Université de Bordeaux | **MHT633 – Arithmétique et Cryptologie**
Mathématiques | 2014–2015

**FEUILLE D'EXERCICES n° 1**

# Arithmétique

**Exercice 1** – Soit $a$ un nombre rationnel tel que $18a$ et $25a$ sont des nombres entiers. Montrez que $a$ est aussi entier.

**Exercice 2** – Montrez qu'il existe une infinité de nombres premiers de la forme $4n + 3$.

**Exercice 3** – Pour quels entiers $n$ le nombre $n^2 - 1$ est-il premier ?

**Exercice 4** – Trouvez tous les entiers $p$ et $q$ tels que $4p + 7q = pq$.

**Exercice 5** – Soit $a$ et $b$ des entiers distincts.

**1)** Montrez que $a - b$ divise $a^2 - b^2$ et déterminez le quotient.

**2)** Montrez que $a - b$ divise $a^3 - b^3$ et déterminez le quotient.

**3)** Montrez que $a - b$ divise $a^n - b^n$ pour tout $n$

**4)** Montrez que $a + b$ divise $a^{2n+1} + b^{2n+1}$ pour tout $n$.

**5)** Trouvez la factorisation en nombres premiers de $5^{10} - 2^{10}$.

**Exercice 6** – [Nombres de Fermat]

**1)** Vérifiez que les nombres $3 = 2 + 1$, $5 = 2^2 + 1$, $17 = 2^4 + 1$, $257 = 2^8 + 1$, $65537 = 2^{16} + 1$ sont premiers.

**2)** En déduire la factorisation de $2^{32} - 1$.

**3)** Montrez que, si $N = 2^k+1$ est premier, alors $k$ est nécessairement une puissance de 2.

**4)** Fermat conjecturait que les nombres de la forme $2^{2^n} + 1$ sont premiers. Cela est vrai pour $n = 0, 1, 2, 3, 4$ mais n'est pas vrai pour $n = 5$. Montrez, à l'aide des observations suivantes, que 641 divise $2^{2^5} + 1$ :

a) $641 = 2^9 + 2^7 + 1$ donc $2^7 \cdot 5 \equiv -1 \pmod{641}$,

b) $2^4 \equiv -5^4 \pmod{641}$.

**Exercice 7** – Montrez qu'un entier est divisible par 4 si et seulement si le nombre formé par ses deux derniers chiffres dans son écriture décimale est divisible par 4.

**Exercice 8** – Trouvez le pgcd et une relation de Bezout pour les couples $(a, b)$ suivants :

$$(34, 21), \quad (136, 51), \quad (481, 325), \quad (8771, 3206)$$

puis répondez aux questions

**1)** $a$ est-il inversible modulo $b$ ? Si oui quel est son inverse ?

**2)** $b$ est-il inversible modulo $a$ ? Si oui quel est son inverse ?

**Exercice 9** – La date de naissance d'Alice est telle que le jour multiplié par 12 ajouté au mois multiplié par 31 fait 442. Déterminez la.

**Exercice 10** – Calculez les inverses multiplicatifs des nombres suivants ou bien montrez qu'ils ne sont pas inversibles :

**1)** $3 \in \mathbb{Z}/37\mathbb{Z}$

**2)** $4 \in \mathbb{Z}/14\mathbb{Z}$.

**Exercice 11** –

**1)** Quels sont les inversibles de $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ ?

**2)** Si $p$ est premier, quels sont les inversibles de $\mathbb{Z}/p^2\mathbb{Z}$ ?

**Exercice 12** – Résoudre les équations suivantes :

(a) $2x = 37$ dans $\mathbb{Z}/21\mathbb{Z}$, (b) $5x = 15$ dans $\mathbb{Z}/25\mathbb{Z}$, (c) $3x = 7$ dans $\mathbb{Z}/18\mathbb{Z}$.
Explicitez la résolution générale de l'équation $ax = b$ dans $\mathbb{Z}/c\mathbb{Z}$.

**Exercice 13** – Résoudre les systèmes d'équations :

$$(a) \begin{cases} x + y = 6 \\ 2x - y = 8 \end{cases}, \quad x, y \in \mathbb{Z}/11\mathbb{Z} \qquad (b) \begin{cases} 3x + 17y = 9 \\ 9x + 6y = 6 \end{cases}, \quad x, y \in \mathbb{Z}/51\mathbb{Z}.$$

Explicitez les opérations transformant un système linéaire en un système équivalent lorsque les coefficients sont dans un anneau $A$ (commutatif unitaire).

**Exercice 14** – Trouver tous les $x \in \mathbb{Z}$ vérifiant

$$\begin{cases} 2x \equiv 37 \pmod 5, \\ 3x \equiv 48 \pmod 7. \end{cases}$$

**Exercice 15** – Résoudre les équations du second degré :

a) $x^2 + x + 7 = 0$ dans $\mathbb{Z}/13\mathbb{Z}$.
b) $x^2 - 2x + 3 = 0$ dans $\mathbb{Z}/4\mathbb{Z}$.
c) $x^2 - 4x + 3 = 0$ dans $\mathbb{Z}/12\mathbb{Z}$.
Explicitez une méthode de résolution générale.