Feuille de TD 1

1. En utilisant l'égalité $512 \times 233 + 717 = 120013$, calculer de tête le quotient et le reste de la division euclidienne de 120013 par 233. Faire de même si on divise par 512.

2. Une application de la division euclidienne : l'écriture d'un nombre en base b.
Soit $b \geq 2$ un entier naturel fixé. Le but de l'exercice est de montrer que tout entier naturel n admet une écriture de la forme $n = a_0 + a_1 b + a_2 b^2 + \ldots + a_\ell b^\ell$, où $\ell \in \mathbb{N}$ et les entiers a_i vérifient $0 \leq a_i \leq b-1$. On appelle ceci l'écriture de b en base b.

1. Quelle est l'écriture en base 10 de 4321 ? et celle de 100200300 ?
2. Déterminer l'écriture de 23 en base 10, puis en base 3, en base 2, et en base 16.
3. Soit $n \in \mathbb{N}^*$. Montrer que l'ensemble $A = \{k \in \mathbb{N}; b^k \leq n\}$ admet un plus grand élément que l'on notera ℓ (Indication : on pourra utiliser la fonction logarithme).
4. On effectue la division euclidienne de n par b^ℓ. Montrer que le quotient q et le reste r vérifient $0 \leq r < b^\ell$ et $0 \leq q < b$.
5. En utilisant les questions qui précèdent, démontrer que tout entier naturel n possède une écriture en base b.

3. Critères de divisibilité.
Soit n un entier naturel écrit en base 10 sous la forme $\overline{a_\ell \ldots a_1 a_0} = a_0 + a_1 10 + a_2 10^2 + \ldots + a_\ell 10^\ell$. Montrer les équivalences suivantes :

1. $2|n \iff a_0$ est pair.
2. $5|n \iff a_0 \in \{0; 5\}$.
3. $4|n \iff 4|\overline{a_1 a_0}$.
4. $3|n \iff 3|a_0 + a_1 + \ldots + a_\ell$.
5. $9|n \iff 9|a_0 + a_1 + \ldots + a_\ell$.

4. On divise un entier naturel a par 15, et on trouve que le reste est 13. Quel peut être le reste de la division de a par 5 ? Quel peut être le reste de la division de a par 30 ? Que peut-on dire sur le reste de la division de a par 4 ?

5. Ecrire un algorithme, utilisant la division euclidienne, permettant de trouver l'écriture d'un entier naturel n en base 2.

6. Un exercice de codage : le chiffrement affine.
Soit A $= \{0; 1; 2; \ldots; 25\}$. On considère l'application $f : A \to A$, qui à un entier $n \in A$ associe $[3n + 11]_{26}$. Montrer que l'application f est bijective en s'aidant d'un tableau de valeurs.
Pour communiquer secrètement, deux interlocuteurs conviennent d'utiliser la méthode suivante :
a) On code les lettres de l'alphabet de A à Z par les nombres de 0 à 25 ;
b) Ceci permet de traduire le texte à envoyer en une suite de nombres $(a_1; a_2; \ldots; a_N), a_i \in A$;
c) On applique alors à chacun des nombres a_i la fonction f ; on obtient ainsi une nouvelle suite de nombres $(b_1; b_2; \ldots; b_N), b_i \in A$;
d) Enfin, chacun de ces nombres correspond à une lettre.
Coder le mot FUYONS suivant la méthode précédente.
Décoder la réponse YBYKXNJNQXI.
Cette méthode de codage est appelée le chiffrement affine. Elle repose sur le choix d'un couple de nombres (ici (3; 11)) qui doit être connu des deux interlocuteurs. On dit qu'il s'agit d'une méthode à clé secrète.

7. En utilisant la compatibilité des congruences et des opérations, déterminer successivement les restes dans la division euclidienne par 7 des nombres suivants :

$$50 \quad ; \quad 50^{100} \quad ; \quad 100^3 \quad ; \quad 100^{100} \quad ; \quad 50^{100} + 100^{100}.$$

8. Donnez en fonction de la parité de n le reste dans la division de $7^n + 1$ par 8.

9. Preuve par 3 ou par 9.

1. Montrer que pour tout k dans $\mathbb{N}$, $10^k \equiv 1 \bmod 3$ et $10^k \equiv 1 \bmod 9$.
2. Soit $n = \overline{a_\ell \ldots a_1 a_0} = a_0 + a_1 10 + a_2 10^2 + \ldots + a_\ell 10^\ell$ un nombre écrit en base 10. Montrer que n est congru à la somme de ses chiffres modulo 3, et également modulo 9.
3. Montrer (sans calculatrice) que $233 \times 577 \neq 135441$.

10. Calculs modulo 5

1. Montrer que $4^3 \equiv 4 \bmod 5$.
2. En déduire que pour tout $n \in \mathbb{N}, 4^{3n} - 4^n \equiv 0 \bmod 5$.
3. Que peut-on dire pour tout $n \in \mathbb{N}$ et tous k et ℓ impairs de $4^{kn} - 4^{\ell n} \bmod 5$?

11. En utilisant l'algorithme des carrés itérés, calculer $[3^{172}]_{173}$.
Remarque : En utilisant que 173 est un nombre premier, le résultat du calcul est en fait une conséquence immédiate du petit théorème de Fermat, que nous verrons plus tard dans le cours.