Mathématiques pour l'informatique. L1 Informatique I23.

TD 7. Arithmétique [1]

EXERCICE 1. Déterminez les entiers naturels n tels que $n \mid n+8$.

EXERCICE 2. Déterminez les entiers naturels n tels que leur division euclidienne par 3 donne un quotient égal au double du reste.

EXERCICE 3. Déterminez les entiers naturels n tels que les quotients de la division euclidienne de n par 65 et par 79 sont identiques et les restes respectifs sont 63 et 7 ?

EXERCICE 4. Démontrez que la relation de divisibilité dans $\mathbb{Z}$ définie par *"a divise b, noté $a \mid b$, si et seulement s'il existe $c \in \mathbb{Z}$ tel que $ac = b$"* est réflexive, transitive mais n'est ni symétrique ni antisymétrique (ce n'est donc ni une relation d'équivalence, ni une relation d'ordre).

EXERCICE 5. 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 x par n est nul.

EXERCICE 6. Soit n un entier naturel. Démontrez que la relation de congruence modulo n définie sur $\mathbb{Z}$ par *"x est congru à y modulo n, noté $x \equiv y \pmod{n}$, si et seulement si $y - x \in n\mathbb{Z}$"* est compatible avec l'addition dans $\mathbb{Z}$.

EXERCICE 7. Démontrez les assertions suivantes :

1. $\forall (a,b,c) \in \mathbb{Z}^3 \quad a \mid b \;\Rightarrow\; a \mid bc$,

2. $\forall (a,b,c) \in \mathbb{Z}^3 \quad \big((a \mid b) \wedge (a \mid c)\big) \;\Rightarrow a \mid (b+c)$,

3. $\forall (a,a',b,b') \in \mathbb{Z}^4 \quad \big((a \mid a') \wedge (b \mid b')\big) \;\Rightarrow ab \mid a'b'$,

4. $\forall (a,b) \in \mathbb{Z}^2 \;\forall n \in \mathbb{N} \quad a \mid b \;\Rightarrow\; a^n \mid b^n$.

EXERCICE 8. La somme des âges (non-nuls) de trois frères est égale à 39, l'aîné a deux fois l'âge du benjamin (le plus jeune donc). Quels sont les âges des trois frères ? Indication : ne pas faire une étude de cas directe, mais utilisez la division euclidienne de l'âge du cadet par l'âge du benjamin.

1. version du 24 août 2022, 10 : 37

EXERCICE 9. Quel est le nombre de diviseurs positifs de 1 296 ? Indication : décomposez ce nombre en produit de facteurs premiers. Généralisez le résultat à un entier naturel quelconque.

EXERCICE 10. Calculez $(294, 350)$ en décomposant ces deux nombres en produits de facteurs premiers puis utilisez l'algorithme du PGCD d'Euclide.

EXERCICE 11. **1.** Soit n un entier naturel non-nul. Démontrez que pour trouver tous les diviseurs d de n, on peut se contenter de tester la divisibilité des valeurs de l'intervalle $[\![2, \lfloor\sqrt{n}\rfloor]\!]$ dans l'ordre croissant.

2. Un entier naturel $n \leqslant 160$ n'est divisible par aucun des 5 premiers nombres premiers. Est-il premier ?

EXERCICE 12. 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 $n \geqslant 1$. On définit le produit partiel π_n des nombres premiers

$$\pi_n := \prod_{i=1}^{n} p_i.$$

Quelle est la plus petite valeur a de n telle que $\pi_n + 1$ n'est pas un nombre premier ? Quelle est la décomposition en produit de facteurs premiers de $1 + \pi_a$?

EXERCICE 13. † Soit k un entier naturel impair. Démontrez que

$$\forall n \in \mathbb{N}\backslash\{0\} \quad \sum_{i=1}^{n} i^k \quad \text{est divisible par } \frac{n(n+1)}{2} \tag{1}$$

Indication : en notant $S(n,k)$ la somme de la proposition (1) calculez la somme $S(n,k) + S(n,k)$ dans $\mathbb{Z}/n\mathbb{Z}$ en appariant les termes i^k et $(n-i)^k$ puis en appariant les termes i^k et $(n-i+1)^k$.

EXERCICE 14. On suppose que les représentants de $\mathbb{Z}/26\mathbb{Z}$ sont les entiers de l'intervalle $[\![0, 25]\!]$. On note $\mathscr{A} := \{A, B, \ldots, Z\}$ l'alphabet latin et on définit l'application $f : \mathbb{Z}/26\mathbb{Z} \to \mathscr{A}$ par $f(i) :=$ $(i+1)$-ème lettre de $\mathscr{A}$.

1. On munit $\mathbb{Z}/26\mathbb{Z}$ de l'ordre $\leqslant$ induit par $\mathbb{Z}$ et $\mathscr{A}$ de l'ordre alphabétique $\leqslant_{\mathscr{A}}$. Démontrer que f est un isomorphisme d'ensembles ordonnés.

2. Démontrez que l'application $a_k : \mathbb{Z}/26\mathbb{Z} \to \mathbb{Z}/26\mathbb{Z}$ définie par $a_k(x) = x + k$ est une bijection. Quelle est sa bijection réciproque ?

3. Formalisez le chiffrement de César avec un décalage circulaire de k lettres à l'aide d'une application $e_k : \mathscr{A} \to \mathscr{A}$ définie à partir de la bijection f qui identifie les ensembles $\mathscr{A}$ et $\mathbb{Z}/26\mathbb{Z}$ et de l'application a_k.

4. Écrivez les fonctions *Python* `f(x)`, `g(x)` (pour l'application réciproque f^{-1}), `a(k,x)` et `e(k,x)` qui calculent les fonctions définies précédemment.

5. Montrez que e_k est une permutation de $\mathfrak{S}(\mathscr{A})$.

6. Combien existe-t-il d'orbites suivant la permutation e_k ?

EXERCICE 15. Le premier janvier 2000 était un samedi. Quel jour de la semaine était le 275-ème jour de l'année 2000 ?

EXERCICE 16. 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 17. Vérifiez que $\forall a \in \mathbb{Z}\backslash\{0\}\ \ (a,0) = a$ et que $\forall a \in \mathbb{Z}\ \ (a,1) = 1$.

EXERCICE 18. Calculez le PGCD de 231 et 182 avec l'algorithme d'Euclide.

EXERCICE 19. Montrez qu'il n'existe pas d'entiers naturels a et b tels que leur somme est égale à 101 et dont le pgcd est égal à 3.

EXERCICE 20. Pour un examen, on a réparti 367 étudiants dans 9 salles de même capacité en remplissant chaque salle avant d'en ouvrir une autre. Quelle était la capacité des salles et combien d'étudiants composeront dans la dernière salle d'examen ?

EXERCICE 21. † 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 mardi 12 mars et le second le jeudi 14 mars. Quel jour doit-il leur donner rendez-vous pour leur faire effectuer les travaux le plus tôt possible ?

EXERCICE 22. Calculez l'ordre du sous-groupe de $(\mathbb{Z}/16\mathbb{Z}, +)$ engendré par 6.

EXERCICE 23. Démontrez la proposition suivante :
Soit $n \in \mathbb{N}\backslash\{0\}$, 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 24. 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 25. † Retrouvez les critères de divisibilité d'un nombre a (représenté en base 10) par un nombre n pour $n \in \{2,3,5,9,10,11\}$.

EXERCICE 26. Soit n un entier naturel.

1. Montrez que si n est impair alors $n^2 \equiv 1 \pmod 4$ et $n^2 \equiv 1 \pmod 8$.

2. Montrez que si n est pair alors $n^2 \equiv 0 \pmod 4$ et dans ce cas que $n^2 \equiv 0 \pmod 8$ ou $n^2 \equiv 4 \pmod 8$.

EXERCICE 27. Alice et Bob surveillent l'examen terminal de I23 qui se déroule de 9h00 à 12h00. Alice s'est couchée trop tard la veille et somnole 1 minute toutes les 28 minutes tandis que Bob regarde fixement sa montre pendant 1 minute tous les quarts d'heure car les surveillances d'examens l'ennuient. Les étudiants ont vu Alice bailler à 09h08 la première fois, alors que Bob a regardé sa montre dès 09h02.

1. Si t désigne le temps écoulé en minutes depuis le début de l'épreuve, quelle congruence satisfait t pour correspondre aux moments d'inattention d'Alice ? Même question pour Bob ?

2. Justifiez, sans faire de calculs, l'existence de solutions au système de congruences ci-dessus.

3. à quelle(s) heure(s) les étudiants peuvent-ils espérer tricher à l'examen sans être remarqués par les deux surveillants ?

EXERCICE 28. Calculez l'inverse de 7 modulo 2 018 s'il existe. Même question pour 451 modulo 1 236.

EXERCICE 29. Calculez le reste de la division euclidienne de 2^{2021} par 17.

EXERCICE 30. † Démontrez les propositions suivantes :

1. Il existe une infinité d'entiers naturels n tels que $5 \mid 2^n - 3$.

2. Il existe une infinité d'entiers naturels n tels que $13 \mid 2^n - 3$.

3. Démontrez qu'il n'existe aucun entier naturel n tel que $65 \mid 2^n - 3$.

EXERCICE 31. † Trois comètes passent à proximité de la Terre. La première passe tous les 5 ans et est passée l'an dernier, la deuxième passe tous les 8 ans et a été observée il y a deux ans, et la troisième passe tous les 11 ans et a été observée il y a trois ans. Quelle est la prochaine année où l'on pourra les observer toutes les trois ?