TD 1

Arithmétique

Énoncé des exercices

Division euclidienne

Exercice 1 (★☆☆☆☆)

Donner le quotient et le reste de la division euclidienne de a par b dans les cas suivants.

1. $a = 65$ et $b = 23$
2. $a = 23$ et $b = 65$
3. $a = -65$ et $b = 23$
4. $a = 308$ et $b = 45$
5. $a = 1789$ et $b = 41$
6. $a = 2024$ et $b = 18$

Exercice 2 (★☆☆☆☆)

Les écritures suivantes correspondent-elles à la division euclidienne annoncée ? Si oui, justifier. Si non, donner la division euclidienne correcte.

1. $37 = 8 \times 4 + 5$ est la division euclidienne de 37 par 8.
2. $37 = 8 \times 4 + 5$ est la division euclidienne de 37 par 4.
3. $900 = 16 \times 55 + 20$ est la division euclidienne de 900 par 16.
4. $900 = 16 \times 55 + 20$ est la division euclidienne de 900 par 55.
5. $662 = 31 \times 20 + 42$ est la division euclidienne de 662 par 20.

Exercice 3 (★★☆☆☆)

On écrit dans l'ordre alphabétique les lettres 26 de l'alphabet. Arrivé au z on réécrit à nouveau l'alphabet et ainsi de suite :

$$\underbrace{abcdefghijklmnopqrstuvwxyz}_{\text{premier alphabet écrit}}\underbrace{abcdefghijklmnopqrstuvwxyz}_{\text{second alphabet écrit}}abc\cdots$$

Quelle sera la 10000-ème lettre de l'alphabet écrite et combien d'alphabets complets auront été écrits ?

Exercice 4 (★★☆☆☆)

Une développeuse écrit 5070 de code. Pour mettre en page son code elle étudie plusieurs possibilités :

1. Si elle décide de mettre 64 lignes par page. Combien de pages y aura-t-il et combien de lignes restera-t-il sur la dernière page ?
2. Même question si elle décide de mettre 65 lignes par page.

Primalité

Exercice 5 (★☆☆☆☆)

Parmi les entiers suivants dire lesquels sont premiers. Lorsque l'un d'eux n'est pas premier donner un diviseurs strict.

1. 106
2. 107
3. 161
4. 179
5. 253
6. 321
7. 665
8. 1001

Exercice 6 (★★☆☆☆)

1. Déterminer les factorisations en facteurs premiers des entiers suivants
   (a) 106
   (b) 107
   (c) 161
   (d) 80
   (e) 150
   (f) 100
   (g) 200
   (h) 665
   (i) 1001
   (j) 5070 (on rappelle que $5070 = 65 \times 78$)
2. En déduire les pgcd suivants :
   (a) $\text{pgcd}(80, 150)$
   (b) $\text{pgcd}(150, 5070)$
   (c) $\text{pgcd}(161, 5070)$
   (d) $\text{pgcd}(161, 665)$

Exercice 7 (★★☆☆☆)

On pose $A_n = n^2 - 4$ pour $n \geq 2$.

1. Calculer A_n pour $n = 2, 3, 4, 5, 6$ et 7.
2. Montrer que A_n est premier seulement lorsque $n = 3$.

Exercice 8 (★★★☆☆)

On pose $A_n = n^3 + 8$ pour $n \geq 0$.

1. Montrer que si n est pair alors A_n est divisible par 8.
2. (a) Montrer que pour tout $n \in \mathbb{N}, n^2 - 2n + 4 = (n-1)^2 + 3$.
   (b) Développer le produit $(n+2)(n^2 - 2n + 4)$ et en déduire que A_n n'est jamais premier.

Exercice 9 (★★☆☆☆)

On veut montrer que le réel $\sqrt{2}$ est un nombre irrationnel, c'est à dire qu'on ne peut pas l'écrire sous la forme $\frac{a}{b}$ avec $a \in \mathbb{Z}$ et $b \in \mathbb{N}$. On va faire une démonstration par l'absurde en supposant qu'il existe $a, b \in \mathbb{N}$ tels que

$$\sqrt{2} = \frac{a}{b}$$

et on va aboutir à une contradiction.

1. Justifier qu'on peut supposer a et b premiers entre eux.
2. Montrer que $a^2 = 2b^2$. En déduire que $2 \mid a$.
3. En écrivant $a = 2c$ montrer que b^2 est pair.
4. Conclure.

Diviseurs et PGCD

Exercice 10 (★☆☆☆☆)

1. Déterminer la liste des diviseurs positifs des entiers suivants
   (a) 12
   (b) 20
   (c) 30
   (d) 31
   (e) 32
   (f) 63
2. En déduire les pgcd suivants
   (a) $\text{pgcd}(12, 20)$
   (b) $\text{pgcd}(30, 63)$
   (c) $\text{pgcd}(31, 63)$
   (d) $\text{pgcd}(20, 32)$

Exercice 11 (★★★☆☆)

1. Montrer que la somme de trois entiers consécutifs est un multiple de 3.
2. La somme de 4 entiers consécutifs est-elle un multiple de 4 ?
3. Soit p un nombre premier impair. Montrer que la somme de p entiers consécutifs est un multiple de p. *Indication : on pourra se servir de la formule* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

Exercice 12 (★★☆☆☆)

À l'aide de l'algorithme d'Euclide déterminer les $\text{pgcd}(a, b)$ dans les cas suivants puis déterminer une relation de Bézout à l'aide de l'algorithme d'Euclide étendu.

1. $a = 315$ et $b = 85$
2. $a = 84$ et $b = 60$
3. $a = 728$ et $b = 96$
4. $a = 1071$ et $b = 2200$
5. $a = 882$ et $b = 540$
6. $a = 4114$ et $b = 1530$

Exercice 13 (★☆☆☆☆)

Montrer que pour tout entier $a, b, u, v, m \in \mathbb{Z}$ tels qu'on ait

$$au + bv = m.$$

Montrer que $\text{pgcd}(a, b) \mid m$.

Exercice 14 (★★☆☆☆)

Montrer que pour tout entier $a, b \in \mathbb{Z}$ et pour tout $k \in \mathbb{N}$ on a

$$\text{pgcd}(ka, kb) = k \,\text{pgcd}(a, b).$$

Exercice 15 (★★☆☆☆)

Un fleuriste dispose de 280 roses rouges et de 490 roses blanches. Il souhaite faire un maximum de bouquets identiques. Combien de bouquets peut-il faire et quel sera la composition des bouquets.

Exercice 16 (★★☆☆☆)

Soient a et b deux entiers et $d = \text{pgcd}(a, b)$. On considère $u, v \in \mathbb{Z}$ tels que

$$au + bv = d.$$

Montrer que u et v sont premiers entre eux.

Exercice 17 (★★☆☆☆) **Suite de Fibonacci**

On pose (F_n) la suite définie par

$$F_0 = 0, F_1 = 1 \text{ et } \forall n \in \mathbb{N}, F_{n+2} = F_{n+1} + F_n$$

1. Calculer $F_0, \dots, F_8$, les neuf premiers termes de la suite.
2. Montrer par récurrence que pour tout $n \in \mathbb{N}^*$ on a la relation
$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$
3. En déduire que pour tout $n \in \mathbb{N}$, F_n et F_{n+1} sont premiers entre eux.

Calcul modulaire

Exercice 18 (★☆☆☆☆)

1. Montrer que $90 \equiv 6 \mod 7$ et $66 \equiv 3 \mod 7$.
2. Déterminer les plus petits entiers possibles pour compléter les pointillés suivants

$$\begin{array}{lll} 90 + 66 \equiv \dots \mod 7 & 4 \times 90 \equiv \dots \mod 7 & 90 \times 66 \equiv \dots \mod 7 \\ 90^2 \equiv \dots \mod 7 & 66^3 \equiv \dots \mod 7 & 90^{66} \equiv \dots \mod 7 \end{array}$$

Exercice 19 (★★☆☆☆)

1. Justifier qu'il existe une écriture
$$25u + 36v = 1$$
pour certains $u, v \in \mathbb{Z}$ et en déterminer une.
2. Résoudre l'équation modulaire
$$25x \equiv 4 \mod 36.$$

Exercice 20 (★★★☆☆)

On pose $A_n = n^5 + 4n$ pour $n \in \mathbb{Z}$.

1. Calculer A_0, A_1 et A_2.
2. Montrer grâce au petit théorème de Fermat que pour tout $n \in \mathbb{Z}, 5 \mid A_n$.

Exercice 21 (★★★★☆)

1. Montrer que $3^4 \equiv 1 \mod 10$.
2. Montrer par récurrence que pour tout $n \geq 1, 4^{2n} \equiv 6 \mod 10$.
3. Quel est le chiffre des unités de $2024^{2024} + 2023^{2023}$?

Exercice 22 (★★★★☆)

Sachant que le 1er Janvier de l'an 2000 était un samedi. Quel jour sera le 1er Janvier de l'an 3000 ? Et le 1er Janvier de l'an 1000000 ?

Indication : On fera les calculs comme si un an fait exactement $365,25$ *jours, c'est à dire que les années normales font* 365 *jours et tous les* 4 *ans on a une année bissextile à* 366 *jours.*

Numération

Exercice 23 (★☆☆☆☆)

Écrire en base 10 les nombres suivants :

1. $(101)_2$
2. $(101010)_2$
3. $(1011101)_2$
4. $(11011010)_2$
5. $(10)_{16}$
6. $(135)_{16}$
7. $(F2)_{16}$
8. $(4C)_{16}$

Exercice 24 (★☆☆☆☆)

Écrire en base 2 les nombres suivants :

1. 14
2. 16
3. 71
4. 238
5. $(A)_{16}$
6. $(B4)_{16}$
7. $(30A)_{16}$
8. $(6D)_{16}$

Exercice 25 (★☆☆☆☆)

Montrer que pour tout $n \in \mathbb{N}, 2^{n+1} - 2^n = 2^n$ et $2^n + 2^n = 2^{n+1}$

Exercice 26 (★★☆☆☆)

1. On considère $a = (10110)_2$ et $b = (1101)_2$. Sans repasser en base 10 faire les calculs suivants :
   - $a + b$
   - $a - b$
   - Faire la division euclidienne de a par b (donner le reste et le quotient en binaire).
2. Mêmes questions pour $a = (10101101)_2$ et $b = (1100)_2$.

Exercice 27 (★★★★☆)

1. Montrer qu'un nombre $n = (a_k a_{k-1} \dots a_1 a_0)_8$ écrit en base 8 est divisible par 7 si, et seulement si $a_k + \dots + a_1 + a_0 = 0 \mod 7$.
2. L'entier $n = 8^3 + 3 \times 8 + 3$ est-il divisible par 7 ?
3. Même question pour $n = 3 \times 2^6 + 2^5 - 2^3 + 1$.
   Indication : Pour se débarrasser du signe $-$ *qui nous embête on pourra utiliser la relation* $2^{n+1} - 2^n = 2^n$.

Indicatrice d'Euler et protocole RSA

Exercice 28 (★☆☆☆☆)

Soit m un nombre impair. Montrer que $\varphi(2m) = \varphi(m)$.

Exercice 29 (★☆☆☆☆)

Déterminer la valeur de l'indicatrice d'Euler des entiers suivants :

1. 30
2. 64
3. 102
4. $13 \times 17 \times 19$
5. 2^{11}
6. pq lorsque pq sont des nombres premiers distincts

Exercice 30 (★★☆☆☆)

Pour chacun des protocoles RSA ci-dessous déterminer le message codage du message M et décoder le message codé N.

1. $M = 2$ et $N = 11$ pour le protocole $(15, 7)$.
2. $M = 3$ et $N = 2$ pour le protocole $(21, 5)$.

Exercice 31 (★★★☆☆)

Expliquer comment on peut calculer la clé privée et déchiffrer les messages en connaissant la factorisation en nombres premiers d'un protocole RSA (n, e).

Exercice 32 (★★★☆☆)

Expliquer comment on peut calculer la clé privée et déchiffrer les messages d'un protocole RSA en trouvant un message $M < n$ qui ne possède d'inverse modulaire modulo n.

Exercice 33 (★★★★★)

Une personne souhaite envoyer des messages codés à deux destinataires via des protocoles RSA avec des clés publiques (n, e) et (n, f) avec e et f premiers entre eux.

1. Montrer qu'il est possible de décoder les messages sans l'aide de la clé privée d.
   Indication : On pourra s'aider d'une identité de Bézout entre e et f.
2. On considère les protocole RSA de paramètres $(221, 5)$ et $(221, 7)$. On intercepte le même message chiffré M chiffré par chacune des deux clés publiques. Il s'agit de 22 pour la première et 198 pour la seconde.
   (a) Traduire sous forme d'écriture modulaire les informations de l'énoncé.
   (b) Expliciter une identité de Bézout très simple pour les entiers 5 et 7.
   (c) Décoder le message sans calculer la clé privée.
   Indication : on pourra vérifier que $22^3 = 40 \mod n, 198 = 87 \mod n$ *et que* 94 *est l'inverse modulaire de* 84 *modulo* n.
   (d) En remarquant que $13 \times 17 = 221$ retrouver la clé privée de $(n, 5)$ et confirmer le retrouver le résultat de la question précédente.
   Indication : On donne $2^{77} \equiv 32 \mod n$ *et* $11^{11} \equiv 7 \mod n$.