II. L'anneau $\mathbb{Z}/n\mathbb{Z}$

Question 1. Quel jour était le 14 juillet 1789 ?

Indice 1 : Le 14 juillet 2013 sera un dimanche.

Indice 2 : Combien de jours séparent le 14 juillet 1789 du 14 juillet 2013 ?

Indice 3 : Les années bisextiles sont les annéen divible par 4 mais pas par 100 ou celles divisibles par 400.

Solution : Il y a $2013-1789 = 224$ années entre les deux 14 juillet. Soit $224 \times 365 = 81760$ jours sans prendre en compte les années bisextiles. La première année multiple de 4 est 1792, la dernière 2012. Entre 1792 et 2012 il ya exactement

$$\frac{2012-1792}{4} + 1 = 56$$

années divibles par 4. Les années 1800, 1900 et 2000 sont divibles par 100. L'année 2000 est disible par 400. Il y a donc $56 - 3 + 1 = 54$ années bisextiles entre 1792 et 2013. Il s'en suit qu'il y a exactement $81760 + 54 = 81814$ jours entre le 14 juillet 1789 et le 14 juillet 2013.

Ces 81814 représentent $\lfloor \frac{81814}{7} \rfloor = 11687$ semaines et 5 jours. Le 5 ème jour avant dimanche est un mardi. Le 14 juillet 1789 était donc un mardi.

1 Congruences

Bien des problème de divisibilité se résolvent par la connaissance des restes. Ainsi, par exemple, savoir si a divise b revient à savoir si le reste de la division euclidienne de b apr a est nul. D'où la notion de congruence.

Définition 2.1. On dit que deux entier a et b son congrus modulo n, lorsqu'il donne le même reste par la division euclidienne par n. On note alors $a \equiv b \mod n$.

Ou de manière équivalente, deux entiers a et b sont congrus modulo n lorsque $a - b$ est un multiple de n, c'est-à-dire, lorsqu'il existe $k \in \mathbb{Z}$ tel que $a - b = nk$.

Exercice 2.2. Montrer que ces deux définitions sont équivalentes.

Solution : Supposons que deux entiers a et b aient le même reste pour la division euclidienne par n, que l'on note r . Il existe alors q et q' vérifiant $a = qn + r$ et $b = q'n + r$. On a alors

$$a - b = (qn + r) - (q'n + r) = qn + r - q'n - r = (q - q')n,$$

ce qui implique que $a - b$ est divible par n.

Réciproquement, suposons que $a - b$ soit divisible par n. Il existe alors $k \in \mathbb{Z}$ tel que $a - b = kn$. La division euclidienne de a et b par n donne l'existence d'entiers q, q', r et r' vérifiant $a = qn + r$ et $b = q'n + r'$ ainsi que $0 \leqslant r, r' < n$. On a donc la relation

$$kn = a - b = (qn + r) - (q'n + r') = (q - q')n + r' - r$$

et donc l'égalité $(q-q'-k)n = r-r'$. Des inégalités $0 \leqslant r, r' < n$, on obtient $-n < r-r' < n$. Comme $r - r'$ doit être un multiple de n, la seule possibilité est $r - r' = 0$, à savoir $r = r'$.

Exemple. Quels que soient $a \in \mathbb{Z}$ et $n \in \mathbb{N}$, on a
– $a \equiv a \mod n$
– $a \equiv r \mod n$ si r est le reste de la division euclidienne de a par n.
– $14 \equiv 2 \mod 6$, $-2 \equiv 5 \mod 7$, $9 \equiv -1 \mod 10$.

Exercice 2.3.
3. Comment écrire par une congruence que a est un multiple de n ?
4. Compléter les congruences suivantes :

$$17 \equiv \quad \mod 5,\ -3 \equiv \quad \mod 8,\ 21 \equiv \quad \mod 3$$

5. Les congruences suivantes sont-elles vraies ?

$$27 \equiv 37 \mod 3,\ 145 \equiv 1315 \mod 5,\ -5 \equiv -4 \mod 2$$

Proposition 2.4. *Soeint $a, b, c, d \in \mathbb{Z}$ et $n \in \mathbb{N}$, on a*
– *si $a \equiv b \mod n$ et $b \equiv c \mod n$ alors $a \equiv c \mod n$.*
– *si $a \equiv b \mod n$ et $c \equiv d \mod n$ alors $a + c \equiv b + d \mod n$, $a - c \equiv b - d \mod n$ et $ac \equiv cd \mod n$.*

Exercice 2.5. Montrer que le nombre $a \in \mathbb{N}$ dont l'écriture en base 10 est $a_n...a_1a_0$ est divisible par 9 si et seulement si $a_n + ... + a_1 + a_0$ l'est.

2 Anneau $\mathbb{Z}/n\mathbb{Z}$

Définition 2.6. Soient G un ensemble et $\cdot : G \times G \to G$ une application. On dit que $(G, \cdot)$ est un groupe si
– Associativité : $\forall a, b, c \in G,\ a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
– Neutre : $\exists e \in G\ \forall a \in G\ e \cdot a = a \cdot e = a$;
– Inverse : $\forall a \in G,\ \exists b \in G\ a \cdot b = b \cdot a = e$.
L'application $\cdot$ est la *loi* du groupe. L'élement e est le *neutre* du groupe, b est l'*inverse* de a dans e groupe.

Exemple. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \times)$, $(\mathbb{R} \setminus \{0\}, \times)$, $(\mathbb{C} \setminus \{0\}, \times)$.

Exercice 2.7. Dire pourqoui les couples (ensembl,loi) suivant ne sont pas des groupes : $(\mathbb{N}, +)$, $(\mathbb{Z} - \{0\}, +)$, $(\mathbb{Q}, \times)$.

Définition 2.8. On dit qu'un groupe $(G, \cdot)$ est commutatif si pour tout a et b de G, on a $a \cdot b = b \cdot a$.

Exemple. $(\mathbb{Z}, +)$ est commutatif mais pas $(M_n(\mathbb{R}), +)$ ne l'est pas.

Définition 2.9. Soient A un ensemble et $+ : A \times A \to A$, $\times : A \times A \to A$ deux lois de A. On dit que $(A, +, \times)$ est un anneau si
– $(A, +)$ est un groupe commutatif
– Associativité : $\forall a, b, c \in G,\ a \times (b \times c) = (a \times b) \times c$;
– Neutre : $\exists 1_A \in A\ \forall a \in A, 1_A \times A = A \times 1_A = A$;
– Distributivité : $\forall a, b \in A\ a \times (b + c) = a \times b + a \times c,\ (b + c) \times a = b \times a + c \times a$.

Définition 2.10. On dit qu'un anneau $(A, +, \times)$ est comlutatif si pour tout $a, b \in A$, on a $a \times b = b \times a$.

Exemple. $(\mathbb{Z}, +, \times)$, $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$, $(M_n(\mathbb{R}), +, \times)$ sont des anneaux. A part $(M_n(\mathbb{R}), +, \times)$ pour $n \geqslant 2$ ils sont tous commutatifs.

Définition 2.11. Soit m un entier $\geqslant 2$. Pour $x \in \mathbb{Z}$, on pose

$$[x]_n = \{y \in \mathbb{Z} \mid y \equiv x \mod n\}.$$

On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\{[x]_n \mid x = 0, ..., n-1\}$.

Exemple.

$$[0]_2 = \{..., -6, -4, -2, 0, 2, 4, 6, ...\}$$
$$[1]_2 = \{..., -5, -3, -1, 1, 3, 5, 7, ...\}.$$

Si $a \equiv b \mod n$ alors $[a]_n = [b]_n$.

Définition 2.12. Soient $n \geqslant 2$ et x, y des éléments de $\mathbb{Z}$, on pose
– $[x]_n + [y]_n = [x + y]_n$;
– $[x]_n \times [y]_n = [x \times y]_n$.

Exemple. $[0]_5 + [3]_5 = [3]_5$, $[3]_5 + [3]_5 = [6]_5 = [1]_5$.

Proposition 2.13. *Pour tout $n \geqslant 2$, $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est iun anneau.*

Exercice 2.14. Ecrire les tables d'additions et de multiplications de $\mathbb{Z}/5\mathbb{Z}$ et $\mathbb{Z}/6\mathbb{Z}$.

3 Eléments inversibles de $\mathbb{Z}/n\mathbb{Z}$

Définition 2.15. Soit $(A, +, \times)$ un anneau. On dit qu'un élément x de A est inversible s'il existe y dans A tel qu'on ait $x \times y = y \times x = 1_A$. L'ensemble des éléments inversibles de A est noté A^*.

Exemple. $(\mathbb{Z}, +, \times)^* = \{-1, 1\}$, $(\mathbb{Q}, +, \times)^* = \mathbb{Q} \setminus \{0\}$.

Proposition 2.16. *Soit $(A, +, \times)$ un anneau, alors $(A^*, \times)$ est un groupe.*

Exercice 2.17. A l'aide du théorème I.1.23 montrer que $[x]_n$ (pour $x \in \{0, ..., n-1\}$) est un élément inversibles de $\mathbb{Z}/n\mathbb{Z}$ si et seuelement si $\mathrm{pgcd}(x, n) = 1$.

Solution : Si $\mathrm{pgcd}(x, n)$ vaut 1, alors il existe u et v de $\mathbb{Z}$ tel qu'on ait $ux + vn = 1$, d'où $ux = 1 - vn$, puis $[ux]_n = [1]_n$. Comme par definition, on a $[ux]_n = [u]_n \times [x]_n$, on obtient $[u]_n \times [x]_n = [1]_n$, ce qui implique que $[x]_n$ est inversible.

Réciproquement si $[x]_n$ est inversible, il existe $[y]_n$ tel que $[x]_n \times [y]_n$ soit égal à $[1]_n$. De $[x]_n \times [y]_n = [xy]_n$, on obtient $xy \equiv 1 \mod n$. Il existe alors $k \in \mathbb{Z}$ tel qu'on ait $xy = 1 + kn$ et donc $xy - kn = 1$. Le théorème I.1.23 garantit que cette relation est possible si et seulement si $\mathrm{pgcd}(x, n) = 1$.

Exercice 2.18. Trouver les éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$.

Définition 2.19. On dit qu'un anneau $(A, +, \times)$ est un corps si $A^* = A - \{0_A\}$ où 0_A est l'élément neutre de $+$.

Exemple. $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$ et $(\mathbb{C}, +, \times)$ sont des corps mais pas $(\mathbb{Z}, +, \times)$.

Exercice 2.20. Parmi les anneaux $\mathbb{Z}/n\mathbb{Z}$ de l'exrecice précédent lesquels sont des corps ?

Exercice 2.21. Montrer que $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ est un corps si et seulement si n est premier.

4 Indicatrice d'Euler

Définition 2.22. Pour $n \geqslant 2$, on note $\phi(n)$ le nombre d'élément inversible de $\mathbb{Z}/n\mathbb{Z}$.

Exemple. $\phi(4) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(7) = 6$. De manière générale, si p est un nombre premier alors $\phi(p)$ vaut $p - 1$.

Proposition 2.23. *Soient p et q deux nombres premiers distincts. On a $\phi(pq) = (p-1)(q-1)$.*

Exercice 2.24. Démontre la proposition précédente.

Solution : Soit x un entier de l'intervale $[0, pq-1]$. Le pgcd de x et pq est différent de 1 si et seulement p divise x ou q divise x car p et q sont des nombres premiers. Les multiples de p dans $[0, pq-1]$ sont

$$0, p, 2p, ..., (q-1)p,$$

il y en a exactement q. Les multiples de q dans $[0, pq-1]$ sont

$$0, q, 2q, ..., (p-1)q,$$

il y en a exactement p. Dans $[0, pq-1]$ seul 0 est multiple de p et de q à la fois. Ainsi $[0, pq-1]$ contient $p + q - 1$ entiers mulitple de p ou de q. Comme $[0, pq-1]$ est de cardinal pq, il y a

$$pq - (p + q - 1) = (p-1)(q-1)$$

éléments inversibles dans $\mathbb{Z}/pq\mathbb{Z}$. On a donc montré $\phi(pq) = (p-1)(q-1)$.

Exercice 2.25. Calculer $\phi(35)$.