1. Arithmétique élémentaire

Exercice 1.1 Sachant que $85566 = 239 \times 355 + 721$, déterminer le reste de la division euclidienne du nombre 85566 par 355.

Exercice 1.2 ($\star$) Montrer que pour tout entier n, l'entier $n(n+1)(n+2)(n+3)$ est divisible par 24.

Exercice 1.3 ($\star$) Combien 13! admet-il de diviseurs dans $\mathbb{Z}$?
Soient p, q des nombres premiers distincts. Combien p^2q admet-il de diviseurs dans $\mathbb{Z}$?

Exercice 1.4 Soient p, q des nombres premiers distincts. Quels sont les diviseurs positifs de p^2q ?

Exercice 1.5 ($\star$ - Extrait brevet juin 2005) Un pâtissier dispose de 411 franboises et de 685 fraises. Afin de préparer des tartelettes, il désire répartir ces fruits en les utilisant tous et en obtenant le maximum de tartelettes identiques.
- Calculer le nombre de tartelettes.
- Calculer le nombre de framboises et de fraises dans chaque tartelette.

Exercice 1.6 (Extrait du manuel Triangle 3ème Programme 2007) Pour fêter la nouvelle année, des grands parents annoncent à leurs petits enfants qu'ils donnent 525 €à partager entre tous leurs petits fils et 450 €à partager entre toutes leurs petites filles.
Rassurez-vous, chacun des petits enfants reçoit ainsi la même somme : un nombre entier d'euros supérieur à 50.
- Quelle est cette somme ?
- Combien ces grands parents ont-ils de petits fils et de petites filles ?

PPCM. Soient $a, b \in \mathbb{Z}$ tous deux non nuls. On note $\mathrm{ppcm}(a, b)$ le plus petit multiple commun de a et b strictement positif.

Exercice 1.7
1. Montrer que $\mathrm{ppcm}(a, b)\,\mathrm{pgcd}(a, b) = \pm ab$.
2. Décomposer 360 en facteurs premiers.
3. Trouver tous les entiers positifs a, b tels que $a \geq b$, $\mathrm{pgcd}(a, b) = 4$ et $\mathrm{ppcm}(a, b) = 360$.

Exercice 1.8 ($\star$) Déterminer l'ensemble des couples d'entiers naturels de pgcd 18 et de somme 360. De même avec pgcd 15 et produit 600.

Identité de Bézout. Si $d = \mathrm{pgcd}(a, b)$, il existe u et v dans $\mathbb{Z}$ tels que $au + bv = d$.

Exercice 1.9
1. Soient $a, b \in \mathbb{Z} \setminus \{0\}$ et $c \in \mathbb{Z}$. Rappeler une condition nécessaire et suffisante pour que l'équation $ax + by = c$ ait une solution entière $(x, y) \in \mathbb{Z}^2$. Lorsque cette équation a une solution $(x_0, y_0) \in \mathbb{Z}^2$ déterminer l'ensemble de ses solutions dans $\mathbb{Z}^2$ en fonction de x_0, y_0, a, b.
2. Résoudre dans $\mathbb{Z}^2$:

a) $3x + 5y = 4$ b) $261x - 406y = 87$
c) $15x - 9y = 21$ d) $15x + 54y = 38$

Exercice 1.10 ($\star$) Calculer le pgcd de 18480 et 9828. En déduire une écriture de 84 comme combinaison linéaire de 18480 et 9828.

Exercice 1.11
- Donner un exemple de trois nombres entiers p, q, a tels que $p|a$, $q|a$ mais $pq \not| a$. À quelle condition $p|a$ et $q|a$ implique $pq|a$? Prouver alors l'implication.
- Donner un exemple de trois nombres entiers p, a, b tels que $p|ab$ mais $p \not| a$ et $p \not| b$. À quelle condition $p|ab$ implique $p|a$ ou $p|b$? Prouver alors l'implication.

Exercice 1.12 ($\star$) Démontrer que, si a et b sont des entiers premiers entre eux, il en est de même des entiers $a + b$ et ab.

Exercice 1.13 Soient a et b deux nombres entiers positifs et premiers entre-eux. Montrer que si le produit ab est une puissance k-ième ($k \geq 2$) alors les nombres a et b le sont également.

Exercice 1.14 (Triplets pythagoriciens) Déterminer tous les triplets d'entiers (x, y, z) tels que $x^2 + y^2 = z^2$;

Indications :
1. vérifier que l'on peut se ramener à la recherche de solutions où x, y, z sont positifs et premiers entre eux deux à deux ;
2. Étudier ensuite la parité de x, y et z ;
3. en supposant que y est pair, montrer que $z + y$ et $z - y$ sont premiers entre eux et en déduire que ces deux nombres sont des carrés.

Exercice 1.15 Pour $n \geq 0$, on note F_n le n-ème nombre de Fermat $2^{2^n} + 1$.
1. Montrer par récurrence que pour tout $n \in \mathbb{N}$ et tout $k \geq 1$ on a :
$$2^{2^{n+k}} - 1 = \left(2^{2^n} - 1\right) \times \prod_{i=0}^{k-1} F_{n+i}.$$
2. En déduire que les nombres de Fermat sont premiers entre-eux deux à deux.

Exercice 1.16 Vous connaissez sans doute le critère de divisibilité par 9 : on fait la somme des chiffres, puis la somme des chiffres du résultat, et ainsi de suite... Si le résultat final est 9, le nombre de départ était divisible par 9.
1. Montrer que ce critère repose sur le fait que $10 \equiv 1 \pmod 9$.
2. De façon analogue, inventer un critère de divisibilité par 7 (disons pour un nombre à 3 chiffres, ou plus si vous êtes très ambitieux) et par 11 (sans doute plus facile).

Exercice 1.17
1. Trouver le reste de la division euclidienne de 1012×2011 par 2012, de $2011^{1000!}$ par 2012 et de 10^{1000} par 13.
2. Calculer le dernier chiffre dans l'écriture décimale de 7^{25}. Même question avec $7^{100!}$.

Exercice 1.18 (Extrait du contrôle final du 19 janvier 2012) On cherche à résoudre dans $\mathbb{Z}$ l'équation
$$2x^2 + y^2 = 5z^2 \qquad (E).$$
Supposons qu'il existe des entiers a, b, c non tous nuls tel que (a, b, c) soit solution de (E).

1. Montrer qu'il existe des entiers a', b', c' qui ne sont pas tous multiples de 5 tel que (a', b', c') soit solution de (E).
2. Montrer que a' ou b' n'est pas multiple de 5.
3. Soit $x \in \mathbb{Z}$. Montrer que $x^2 \equiv 0, 1$ ou 4 mod 5.
4. En déduire que (E) a pour unique solution $(0, 0, 0)$.

Exercice 1.19

1. Calculer les tables d'addition et de multiplication dans $\mathbb{Z}/n\mathbb{Z}$ pour $n = 5$ et $n = 6$.
2. Dans chaque cas faire la liste des éléments inversibles pour la multiplication.
3. Soit $n \geq 1$ et k un entier. Montrer que la classe $\bar{k}$ dans $\mathbb{Z}/n\mathbb{Z}$ est inversible pour la multiplication si et seulement si k et n sont premiers entre-eux.
4. Déterminer l'inverse multiplicatif de $\overline{6}$ dans $\mathbb{Z}/37\mathbb{Z}$. Même question pour $\overline{11}$ dans $\mathbb{Z}/24\mathbb{Z}$.

Exercice 1.20 1. Examiner les carrés de $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$ et $\mathbb{Z}/8\mathbb{Z}$.

2. Examiner les cubes de $\mathbb{Z}/9\mathbb{Z}$.

Exercice 1.21 Montrer que les équations suivantes n'ont aucune solution dans $\mathbb{Z}$:

1. $3x^2 + 2 = y^2$,
2. $x^3 + y^3 + z^3 = 5$.

Indication : passer modulo un entier approprié.

Exercice 1.22 Déterminer les solutions $n \in \mathbb{Z}$ des systèmes :

$$a) \begin{cases} n \equiv 3 \pmod{17} \\ n \equiv 4 \pmod{11} \\ n \equiv 5 \pmod{6} \end{cases} \quad b) \begin{cases} n \equiv 3 \pmod{6} \\ n \equiv 2 \pmod{5} \\ n \equiv 6 \pmod{7} \end{cases} \quad c) \begin{cases} 2n \equiv 3 \pmod{5} \\ 3n \equiv 2 \pmod{4} \end{cases}$$

Exercice 1.23 Résoudre dans $\mathbb{Z}$:

$$a) \begin{cases} 3x \equiv 3 \pmod{6} \\ 2x \equiv 10 \pmod{3} \\ 2x \equiv 4 \pmod{4} \end{cases} \quad b) \begin{cases} 2x \equiv 2 \pmod{8} \\ x \equiv 2 \pmod{11} \\ 5x \equiv 5 \pmod{6} \end{cases} \quad c) \begin{cases} 3y \equiv 11 \pmod{2} \\ 2y \equiv 10 \pmod{6} \\ y \equiv 12 \pmod{40} \end{cases}$$

Exercice 1.24 Un phare émet un signal jaune toutes les 15 minutes et un signal rouge toutes les 28 minutes. On aperçoit le signal jaune à 0h02 mn et le rouge à 0h08 mn. À quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?

Exercice 1.25 Trouver toutes les solutions dans $\mathbb{Z}$ de :

$$a) 2x + 13 \equiv 10 \pmod{13} \quad b) \begin{cases} 2x + 3y \equiv 5 \pmod{7} \\ 5x + 2y \equiv 2 \pmod{7} \end{cases} \quad c) x^2 + 2x + 14 \equiv 0 \pmod{17}$$

Indicatrice d'Euler. Pour $n \geq 1$, l'indicatrice d'Euler $\varphi(n)$ est définie comme le nombre d'éléments inversibles pour la multiplication dans $\mathbb{Z}/n\mathbb{Z}$.

Exercice 1.26

1. Calculer $\varphi(13)$, $\varphi(12)$, $\varphi(8)$, $\varphi(27)$.
2. Que vaut $\varphi(p^r)$ pour p un nombre premier et r un entier strcitement positif ?
3. Si n et m sont deux entiers strictement positifs premiers entre-eux, comment s'exprime $\varphi(mn)$ en fonction de $\varphi(m)$ et de $\varphi(n)$?
4. Donner une formule générale de $\varphi(n)$ en fonction de n.
5. Montrer par récurrence que pour tout $n \geq 1$,

$$n = \sum_{d|n} \varphi(d).$$

Exercice 1.27 (Preuve élémentaire du petit théorème de Fermat)

1. Montrer que pour tout couple d'entiers a et b et tout p premier, on a :

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

2. En déduire le petit théorème de Fermat :

$$n^p \equiv n \pmod{p}.$$

3. A quelle condition a-t-on $n^{p-1} \equiv 1 \pmod{p}$?

Rappel. Soit $n > 1$. Pour tout entier a premier avec n, $a^{\varphi(n)} \equiv 1 \pmod{n}$

Exercice 1.28 Calculer l'indicatrice d'Euler $\varphi(100)$, montrer que $7^{40} \equiv 1 \pmod{100}$ et en déduire les deux derniers chiffres des nombres $7^{100!}$ et $7^{(9^8)}$.

Calculer les deux derniers chiffres de $7^{(3^{(7^{1000})})}$.

Exercice 1.29 Soient n et m deux entiers strictements positifs premiers entre eux. Montrer que

$$n^{\varphi(m)} + m^{\varphi(n)} \equiv 1 \pmod{nm}.$$