Module Arithmétique sur $\mathbb{Z}$ et corps finis FLMA 401
Exercices de TD

1 Divisibilité, congruences, PGCD, Identité de Bézout

1. Démontrer que la somme de deux nombres impairs consécutifs est divisible par 4. Réciproquement, un multiple de 4 est-il somme de deux entiers impairs ?
2. Résoudre dans $\mathbb{Z}$ les équations
   (a) $x^2 - y^2 = 15$.
   (b) $x^2 - y^2 = 24$.
3. Montrer que les nombres de 3 chiffres dont le deuxième chiffre vaut la somme des deux autres sont des multiples de 11.
4. Montrer que $5^n + 19$ est toujours divisible par 4 si $n \in \mathbb{N}$.
5. (a) Montrer que $x^2 = 2^n - 1$ n'a pas de solution si $n > 1$.
   (b) Existe-t-il des entiers naturels y et n tels que $y^2 = 2^n + 1$? Trouver toutes les solutions.
   (c) Montrer que $z^3 = 2^n - 1$ n'a pas de solution si $n > 1$.
6. (a) Soit n un entier relatif. On note $s(n)$ la somme des chiffres de n (en base 10). Montrer que $n \equiv s(n)$ mod9.
   (b) Soit a la somme des chiffres de 4444^{4444} (écrit en base 10) et b la somme des chiffres de a. Que vaut c, la somme des chiffres de b ?
7. Résoudre $n^3 - m^3 = 999$ dans $\mathbb{N}$.
8. Soit n un entier relatif. Calculer le reste de la division euclidienne de n^2 par 4 suivant que cet entier est pair ou impair. Existe-t-il des entiers a et b tels que $a^2 + b^2 = 8123$?
9. Soient $a, b, c \in \mathbb{N}^*$ tels que $9|a^3 + b^3 + c^3$. En ecrivant la division euclidienne de a, b et c par 3, montrer que 3 divise a, b ou c.
10. Montrer que 15 et 28 sont premiers entre eux.
11. Déterminer les triples $(a, b, c) \in (\mathbb{N}^*)^3$ tels que

$$(i)\ \text{ppcm}(a, b) = 42, \qquad (ii)\ \text{pgcd}(a, c) = 3, \qquad (iii)\ a + b + c = 29.$$

12. Calculer le pgcd de $12n^2 + 16n + 5$ et $6n + 5$.
13. Déterminer les entiers naturels n tel que $n + 1|n^2 + 1$.
14. (a) Résoudre dans $\mathbb{Z}$ l'équation $x^2 - 2y^2 = 0$. Qu'en déduit-on sur $\sqrt{2}$?
   (b) Soit $n \in \mathbb{Z}$. Montrer qu'il existe un unique couple d'entiers (a_n, b_n) tel que $(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}$.
   (c) Montrer que a_n et b_n sont premiers entre eux.
   Indication : montrer que $\text{pgcd}(a_{n+1}, b_{n+1}) = \text{pgcd}(a_n, b_n)$.
15. Démontrer que le pgcd de deux entiers naturels consécutifs non nuls vaut 1.
16. En utilisant l'algorithme d'Euclide, calculer le pgcd de
   (a) 853 et 212

(b) 385 et 330

(c) 1395 et 1054

17. Résoudre dans $\mathbb{Z}$ les équations suivantes

(a) $3x - 4y = 1$

(b) $7x - 9y = 2$

(c) $29x + 24y = 3$

18. Soient a, b et c des entiers relatifs. Montrer que $\text{pgcd}(a, b, c) = \text{pgcd}(\text{pgcd}(a, b), c)$.

19. Calculer $\text{pgcd}(105, 294)$ puis $d = \text{pgcd}(105, 294, 770)$. Trouver des entiers u, v et w tels que $105u + 294v + 770w = d$

20. Soient $x = \frac{a}{b}$ et $y = \frac{c}{d}$ des nombres rationnels donnés sous forme irréductible et tels que $x + y$ soit un entier. Démontrer que x et y ont même dénominateur.

2 Structures algébriques : groupes, anneaux, corps

1. Soit $\mathbb{R}$ l'ensemble des nombres réels.

(a) Montrer que $\mathbb{R}$ muni de l'addition usuelle est un groupe commutatif.

(b) Montrer que $\mathbb{R}$ muni de l'addition et de la multiplication usuelle est un anneau commutatif.

(c) Montrer que $\mathbb{R}$ muni de l'addition et de la multiplication usuelle est un corps.

2. Soit $\mathbb{R}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{R}$.

(a) $\mathbb{R}[X]$ muni de l'addition usuelle est-il un groupe ?

(b) $\mathbb{R}[X]$ muni de la multiplication usuelle est-il un groupe ?

(c) $\mathbb{R}[X]$ muni de l'addition et de la multiplication usuelle est-il un anneau ?

(d) $\mathbb{R}[X]$ muni de l'addition et de la multiplication usuelle est-il un corps ?

3 Nombres premiers, Théorème de Fermat, Théorème des restes chinois, Théorème d'Euler

1. *Triplets pythagoriciens* On appelle triplet pythagoricien un triplet d'entiers x, y et z strictement positifs, premiers entre eux dans leur ensemble et vérifiant

$$x^2 + y^2 = z^2.$$

Les conditions imposées sur x, y et z ne sont bien sûr pas restrictives dans le sens où on peut toujours se ramener à ce cas.

(a) Soient a et b deux entiers premiers entre eux. Montrer que si ab est un carré, alors a et b sont nécessairement des carrés.

(b) Soit $d = \text{pgcd}(x, y)$. Montrer que d divise z (on pourra décomposer d en facteurs premiers). En déduire que x, y et z sont premiers entre eux 2 à 2.

(c) Montrer que x et y sont de parité différente. On supposera dans la suite que x est pair.

(d) Montrer que le pgcd de $z-y$ et de $z+y$ vaut 2. En utilisant que $x^2 = z^2 - y^2 = (z-y)(z+y)$, montrer qu'il existe u et v dans $\mathbb{N}$ avec $u > v$, premiers entre eux tels que

$$\begin{aligned} x &= 2uv \\ y &= u^2 - v^2 \\ z &= u^2 + v^2 \end{aligned}$$

(e) Réciproquement, montrer qu'un tel triplet est pythagoricien quels que soient u et v premiers entre eux.

2. Soit X l'ensemble des nombres premiers de la forme $4k+3$ avec $k \in \mathbb{N}$.
   (a) Montrer que X est non vide.
   (b) Montrer que le produit de nombres de la forme $4k+1$ est encore de cette forme.
   (c) On suppose que X est fini et on écrit $X = \{p_1, \ldots, p_n\}$. Soit $a = 4p_1p_2 \ldots p_n - 1$. Montrer par l'absurde que a admet un diviseur premier de la forme $4k+3$.
   (d) Montrer que ceci est impossible et donc que X est infini.
3. *Une autre preuve du petit théorème de Fermat*
   (a) Soit p un nombre premier et $i \in \mathbb{N}$ compris entre 1 et $p-1$. Montrer que p divise le coefficient binomial
   $$C_p^i = \frac{p!}{i!(p-i)!}.$$
   (b) En déduire une preuve par récurrence du petit théorème de Fermat.
4. Montrer que 13 divise $2^{70} + 3^{70}$.
5. Montrer que 7 divise $2222^{5555} + 5555^{2222}$.
6. Montrer que pour tout entier naturel n, $2^{3n+5} + 3^{n+1}$ est divisible par 5.
7. Montrer que pour tout entier naturel n, $n^5 - n$ est divisible par 30.
8. Trouver le reste de la division euclidienne de $16^{(2^{1000})}$ par 7 ?
9. Trouver le reste de la division euclidienne de 100^{1000} par 13 ?
10. Trouver tous les entiers x vérifiant les conditions suivantes

$$\begin{aligned} x &\equiv 3 \bmod 7 \\ x &\equiv 5 \bmod 11 \end{aligned}$$

11. (a) Trouver un entier a compris entre 1 et 12 congru à 27^{103} modulo 13.
    (b) Trouver un entier b compris entre 1 et 10 congru à 27^{103} modulo 11.
    (c) Quel est le reste de la division euclidienne de 27^{103} par 143 ?
12. Dix-sept pirates s'emparent d'un lot de pièces d'or toutes identiques dans un coffre ne pouvant pas en contenir plus de 1500. Leur loi exige un partage à égalité : chacun doit recevoir le même nombre de pièces d'or et, s'il y a un reste, celui-ci est attribué au cuisinier de bord. Dans le cas présent, la part du cuisinier serait de trois pièces, mais les pirates se querellent et six d'entre eux sont tués, ce qui porte la part du cuisinier à quatre pièces. Au cours d'une terrible tempête, le bateau fait naufrage et ne survivent que six pirates et le cuisinier. Par bonheur, le butin est sauvé. La part du cuisinier est maintenant de cinq pièces. Que peut espérer gagner le cuisinier lorsqu'il décide d'empoisonner le reste de l'équipage ?

13. (a) Décomposer 187 en facteurs premiers.
    (b) Combien y a-t-il d'entiers compris entre 1 et 187 qui sont premiers avec 187 ?
    (c) Quels sont les 3 plus petits entiers strictement positifs qui ne sont pas premiers avec 187 ?
    (d) Calculer 20^{322} modulo 187.
14. Quels sont les deux derniers chiffres de 2006^{2006} ?
15. Soit $n \in \mathbb{N}$ non divisible par 2 et 5. Prouver qu'il existe un multiple de n dont l'écriture décimale ne comporte que le chiffre 1.
    Indication : utiliser le théorème d'Euler avec 10 modulo $9n$.
16. Montrer que les deux groupes $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ et $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$ sont isomorphes.

4 Corps finis

Dans cette section p désignera un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments. On notera $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ son groupe multiplicatif.

1. *Le corps fini* $\mathbb{F}_7$
    (a) Donner pour chaque élément de $\mathbb{F}_7^*$ son ordre dans le groupe multiplicatif.
    (b) Déterminer les générateurs de $\mathbb{F}_7^*$.
    (c) Décrire un isomorphisme de groupes
    $$(\mathbb{Z}/6\mathbb{Z}, +) \longrightarrow (\mathbb{F}_7^*, \cdot).$$
2. *Ordre d'un élément*
    (a) Quels sont les ordres possibles pour un élément de $\mathbb{F}_{67}^*$?
    (b) Calculez l'ordre de (la classe de) 3 dans $\mathbb{F}_{67}^*$.
3. Soient $P(X) = X^3 + X + 1$ et $Q(X) = X^2 + 1$ deux polynômes de $\mathbb{F}_2[X]$. Calculer la somme et le produit de P et Q
4. Soient $P(X) = X^3 + 2X + 3$ et $Q(X) = 4X^2 + 1$ deux polynômes de $\mathbb{F}_5[X]$. Calculer la somme et le produit de P et Q
5. Montrer que $X + 2$ divise $X^3 + X^2 + 1$ dans $\mathbb{F}_3[X]$.
6. Montrer que $X^2 + X + 1$ divise $X^5 + X^4 + 1$ dans $\mathbb{F}_2[X]$
7. Montrer que $X^2 + 5X + 3$ et $X^3 + 5X^2 + 4$ sont congrus modulo $X^2 + 2$ dans $\mathbb{F}_7[X]$.
8. Montrer que $X^3 + X + 1$ et $X^4 + X^3 + 2X^2 + X$ sont congrus modulo $X^2 + X + 2$ dans $\mathbb{F}_3[X]$.
9. Calculer dans $\mathbb{F}_3[X]$ le produit de $X^2 + 2X + 1$ et de $X^2 + 2$ modulo $X^3 + X + 2$.
10. Calculer dans $\mathbb{F}_2[X]/(X^3+1)$ le produit (des classes) de X^2+X+1 et de X^2+1 (on donnera bien sûr le représentant de degré minimal).
11. Réaliser dans $\mathbb{F}_5[X]$ la division euclidienne de $X^5+X^4+X^3+4X^2+3$ par X^3+3X^2+X+2.
12. Réaliser dans $\mathbb{F}_3[X]$ la division euclidienne de $X^3 + 2X + 2$ par $X^2 + X + 2$.
13. Calculer le produit (des classes) de X^3+X+1 et de X^3+X^2+X+1 dans $\mathbb{F}_2[X]/(X^4+X^3+1)$ (on utilisera la division euclidienne).
14. Calculer le produit précédent dans $\mathbb{F}_3[X]/(X^4 + 2X^2 + 1)$.

15. Calculer le pgcd de X^3+X^2+2X+2 et de X^3+X+1 dans $\mathbb{F}_3[X]$.
16. Montrer qu'un polynôme de degré 2 ou 3 de $\mathbb{F}_p[X]$ est irréductible si et seulement si il ne possède pas de racine dans $\mathbb{F}_p$.
17. Montrer que le polynôme X^3+X+1 est irréductible dans $\mathbb{F}_5[X]$ et calculer l'inverse de X^2+3X+2 dans $\mathbb{F}_5[X]/(X^3+X+1)$ en utilisant l'algorithme d'Euclide.
18. Montrer que le polynôme X^4+X^3+1 est irréductible dans $\mathbb{F}_2[X]$ et calculer l'inverse de X^3+X+1 dans $\mathbb{F}_2[X]/(X^4+X^3+1)$ en utilisant l'algorithme d'Euclide.
19. Construire un corps à 9 éléments. Énumérer ses éléments. Donner leur ordre. Trouver un élément primitif et énumérer les inverses de tous les éléments non nuls.

5 Exercices plus difficiles

1. *Nombres de Mersenne*
   (a) Soient a et n des entiers supérieurs à 2 tels que a^n-1 est premier. Montrer que $a=2$. (Indication : on factorisera a^n-1). On pose alors $M_n=2^n-1$. M_n est le n-ième nombre de Mersenne.
   (b) En raisonnant par contraposée, montrer que si M_n est premier alors n est premier.
   (c) On suppose dans la suite que q est premier et M_q est un nombre de Mersenne non premier. Soit p un facteur premier de M_q. Soit
   $$A=\{n\in\mathbb{N}^* \text{ tel que } p|2^n-1\}.$$
   L'ensemble A peut-il être vide ?
   (d) On note ω le plus petit élément de A. Montrer que ω divise tous les éléments de A. En déduire que $\omega=q$.
   Indication : effectuer la division euclidienne de n par ω et montrer que le reste est aussi dans A.
   (e) Montrer que $p-1$ est dans A et en déduire que q divise $p-1$.
   (f) Utiliser ce résultat pour factoriser $M_{11}=2047$ à l'aide d'une calculatrice.
2. *Nombres de Mersenne et nombres parfaits*
   Si $n\in\mathbb{N}^*$, on note $D(n)$ la somme des diviseurs de n. Un nombre n est dit parfait si $D(n)=2n$ (par exemple 6 est parfait car 6+3+2+1=12).
   (a) Soit M_p un nombre de Mersenne premier (p est donc premier). Montrer que $2^{p-1}M_p$ est parfait.
   (b) Soit n un entier parfait pair. Il s'écrit donc $n=2^ab$ avec $a\geq 1$ et b impair.
      i. Montrer qu'il existe $c\in\mathbb{N}^*$ tel que
      $$b=(2^{a+1}-1)c \text{ et } D(b)=2^{a+1}c.$$
      ii. Prouver que $c=1$, et que $2^{a+1}-1$ est premier.
      iii. Montrer qu'il existe un nombre de Mersenne premier M_p tel que $n=2^{p-1}M_p$.
3. *Nombres de Fermat*
   (a) Soit $m\in\mathbb{N}^*$. Montrer que si 2^m+1 est premier, alors m est une puissance de 2.
   Indication : écrire m sous la forme $m=2^q(2r+1)$.
   On pose alors $F_n=2^{2^n}+1$. F_n est le n-ième nombre de Fermat.

(b) Montrer que F_0, F_1, F_2 et F_3 sont premiers. Vérifier que F_5 est divisible par 641.

(c) Soient m et n deux entiers tels que $n > m$ et $q = n - m$. Exprimer F_n en fonction de F_m et de q.

(d) Soit r un diviseur de F_m. Montrer qu'il existe $k \in \mathbb{Z}$ tel que $F_n = kr + 2$.

(e) Prouver que F_n et F_m sont premiers entre eux.

(f) En déduire qu'il y a une infinité de nombres premiers.