Mathématiques pour l'informatique. L1 Informatique I23.

TD 6. Arithmétique [1]

EXERCICE 1. La somme des âges (non-nuls) de trois frères est égale à 39, l'ainé a deux fois l'âge du cadet. Quel est l'âge des trois frères ? Indication : ne pas faire une étude de cas, mais utiliser la division euclidienne en remarquant que l'âge du frère intermédiaire est égal à $q + r$ si q désigne l'âge du cadet.

EXERCICE 2. Un chef de chantier essaie d'organiser la construction d'une villa dans le Var. Il doit faire intervenir deux artisans le même jour. Le premier n'est disponible qu'un jour sur 6, l'autre une fois tous les 11 jours. Le chef de chantier a pu rencontrer le premier artisan le lundi 12 mars et le second le mercredi 14 mars. Quel jour doit-il leur donner rendez-vous pour leur faire effectuer les travaux le plus tôt possible ?

EXERCICE 3. On rappelle l'algorithme du crible d'Eratosthène pour construire une liste de N booléens indiquant quels sont les entiers premiers :

Algorithme CRIBLE(N) : liste de booléens
données
  N :entier
variables
  EstPremier : liste de booléens ;
  p, k :entiers

```
1  EstPremier ← N * [VRAI]
2  EstPremier[1] ← FAUX
3  p ← 2
4  tantque (p² ≤ N) faire
5      tantque ((p² ≤ N) et (¬EstPremier[p])) faire
6          p ← p + 1
7          k ← 2
8      ftq
9  ftq
10 tantque (k.p ≤ N) faire
11     EstPremier[k.p] ← FAUX
12     k ← k + 1
13 ftq
14 renvoyer(EstPremier)
```

1. version du 14 janvier 2019, 11 : 26

Démontrez qu'à la sortie de la boucle de la ligne 4, le nombre p est un nombre premier. Pourquoi peut-on arrêter la boucle dès que $p^2 > N$?

EXERCICE 4. On note $(p_i)_{i\in\mathbb{N}^*}$ la suite croissante des nombres premiers, i.e. $p_1 = 2$, $p_2 = 3$, etc. Soit $n \in \mathbb{N}$ et $n \geq 1$. On définit $\rho_n := 1 + \prod_{i=1}^{n} p_i$. Quelle est la plus petite valeur de n telle que ρ_n n'est pas un nombre premier ? Quel est la décomposition en produit de facteurs premiers de ρ_n ?

EXERCICE 5. Le premier janvier 2000 était un samedi. Utilisez la division euclidienne pour calculer quel jour de la semaine était le 273-ème jour de cette année.

EXERCICE 6. Le compas d'un bateau à la dérive tourne de 7° dans le sens horaire toutes les 8 minutes. Quelle direction indique le compas après 3 jours, 2 heures et 32 minutes si la direction initiale était de 23° ?

EXERCICE 7. Calculez l'ordre du sous-groupe de $\mathbb{Z}/16\mathbb{Z}$ engendré par 6.

EXERCICE 8. Démontrez la proposition suivante : Soit $n \in \mathbb{N} \setminus \{0\}$, alors $\forall (a, b, c, d) \in \mathbb{Z}^4$, on a

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \pmod{n} \\ ac \equiv bd \pmod{n} \end{cases}$$

EXERCICE 9. Soit $n \in \mathbb{N}$. Démontrez qu'un entier $x \in \mathbb{Z}$ est un multiple de n si et seulement si le reste de la division euclidienne de n par x est nul.

EXERCICE 10. Comment lire dans la table de multiplication de $\mathbb{Z}/n\mathbb{Z}$ si un élément $x \in \mathbb{Z}/n\mathbb{Z}$ est inversible ? Dans ce cas, comment trouver son inverse ? Quel est l'inverse de 7 modulo 25 ? Quel est l'inverse de 11 modulo 26 ?

EXERCICE 11. Un enseignant du collège donne des multiplications de deux nombres de 2 chiffres à ses élèves, et tire ces nombres au hasard. Quelle est la probabilité qu'un élève détecte son erreur de calcul avec la preuve par 9, s'il se trompe sur un seul chiffre du résultat ?

EXERCICE 12. Retrouvez les critères de divisibilité d'un nombre (écrit en base 10) par 5 et par 10 en vous inspirant des calculs faits en cours pour élaborer la preuve par 9. Trouvez de la même façon les critères de divisibilité par 3, 7 et 11.

EXERCICE 13. Vérifiez que $\forall a \in \mathbb{Z} \setminus \{0\} \quad (a, 0) = a$ et que $\forall a \in \mathbb{Z} \quad (a, 1) = 1$.

EXERCICE 14. En supposant qu'un ordinateur est capable de calculer 10^9 éléments de la table de multiplication de $\mathbb{Z}/n\mathbb{Z}$ par seconde, combien de temps faudrait-il pour calculer cette table pour $n = 10^{616}$? NB. Toute vie humaine devrait cesser sur notre planète d'ici 2 à 3 milliards d'années.

EXERCICE 15. Vérifiez qu'appliquer la règle de réécriture

$$R_i : \qquad (u, v) \leftarrow (v, u - q_i v).$$

R_i au couple (u, v) équivaut à remplacer le couple (u, v) par le résultat du produit matriciel suivant :

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \times \begin{pmatrix} u \\ v \end{pmatrix}.$$

EXERCICE 16. Calculez l'inverse de 7 modulo 2018 et l'inverse de 451 modulo 1236.

EXERCICE 17. Expliquez comment un maçon peut s'assurer qu'un mur est à angle droit sans disposer d'une équerre ni d'un mètre en s'appuyant sur l'égalité $3^2 + 4^2 = 5^2$?