Arithmétique

1. (66) On note p un entier naturel supérieur ou égal à 2.

   On considère dans $\mathbb{Z}$ la relation d'équivalence $\mathcal{R}$ définie par : $x \mathcal{R} y \overset{\text{déf.}}{\iff} \exists k \in \mathbb{Z}$ tel que $x - y = kp$.

   On note $\mathbb{Z}/p\mathbb{Z}$ l'ensemble des classes d'équivalence pour cette relation $\mathcal{R}$.

   (a) Quelle est la classe d'équivalence de 0 ? Quelle est celle de p ?

   (b) Donner soigneusement la définition de l'addition usuelle et de la multiplication usuelle dans $\mathbb{Z}/p\mathbb{Z}$.
   On justifiera que ces définitions sont cohérentes.

   (c) On admet que, muni de ces opérations, $\mathbb{Z}/p\mathbb{Z}$ est un anneau.
   Démontrer que $\mathbb{Z}/p\mathbb{Z}$ est un corps si et seulement si p est premier.

2. (86) Soit p un nombre premier.

   (a) i. Soit $(a, b) \in \mathbb{Z}^2$. Prouver que si $p \wedge a = 1$ et $p \wedge b = 1$, alors $p \wedge (ab) = 1$.

   ii. Prouver que $\forall k \in [\![1, p-1]\!]$, p divise $\binom{p}{k} k!$ puis que p divise $\binom{p}{k}$.

   (b) i. Prouver que : $\forall n \in \mathbb{N}$, $n^p \equiv n \mod p$.
   Indication : Procéder par récurrence.

   ii. En déduire que : $\forall n \in \mathbb{N}$, p ne divise pas $n \implies n^{p-1} \equiv 1 \mod p$.

3. (94)

   (a) Énoncer le théorème de Bézout dans $\mathbb{Z}$.

   (b) Soit a et b deux entiers naturels premiers entre eux.
   Soit $c \in \mathbb{N}$.
   Prouver que : $(a|c \text{ et } b|c) \iff ab|c$.

   (c) On considère le système $(S) : \begin{cases} x \equiv 6 \mod(17) \\ x \equiv 4 \mod(15) \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.

   i. Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.

   ii. *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

4. Montrer que
   $\forall n \in \mathbb{Z}$, $6 \mid 5n^3 + n$
   $\forall n \in \mathbb{N}$, $13 \mid 2^{4n+2} + 3^{4n+2}$
   $\forall n \in \mathbb{N}$, $n^2 \mid (n+2)^{n+2} - 2^{n+2}(n+1)^{n+1}$.

5. Montrer que
   $\forall (a, b) \in \mathbb{Z}^2$, $7 \mid a^2 + b^2 \implies (7 \mid a \text{ ou } 7 \mid b)$,
   puis que $7 \mid a^2 + b^2 \implies (7 \mid a \text{ et } 7 \mid b)$.

6. (a) Montrer que $\forall n \in \mathbb{Z}$, $\dfrac{15n^2 + 8n + 6}{30n^2 + 21n + 13}$ est irréductible.

   (b) Pour quels entiers naturels n la fraction $\dfrac{n^3 + n}{2n + 1}$ est-elle irréductible ?

7. Résoudre les équations suivantes :
   $\dot{x}^2 - \dot{2}\dot{x} - \dot{2} = \dot{0}$ dans $\mathbb{Z}/5\mathbb{Z}$.
   $\dot{2}\dot{x}^2 - \dot{3}\dot{x} - \dot{2} = \dot{0}$ dans $\mathbb{Z}/7\mathbb{Z}$.
   $\dot{x}^3 - \dot{3}\dot{x}^2 + \dot{2}\dot{x} = \dot{0}$ dans $\mathbb{Z}/24\mathbb{Z}$.

8. Montrer que $\forall n \in \mathbb{N}^*$, $\text{ppcm}(1, 2, ..., 2n) = \text{ppcm}(n+1, n+2, ..., 2n)$ (on commencera par montrer par récurrence que
   $\forall n \in \mathbb{N}^*$, $\text{ppcm}(1, 2, ..., n) | \text{ppcm}(n+1, n+2, ..., 2n)$).

9. Trouver toutes les applications $f : (\mathbb{N}^*)^2 \longrightarrow \mathbb{N}^*$ telles que :

$$\begin{cases} \forall a \in \mathbb{N}^*,\ f(a,a) = a \\ \forall (a,b) \in (\mathbb{N}^*)^2,\ f(a,b) = f(b,a) \\ \forall (a,b) \in (\mathbb{N}^*)^2,\ f(a,b) = f(a,a+b) \end{cases}$$

On fera une récurrence sur n en prouvant que $a+b=n \Longrightarrow f(a,b) = a \wedge b$.

10. Soit $(a,n) \in (\mathbb{N} - \{0,1\})^2$.
    (a) Montrer que si $a^n - 1$ est premier, alors $a = 2$ et n est premier. (Ainsi, en particulier, si $2^n - 1$ est premier, alors n est premier).
    Les nombres $M_n = 2^n - 1$ sont appelés les nombres de Mersenne. la plupart des très grands nombres premiers connus explicitement (avec toutes leurs décimales) sont des nombres de Mersenne ; il existe en effet un test assez "commode" pour savoir si un nombre de Mersenne est premier ou non ; c'est le test de Lucas-Lehmer. Bien entendu, on choisit au départ un nombre M_n, avec n premier .
    (b) Montrer que si $a^n + 1$ est premier, alors a est pair et n est une puissance de 2.
    Les nombres $F_n = 2^{2^n} + 1$ sont appelés les nombres de Fermat ; Fermat avait fait la conjecture que les nombres F_n étaient tous premiers. En réalité, pardonnons-lui, ce résultat est faux, comme le prouve le paragraphe suivant.
    (c) En constatant que $641 = 5.128 + 1$ et que $641 = 2^4 + 5^4$, montrer que $641 \mid F_5$.
    Préciser le nombre de chiffres de l'écriture décimale de F_5.
11. (a) Vérifier que 429 et 700 sont premiers entre eux.
    (b) Déterminer tous les couples $(x,y) \in \mathbb{Z}^2$ tels que $700x + 429y = 1$.
    (c) Quel est l'inverse de $4\dot{2}9$ dans $\mathbb{Z}/700\mathbb{Z}$?
12. Montrer qu'il existe une infinité de nombres premiers de la forme $4n+3$. (*Indication* : p étant un nombre premier de la forme $4n+3$, on considèrera le nombre $q = (2^2.3.5.7.11....p) - 1 = 2 \times (\prod_{\substack{k\ premier \\ k \leq p}} k) - 1$).
    Un théorème extrêmement difficile, dû à Dirichlet, affirme que si a et b sont deux entiers naturels premiers entre eux, alors il y a une infinité de nombres premiers de la forme $an+b$.
13. Démontrer le théorème de Wilson :
    si p est un entier premier, alors $(p-1)! \equiv -1$ (modulo p).
    (*Indication* : dans le produit $\prod_{i=1}^{p-1} i$, on tentera de regrouper chaque entier et le représentant appartenant à $[\![1, p-1]\!]$ de son inverse dans $\mathbb{Z}/p\mathbb{Z}$, à condition que ces deux nombres soient distincts).
    Prouver par contraposée la réciproque du théorème de Wilson.
    On peut finalement énoncer :

$$p \text{ est un entier premier } \iff (p-1)! \equiv -1 \text{ (modulo } p).$$

14. Existe-t-il des années sans vendredi 13 ?
15. Soit $r = \dfrac{p}{q}$ un réel appartenant à [0,1[, avec $p \in \mathbb{N}, q \in \mathbb{N}^*, p \wedge q = 1$ et $10 \wedge q = 1$.
    Montrer que l'écriture décimale illimitée de r est $r = 0, a_1 a_2 ... a_s a_1 a_2 ... a_s ...$, et que la longueur s de la plus petite période de cette écriture est égale à l'ordre de 10 dans $\mathbb{Z}/q\mathbb{Z}$, c'est-à-dire $\inf\{k \in \mathbb{N} \ / \ 10^k \equiv 1 \text{ (modulo } q)\}$.
16. Montrer que $r \in \mathbb{Q}$ si et seulement si le développement décimal de r est périodique à partir d'un certain rang.
17. Déterminer les entiers $n \in \mathbb{Z}$ tels que $n \equiv 3(\mod 7)$ et $n \equiv 8(\mod 17)$
18. Déterminer les entiers $n \in \mathbb{Z}$ tels que $n \equiv 3(\mod 4)$ et $n \equiv 5(\mod 6)$
19. Calculer $\varphi(22896)$ où φ est l'indicatrice d'Euler.