Feuille de TD n° 3

Arithmétique dans $\mathbb{Z}$

Divisibilité et congruences

Exercice 1. Montrer que pour tout $n \in \mathbb{N}$,

1. $8|n^2 - 1$,
2. $7|2^{3n} - 1$,
3. $5|2^{2n+1} + 3^{2n+1}$,
4. $17|2^{6n+3} + 3^{4n+2}$,
5. $676|27^{n+1} - 26n - 27$,
6. pour tout $a, b \in \mathbb{Z}$ et $n \in \mathbb{N}^*$, $a - b|a^n - b^n$.

Exercice 2. ***Numérotation en base*** $b \geq 2$

1. Démontrer que tout entier $a \in \mathbb{N}^*$ s'écrit sous la forme
$$a = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0,$$
où $n \in \mathbb{N}$ et $0 \leq a_i \leq b - 1$, $a_n \neq 0$.
2. Démontrer que la décomposition précédente est unique. On l'appelle **l'écriture de l'entier** a **dans la base** b.
3. Applications.
   (a) Écrire 17 en base $10, 9, 8, 7, 6, 5, 4, 3, 2$ respectivement.
   (b) Écrire 5435 en base hexadécimale.
   (c) Trouver la base b dans laquelle on a $14 \times 41 = 1224$.
   (d) Trouver en base 10 les entiers qui s'écrivent simultanément sous les formes suivantes : $\overline{xyz}$ en base 7 et $\overline{zyx}$ en base 11.
   (e) $b = 10$. Trouver les entiers $0 \leq p, q \leq 9$ tels que $\overline{356q2p}$ est divisible par 35.
   (f) $b = 10$. Trouver les entiers $0 \leq p, q \leq 9$ tels que $\overline{ppqq}$ est un carré.
4. En notant que $7 \times 11 \times 13 = 1001$, déterminer un critère de divisibilité d'un entier $n = \overline{a_n \cdots a_2 a_1 a_0}$ par $7, 11$ ou 13 faisant intervenir la somme $\overline{a_2 a_1 a_0} - \overline{a_5 a_4 a_3} + \cdots$.
5. Écrire un algorithme de numérotation en base b.

PGCD et PPCM

Exercice 3. Calculer le pgcd de $a = 9100$ et $b = 1848$, puis de $a = n^3 + 2n$ et $b = n^4 + 3n^2 + 1$ pour tout $n \in \mathbb{N}^*$. Dans les deux cas, trouver ensuite un couple de Bezout pour ces entiers.

Exercice 4. Montrer que si $a \wedge b = 1$, alors pour tout $p, q \in \mathbb{N}^*$, $a^p \wedge b^q = 1$.

En déduire que $\forall n \in \mathbb{N}^*$, $a^n \wedge b^n = (a \wedge b)^n$.

Exercice 5. Soient $a, b \in \mathbb{Z}$. Montrer que $(a|b) \Leftrightarrow (a^2|b^2)$.

Exercice 6. 17 pirates s'emparent d'un navire. S'ils se partagent le butin, il reste 3 pièces d'or pour le cuisinier chinois. Les pirates se querellent et 6 d'entre eux sont tués. S'ils se partagent le butin, il reste 4 pièces d'or pour le cuisinier chinois. Le navire fait naufrage, et seuls 6 pirates survivent. Le partage laisserait alors 5 pièces d'or au cuisinier. Combien celui-ci aura-t-il au minimum lorsqu'il empoisonnera les pirates survivants ?

Exercice 7. Résoudre dans $\mathbb{Z}^2$ les équations suivantes :

$$56x + 72y = 41 \ , \ 56x + 72y = 40.$$

Exercice 8. On cherche les couples $(x, y) \in \mathbb{N}^2$ tels que $x + y = 56$ et $x \vee y = 105$.

1. Soit (x, y) une solution, et $\delta = x \wedge y$. Montrer que $\delta = 1$ ou $\delta = 7$.
2. Déterminer les couples (x, y) dans chacun des cas proposés.

Exercice 9. Chercher les couples d'entiers (a, b) tels que $a \wedge b = 42$ et $a \vee b = 1680$.

Exercice 10. Déterminer tous les couples d'entiers naturels (m, d) tels que

$$8m = 105d + 30.$$

En déduire tous les couples (a, b) dont m est le PPCM et d est le PGCD.

Exercice 11. On considère $a, b, c, d \in \mathbb{Z}$ et on cherche $u, v, w \in \mathbb{Z}$ vérifiant la relation $ua + bv + cw = d$.

1. À quelle condition nécessaire et suffisante cette équation a-t-elle des solutions ?
2. Montrer que l'équation est équivalente aux deux suivantes, avec $y \in \mathbb{Z}$:

$$ua + bv = y(a \wedge b) \text{ et } y(a \wedge b) + wc = d.$$

3. En déduire tous les triplets d'entiers (u, v, w) tels que $4u + 6v + 8w = 10$.

Exercice 12. Résoudre dans $\mathbb{Z}^2$ les équations $xy = 2x + 3y$, puis $x^2 - y^2 - x + 3y = 30$.

Exercice 13. On considère trois entiers naturels n, p, q avec $n \geq 2$ et $q > 0$.

1. On écrit la division euclidienne de p par q sous la forme $p = aq + r$. Montrer que la division euclidienne de $n^p - 1$ par $n^q - 1$ est

$$n^p - 1 = (n^{(a-1)q+r} + \cdots + n^{2q+r} + n^{q+r} + n^r)(n^q - 1) + (n^r - 1).$$

2. En déduire $(n^p - 1) \wedge (n^q - 1)$ en fonction de n et $p \wedge q$.

Exercice 14. On considère trois entiers naturels a, b, c. Etablir la relation

$$(a \vee b \vee c) \times (bc \wedge ca \wedge ab) = |a| \times |b| \times |c|.$$

Exercice 15. ***Théorème des restes chinois***

Soient p, q premiers entre eux et a, b des entiers tels que $0 \leq a < p$, $0 \leq b < q$. Déterminer les solutions du système

$$\begin{cases} n \equiv a & [p], \\ n \equiv b & [q] \end{cases}$$

Anneau $(\mathbb{Z}/n\mathbb{Z}, +, \times)$

Exercice 16. Écrire les tables de l'addition et de la multiplication dans l'anneau $\mathbb{Z}/n\mathbb{Z}$ pour $n = 2, 3, 4, 5$. Lesquels de ces anneaux sont intègres ? Montrer ensuite que l'équation $x^2 - 10y^2 = 2$ n'a pas de solution dans $\mathbb{Z}^2$ [raisonner dans $\mathbb{Z}/5\mathbb{Z}$].

Exercice 17. Montrer que les éléments inversibles dans $\mathbb{Z}/n\mathbb{Z}$ sont les classes des éléments qui sont premiers avec n, i.e.

$$(\mathbb{Z}/n\mathbb{Z})^* = \{\overline{x} | x \wedge n = 1\}.$$

Exercice 18. Démontrer les équivalences entre les trois conditions suivantes :

1. n est premier,
2. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un anneau intègre,
3. $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps.

Exercice 19. Résoudre la congruence $a^2 + a \equiv 2[p]$ pour $p \in \mathbb{P}$.

Exercice 20. ***Théorème des restes chinois***

Montrer que si $m \wedge n = 1$, on a

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

Nombres premiers

Exercice 21. Démontrer, pour tout $a, b \in \mathbb{Z}^*$, $a|b \Leftrightarrow a^2|b^2$.

Exercice 22. Soit $p \in \mathbb{P}$ et $a \in \mathbb{Z}$.

1. Établir l'équivalence $p|a \Leftrightarrow p|a^2$.
2. Soient $x, y \in \mathbb{Z}$. Montrer que $x^2 + y^2 \equiv 0[11] \Rightarrow x \equiv 0[11]$ et $y \equiv 0[11]$. En déduire l'ensemble des solutions entières de l'équation $x^2 + y^2 = 11z^2$.

Exercice 23. ***Petit théorème de Fermat***

Soit $p \in \mathbb{P}$.

1. Montrer que pour tout $k = 1, \cdots, p-1$, $p|C_p^k$.
2. Démontrer que pour tout $n \in \mathbb{Z}$, $n^p \equiv n[p]$.
3. En déduire le petit théorème de Fermat : pour tout $n \in \mathbb{Z}$, si p ne divise pas n, alors $n^{p-1} \equiv 1[p]$.
4. Quelques applications.
   (a) Pour tout $a \in \mathbb{Z}$, $a^7 \equiv a[42]$.
   (b) Pour tout $n \in \mathbb{Z}$, $\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$

Exercice 24.

1. Soit $x \in \mathbb{Q}^*$. Démontrer que, parmi les représentants $\frac{p}{q}$ de x, il en existe un, et un seul, vérifiant $p \wedge q = 1$ et $q \in \mathbb{N}^*$. On l'appelle le *représentant irréductible* de x.

2. Démontrer que $\sqrt{2}$ est irrationnel.
3. Généralisation : soit $n \in \mathbb{N}^*$ qui n'est pas un carré. Montrer que $\sqrt{n} \notin \mathbb{Q}$.
4. Montrer que $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$.

Exercice 25. ***Cryptographie asymétrique - Système RSA***

La problématique de la cryptographie asymétrique est la construction de deux fonctions

$$\Phi, \sigma : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \ n \in \mathbb{N},$$

appelées respectivement clefs de codage et de décodage. Φ transforme (la classe d'équivalence $\overline{M}$ d') un message fini $M \in [|1, n|]$, en (la classe d'équivalence $\overline{C}$ d') un message codé $C \in [|1, n|]$, et σ est l'inverse à gauche de Φ, i.e.

$$\sigma \circ \Phi = \mathrm{Id}_{\mathbb{Z}/n\mathbb{Z}}.$$

En pratique, l'entier n est très grand, la clef de codage est publique et celle de décodage est privée. Nous nous proposons ici de construire les applications Φ et σ utilisées en cryptographie RSA (cartes banquaires...).

Soient $p, q \in \mathbb{P}$, $p \neq q$. On pose $n = pq$, et $m = (p-1)(q-1)$. Soit ensuite $e \in \mathbb{Z}$ tel que $e \wedge m = 1$. On a $e \in (\mathbb{Z}/m\mathbb{Z})^*$, et on note d un représentant de l'inverse de e dans $\mathbb{Z}/m\mathbb{Z}$.

1. Soient $\Phi : \overline{x} \mapsto \overline{x}^e$ et $\sigma : \overline{x} \mapsto \overline{x}^d$. Montrer que Φ (resp. σ) définit bien une application de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même, entièrement déterminée par le couple (n, e) (resp. (n, d)).
2. Montrer que pour tout $M \in \mathbb{N}$, $M^{ed} \equiv M[p]$ et $M^{ed} \equiv M[q]$. En déduire que pour tout $M \in \mathbb{N}, M^{ed} \equiv M[n]$.
3. En déduire que σ est l'inverse à gauche de Φ, puis commenter la fiabilité de cette procédure.