\sqrt{I}$ est un idéal de A qui contient I.

(b) Montrer que l'ensemble $\mathrm{Nil}(A)$ des éléments nilpotents de A est $\sqrt{(0)}$.

(c) Montrer que $\sqrt{\sqrt{I}} = \sqrt{I}$.

(d) Montrer que $\mathrm{Nil}(A/I) = \sqrt{I}/I$ et que $A/\mathrm{Nil}(A)$ est sans élément nilpotent non trivial.

Fiche n° 5: Congruences, anneaux, idéaux

Indication 3 Passer modulo l'entier donné ci-dessous et utiliser l'exercice 2.

(a) Passer $\mod 3$.

(b) Passer $\mod 4$ pour $n = 2003$ et $\mod 3$ pour $n = 2004$.

(c) Passer $\mod 8$.

(d) Passer $\mod 9$.

Indication 4 (a) $\mathbb{Z}/5\mathbb{Z}^\times = \{\pm 1, \pm 2\} = \mathbb{Z}/5\mathbb{Z}\backslash\{0\}$, $\mathbb{Z}/6\mathbb{Z}^\times = \{\pm 1\}$, $\mathbb{Z}/9\mathbb{Z}^\times = \{\pm 1, \pm 2, \pm 4\}$, $\mathbb{Z}/11\mathbb{Z}^\times = \mathbb{Z}/11\mathbb{Z} \setminus \{0\}$.

(b) $8 \cdot 281 - 21 \cdot 107 = 1$

(c) Modulo 281, l'inverse de 107 est 21 et celui de 281 modulo 107 est 8.

(d) Utiliser le théorème de Bezout.

Indication 5 Standard.

Indication 6 Pour le sens $\Rightarrow$ dans (a), utiliser que a est inversible modulo p. (b) se déduit ensuite de (a) et (c) de (b).

Indication 8 Pour le (a), une méthode est de reconnaître en les facteurs $1, 2, \ldots, p-1$ de $(p-1)! \mod p$ tous les éléments de $(\mathbb{Z}/p\mathbb{Z})^\times$ et de les regrouper en paires de la forme $\{x, x^{-1}\}$. On obtient le (b) en écrivant $(p-1)! \equiv (1 \cdots m)(m+1 \cdots 2m) \equiv m!(-m \cdots -1) \equiv (-1)^m (m!)^2$.

Indication 9 (a) découle de $x^{p-1} = 1 \mod p$ (exercice 6). Le sens $\Rightarrow$ dans (b) s'en déduit. Pour la réciproque, on utilise l'exercice 8.

Indication 10 voir le cours.

Indication 11 (a) est standard.

(b) $2x \equiv 3 \mod 10$ n'a pas de solution dans $\mathbb{Z}/10\mathbb{Z}$, sinon 3 serait pair. L'équation $2x \equiv 6 \mod 10$ équivaut à $x \equiv 3 \mod 5$.

Indication 12 (a) et (b) sont standard. On obtient alors que si $1_A = 0_A$, pour tout $a \in A$, on a $1_A \cdot a = a = 0_A \cdot a = 0_A$, ce qui prouve le sens $\Rightarrow$ dans (c). L'autre sens est évident.

Indication 13 Standard.

Indication 15 (a) $\mathbb{Z}_{10^\infty}$ est un anneau mais pas un corps (les entiers premiers à 10 n'ont pas d'inverse).

(b) $\mathbb{Z}_{(p)}$ est un anneau mais pas un corps (les entiers multiples de p n'ont pas d'inverse).

(c) $\mathbb{Z}[i]$ et $\mathbb{Z}[\sqrt{2}]$ sont des anneaux mais ne sont pas des corps (un élément $a + ib \in \mathbb{Z}[i]^\times$ (resp. $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$) doit vérifier $a^2 + b^2 = \pm 1$ (resp. $a^2 - 2b^2 = \pm 1$).

(d) $\mathbb{Q}[i]$ et $\mathbb{Q}[\sqrt{2}]$ sont des corps.

Indication 16 (a) $\mathbb{Z}_{10^\infty}^\times = \{2^m \cdot 5^n \mid m, n \in \mathbb{Z}\}$ et $\mathbb{Z}_{(p)}^\times = \mathbb{Z}_{(p)} \setminus p\mathbb{Z}_{(p)}$.
(b) Pour $a, b \in \mathbb{Z}$, on a $a + ib \in \mathbb{Z}[i]^\times$ ssi $a^2 + b^2 = \pm 1$, ce qui donne $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.
(c) Pour $a, b \in \mathbb{Z}$, on a $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ si et seulement si $a^2 - 2b^2 = \pm 1$. Cette dernière équation a une infinité de solutions $a + b\sqrt{2}$: en effet, $1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]^\times$ (remarquer que $(\sqrt{2} + 1)(\sqrt{2} - 1) = 1$) et en conséquence, pour tout $n \in \mathbb{N}$, $(1 + \sqrt{2})^n \in \mathbb{Z}[\sqrt{2}]^\times$.

Indication 17 (a) Les inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$ sont les classes d'entiers m premiers à n. L'ensemble des diviseurs de 0 est égal à l'ensemble des classes d'entiers m, avec m non premier à n ; c'est donc aussi l'ensemble des éléments non inversibles. Les éléments nilpotents sont les classes d'entiers m divisibles par tous les facteurs premiers de n, ou de façon équivalente, divisibles par leur produit ; par exemple, les éléments nilpotents de $\mathbb{Z}/360\mathbb{Z}$ sont les classes d'entiers divisibles par 30.
(b) Si $x^n = 0$, alors $1 - x + x^2 \cdots (-1)^{n-1}$ est l'inverse de $1 + x$.

Indication 19 Utiliser la formule du binôme pour la stabilité pour l'addition. Pas d'autre difficulté.

Indication 20 (a) et (b) sont standard. Dans (c), on a $I \cap J = M\mathbb{Z}$ où $M = \mathrm{ppcm}(m, n)$ et $I + J = \delta\mathbb{Z}$ où $\delta = \mathrm{pgcd}(m, n)$. Dans (e), on a : $I + J = Ax_1 + \cdots + Ax_n + Ay_1 \cdots + Ay_m$, $I \cdot J = Ax_1y_1 + \cdots + Ax_1y_m + \cdots + Ax_ny_1 + \cdots Ax_ny_m$ et I^2 s'obtient en faisant $I = J$ dans la description de $I \cdot J$.

Indication 21 (a) ne pose pas de difficultés et (b) correspond au cas particulier de (a) où $I + J = A$.

Indication 22 Exercice formel sans aucune difficulté.

Fiche n° 5: Congruences, anneaux, idéaux

Correction 1 (a) $999 \cdot 1998 \equiv 999 \cdot (-1) \equiv 1000 \mod 1999$.
$136^7 \equiv (-1)^7 \equiv -1 \mod 137$.
$1997 \cdot 1998 \cdot 1999 \cdot 2000 \equiv (-4) \cdot (-3) \cdot (-2) \cdot (-1) \equiv 24 \mod 2001$.
(b) $2792^{217} \equiv 2^{217} \equiv 2^{4.54+1} \equiv (2^4)^{54} \cdot 2^1 \equiv 2 \mod 5$.
$10^{1000} \equiv (-3)^{1000} \equiv 3^{1000} \equiv 3^{3.333+1} \equiv (3^3)^{333} \cdot 3^1 \equiv 3 \mod 13$.

Correction 2 (a) $\{a^2 \mod 3 \mid a \in \mathbb{Z}\} = \{0, 1 \mod 3\}$.
$\{a^2 \mod 4 \mid a \in \mathbb{Z}\} = \{0, 1 \mod 4\}$ et $\{a^2 \mod 8 \mid a \in \mathbb{Z}\} = \{0, 1, 4 \mod 8\}$.
(b) $\{a^3 \mod 9 \mid a \in \mathbb{Z}\} = \{0, 1, -1 \mod 9\}$ et $\{a^4 \mod 16 \mid a \in \mathbb{Z}\} = \{0, 1 \mod 16\}$.

Correction 7 (a) Modulo 19, 7 et $11 = 7^2$ sont d'ordre 3. On obtient que $7^n + 11^n$ est congru à 2 modulo 19 si n est divisible par 3 et congru à -1 modulo 19 sinon.
(b) L'ordre de 2 modulo 13 est 12 celui de 3 est 3. On en déduit que $2^{70} \equiv 2^{-2} \equiv 7^2 \equiv 10 \mod 13$ et $3^{70} \equiv 3^1 \equiv 3 \mod 13$. On obtient $2^{70} + 3^{70} \equiv 0 \mod 13$.
L'ordre de 2 modulo 11 est 10 celui de 3 est 5. On en déduit que $2^{129} \equiv 2^{-1} \equiv 6 \mod 11$ et $3^{118} \equiv 3^3 \equiv 5 \mod 11$. On obtient $2^{129} + 3^{118} \equiv 0 \mod 11$.

Correction 14 Soit A un anneau intègre. Soit $a \in A$, $a \neq 0$. Les applications $\gamma_a : A \to A$ et $\delta_a : A \to A$ envoyant un élément $x \in A$ respectivement sur ax et xa sont injectives. Si A est fini, elles sont alors bijectives. Leur surjectivité fournit l'existence d'un inverse à droite et d'un inverse à gauche pour a, lesquels coincident d'après des résultats standard de la théorie des groupes (voir fiche 1). Cela montre que tout élément $a \in A$, $a \neq 0$ admet un inverse. L'anneau A est donc un corps.

Correction 18 (a) Si $I = A$ alors $1 \in I$ et si $1 \in I$, I contient l'inversible 1. Supposons maintenant que I contienne un inversible $u \in A^\times$. Alors pour tout $a \in A$, $u.(u^{-1}.a) = a \in I$ et donc $A = I$.
(b) D'après (a), $(a) = A$ ssi $1 \in (a)$ ce qui signifie que a est inversible.
(c) Si A est un corps, alors si I est un idéal propre non nul, il contient un élément $u \neq 0$, lequel est inversible, et donc $I = A$ d'après (a). Réciproquement, si (0) est le seul idéal propre d'un anneau A, alors pour tout $a \in A$, $a \neq 0$, on a $Aa = A$, ce qui signifie que a est inversible, et A est donc un corps.