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 $b = 18$

Correction :

1. $65 = 2 \times 23 + 19$
2. $23 = 0 \times 63 + 23$
3. $-65 = -3 \times 23 + 4$
4. $308 = 6 \times 45 + 38$
5. $1789 = 43 \times 41 + 26$
6. $2024 = 112 \times 18 + 8$

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.

Correction :

1. $37 = 8 \times 4 + 5$ est bien la division euclidienne de 37 par 8 car $5 < 8$.
2. $37 = 8 \times 4 + 5$ n'est pas la division euclidienne de 37 par 4 car $5 \geq 4$. On peut la corriger sans refaire tous les calculs.

$$37 = 8 \times 4 + 5 = 8 \times 4 + (4 + 1) = 9 \times 4 + 1.$$

Cette fois-ci c'est la bonne car on a bien $0 \leq 1 < 4$.

3. $900 = 16 \times 55 + 20$ n'est pas la division euclidienne de 900 par 16. De la même façon qu'au dessus on la corrige en factorisant un 16 qu'on sépare du 20. L'écriture $900 = 16 \times 56 + 4$ est la bonne.
4. $900 = 16 \times 55 + 20$ est bien la division euclidienne de 900 par 55.
5. $662 = 31 \times 20 + 42$ n'est pas la division euclidienne de 662 par 20. On a $662 = 31 \times 20 + 42 = 31 \times 20 + 2 \times 20 + 2 = 33 \times 20 + 2$.

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 ?

Correction :

On fait la division euclidienne de 10000 par 26 et on trouve.

$$10000 = 26 \times 384 + 16.$$

On aura donc écrit 384 fois l'alphabet et on en sera à la 16-ème lettre qui est p du 385-ème alphabet.

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.

Correction :

1. La division euclidienne de 5070 par 64 donne $5070 = 64 \times 79 + 14$. Il y aura donc 79 pages complètes et une dernière page avec 14 lignes de code. Donc 80 pages au total.
2. Ne refaisons pas tous les calculs ! On a

$$5070 = 64 \times 79 + 14 = (65 - 1) \times 79 + 14 = 65 \times 79 - 79 + 14 = 65 \times 79 - 65 = 65 \times 78.$$

Il y aura donc 78 pages complètes.

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

Correction :

1. 106 non premier car pair donc divisible par 2.
2. On a $107 < 121$ donc $\sqrt{107} < 11$. Il suffit de tester si 107 est divisible par des nombres premiers < 11 donc par $\{2,3,5,7\}$ pour établir sa primalité. Les critères de divisibilité par $2,3,5,11$ ne donnent rien. D'autre part $107 \equiv 2 \mod 7$ donc 107 n'est pas non plus divisible par 7.
3. $161 < 169$ donc $\sqrt{161} < 13$. Il suffit donc de tester pour les nombres premiers $\{2,3,5,7,11\}$. On a $161 = 7 \times 23$ donc 161 n'est pas un nombre premier.
4. $179 < 196$ donc $\sqrt{179} < 14$. Il suffit donc de tester pour les nombres premiers $\{2,3,5,7,11,13\}$. On a $1+9 = 10 \neq 7 \mod 11$ donc 179 n'est pas divisible par 11. Par ailleurs, $179 \equiv 4 \mod 7, 179 \equiv 10 \mod 13$ donc il n'est pas divisible non plus par 7 et 13 donc il est premier.
5. On remarque que $2+3 = 5 \mod 11$ donc 253 est divisible par 11.
6. On a $3+2+1 = 6$ divisible par 3 donc 321 est divisible par 3.
7. Le chiffre est unité de 665 est 5 donc il est divisible par 5.
8. On a $1+0 \equiv 0+1 \mod 11$ donc 1001 est divisible par 11 donc non premier.

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) pgcd$(80, 150)$
   (b) pgcd$(150, 5070)$
   (c) pgcd$(161, 5070)$
   (d) pgcd$(161, 665)$

Correction :

1. On a $106 = 2 \times 53$ et 53 est premier car non divisible par $2,3,5$ et 7 car $53 \equiv 4 \mod 7$. Donc $106 = 2 \times 53$ est la décomposition en facteurs premiers de 106.
2. 107 est sa propre décomposition en facteurs premiers car il est premier.
3. $161 = 7 \times 23$ est la décomposition en facteurs premiers car 7 et 23 sont premiers.
4. $80 = 4 \times 20 = 2^2 \times 4 \times 5 = 2^4 \times 5$.
5. $150 = 15 \times 10 = 3 \times 5 \times 2 \times 5 = 2 \times 3 \times 5^2$.
6. $100 = 4 \times 25 = 2^2 \times 5^5$
7. $200 = 2 \times 100 = 2^3 \times 5^5$
8. $665 = 5 \times 133$. Il faut alors déterminer si 133 est premier ou non. On a $133 = 7 \times 19$ donc $665 = 5 \times 7 \times 19$ est la décomposition en facteurs premiers de 665.
9. $1001 = 11 \times 91$ et $91 = 7 \times 13$ donc $1001 = 7 \times 11 \times 13$.
10. $5070 = 65 \times 78$ donc il suffit de décomposer 65 et 78. On a $65 = 5 \times 13$ et $78 = 2 \times 39 = 2 \times 3 \times 13$ donc $5070 = 2 \times 3 \times 5 \times 13^2$.

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 $n = 3$.

Correction :

1. $A_2 = 0, A_3 = 5, A_4 = 12, A_5 = 21, A_6 = 32, A_7 = 45$.
2. On utilise l'identité remarquable $a^2 - b^2 = (a - b)(a + b)$ qui donne

$$A_n = (n - 2)(n + 2).$$

Lorsque $n > 3$ on a donc $n - 2 > 1$ et $n + 2 > 5$ qui sont donc des diviseurs stricts de A_n donc A_n ne peut être premier lorsque $n > 3$ donc $A_3 = 5$ est bien le seul.

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.

Correction :

1. Si n est pair, on peut écrire $n = 2k$ pour un certain $k \in \mathbb{N}$ mais alors $A_n = n^3 + 8 = (2k)^3 + 8 = 8k^3 + 8 = 8(k^3 + 1)$ donc est bien divisible par 8.
2. On développe $(n - 1)^2 + 3 = n^2 - 2n + 1 + 3 = n^2 - 2n + 4$..
3. On a $(n + 2)(n^2 - 2n + 4) = n^3 - 2n^2 + 4n + 2n^2 - 4n + 8 = n^3 + 8 = A_n$. Puisque $n^2 - 2n + 4 \geq 3$ et $n + 2 \geq$ il s'agit toujours d'une factorisation non triviale de A_n donc 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.

Correction :

1. Si a et b ont un diviseur commun on peut le simplifier au numérateur et au dénominateur. Donc quitte à remplacer a et b par $\frac{a}{\text{pgcd}(a,b)}$ et $\frac{b}{\text{pgcd}(a,b)}$ on peut supposer qu'il sont premiers entre eux.
2. En passant la relation $\sqrt{2} = \frac{a}{b}$ au carré et en multipliant par b^2 on obtient bien $a^2 = 2b^2$. Ceci prouve que $2 \mid a^2$ mais alors $2 \mid a$.
3. Avec $a = 2c$ on a $(2c)^2 = 2b^2$, i.e. $4c^2 = 2b^2$ donc $b^2 = 2c^2$ donc par le même raisonnement qu'avant b est aussi divisible par 2. Ceci contredit l'hypothèse selon laquelle a et b sont premiers entre eux. Donc notre hypothèse de départ est fausse et donc $\sqrt{2}$ est irrationnel.

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) pgcd(12, 20)
   (b) pgcd(30, 63)
   (c) pgcd(31, 63)
   (d) pgcd(20, 32)

Correction :

1.

   (a) $D(12) = \{1, 2, 3, 4, 6, 12\}$
   (b) $D(20) = \{1, 2, 4, 5, 10, 20\}$
   (c) $D(30) = \{1, 2, 3, 5, 6, 10, 15, 30\}$
   (d) $D(31) = \{1, 31\}$
   (e) $D(32) = \{1, 2, 4, 8, 16, 32\}$
   (f) $D(63) = \{1, 3, 7, 9, 21, 63\}$

2. (a) pgcd(12, 20) = 4
   (b) pgcd(30, 63) = 3
   (c) pgcd(31, 63) = 1
   (d) pgcd(20, 32) = 4

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* $\sum_{k=0}^{n} k = \frac{n(n+1)}{2}$.

Correction :

1. On note a un entier. Les entiers consécutifs s'écrivent $a+1$ et $a+2$. On a donc $a + (a+1) + (a+2) = 3a + 3 = 3(a+1)$. Il s'agit donc bien d'un multiple de 3.
2. C'est faux. Par exemple $0 + 1 + 2 + 3 = 6$ qui n'est pas divisible par 4.
3. De la même façon que dans la première question il s'agit de déterminer si l'entier

$$a + (a+1) + \cdots + (a+p-1)$$

est un multiple de p. On a

$$a + (a+1) + \cdots + (a+p-1) = pa + 0 + 1 + \cdots + p - 1 = pa + \sum_{k=0}^{p-1} k = pa + \frac{(p-1)p}{2} = pa + p\frac{p-1}{2}.$$

Puisque p est impair $\frac{p-1}{2}$ est bien un entier et donc la somme est bien un multiple de p.

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 $b = 1530$

Correction :

Je détaille seulement le premier et je donne les réponses pour les suivants.

1. On a

$$315 = 3 \times 85 + 60 \quad (1)$$
$$85 = 1 \times 60 + 15 \quad (2)$$
$$60 = 4 \times 15 + 0 \quad (3)$$

Donc $\text{pgcd}(315, 85) = 15$. Par ailleurs $15 = 85 - 60$ d'après la seconde ligne. Puis $15 = 85 - (315 - 3 \times 85)$ d'après la première. Donc que

$$4 \times 85 - 1 \times 315 = 15.$$

Donc 4 et -1 sont des coefficients de Bézout.

2. $\text{pgcd}(84, 60) = 12$ et $3 \times 60 - 2 \times 84 = 12$.
3. $\text{pgcd}(728, 96) = 8$ et $38 \times 96 - 5 \times 728 = 8$.
4. $\text{pgcd}(4114, 1530) = 34$ et $16 \times 4114 - 43 \times 1530 = 34$
5. $\text{pgcd}(882, 540) = 18$ et $18 \times 540 - 11 \times 882 = 18$.
6. $\text{pgcd}(2200, 1071) = 1$ et $277 \times 2200 - 569 \times 1071 = 1$

Exercice 13 (★☆☆☆☆)

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

$$au + bv = m.$$

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

Correction :

En effet, $d \mid a$ et $d \mid b$ donc $d \mid au + bv = m$.

Exercice 14 (★★☆☆☆)

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

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

Correction :

On pose $d = \text{pgcd}(a, b)$ on a $d \mid a$ et $d \mid b$ donc $kd \mid ka$ et $kd \mid kb$ donc $kd \mid \text{pgcd}(ka, kb)$.

Réciproquement, si on considère une relation de Bézout

$$au + bv = d$$

alors $kau + kbv = kd$ donc, d'après l'exercice précédent on a $\text{pgcd}(ka, kb) \mid kd$.

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

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.

Correction :

Si on note d le nombre de bouquets alors d est un diviseur de 280 et de 490. Puisqu'on veut qu'il soit maximum alors $d = \text{pgcd}(280, 490)$. On peut calculer ce pgcd en factorisant 280 et 490 en facteurs premiers ou grâce à l'algorithme d'Euclide mais, pour changer, on va le calculer grâce à l'exercice précédent.

On a

$$\text{pgcd}(280, 490) = \text{pgcd}(10 \times 28, 10 \times 49) = 10 \times \text{pgcd}(28, 49) = 10 \times \text{pgcd}(7 \times 4, 7 \times 7) = 70\,\text{pgcd}(4, 7) = 70$$

car 7 et 4 sont premiers entre eux. On peut donc faire 70 bouquets. Chacun contiendra $280/70 = 4$ roses rouges et $490/70 = 7$ roses blanches.

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.

Correction :

Par définition du pgcd les entiers a et b sont divisibles par d donc en divisant la relation de Bézout par d on obtient

$$\frac{a}{d}u + \frac{b}{d}v = 1$$

qui est une identité de Bézout et donc qui implique 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.

Correction :

1. On a
$$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, F_7 = 13, F_8 = 21.$$
2. On pose $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$. pour $n \geq 1$.

   Initialisation : On prouve $P(1)$. On a $F_2 \times F_0 - F_1^2 = -1$. Par ailleurs $(-1)^1 = -1$ donc l'initialisation est validée.

   Hypothèse de récurrence : Soit $n \geq 1$ tel que $P(n)$ est vraie, i.e. $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$..

   Hérédité : Montrons que $P(n+1)$ est vraie en utilisant $P(n)$. C'est-à-dire qu'on veut montrer que $F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$.

   Par définition de la suite on a $F_{n+2} = F_{n+1} + F_n$ donc, en multipliant par F_n et en enlevant F_{n+1}^2 on a

$$F_{n+2}F_n - F_{n+1}^2 = F_{n+1}F_n + F_n^2 - F_{n+1}^2 = F_{n+1}\underbrace{(F_n - F_{n+1})}_{=-F_{n-1}} + F_n^2 = -F_{n+1}F_{n-1} + F_n^2 \underbrace{=}_{\text{HR}} -(-1)^n = (-1)^{n+1}.$$

Ceci conclut la récurrence.

3. F_0 et F_1 sont premiers entre eux car 1 est premier avec tout entier. Si $n \geq 1$ alors en fonction de si n est pair ou impair on a soit

$$F_{n+1}F_{n-1} - F_n^2 = 1 \text{ soit } -F_{n+1}F_{n-1} + F_n^2 = 1$$

qui fournit une identité de Bézout entre F_n et F_{n+1}. Donc ils sont bien premiers entre eux pour tout $n \in \mathbb{N}$.

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

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

Correction :

1. On a $90 = 7\times 12 + 6$ et $66 = 7\times 9 + 3$.
2. On a

- $90 + 66 \equiv 6 + 3 \equiv 9 \equiv 2 \mod 7$
- $4 \times 90 \equiv 4 \times 6 \equiv 24 \equiv 3 \mod 7$
- $90 \times 66 \equiv 6 \times 3 \equiv 18 \equiv 4 \mod 7$
- $90^2 \equiv 6^2 \equiv 36 \equiv 1 \mod 7$
- $66^3 \equiv 3^3 \equiv 27 \equiv 6 \mod 7$
- Je propose deux solutions qui donnent (heureusement) le même résultat.

  Méthode 1 : Puisque $90 \equiv 6 \equiv -1 \mod 7$ on a $90^{66} \equiv (-1)^{66} \equiv 1 \mod 7$.

  Méthode 2 : Puisque $90 \not\equiv 0 \mod 7$ d'après le petit théorème de Fermat on a $90^6 \equiv 1 \mod 7$ donc $(90^6)^{11} = 90^{66} \equiv 1^{11} \equiv 1 \mod 7$.

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

$$25x \equiv 4 \mod 36.$$

Correction :

1. On a $25 = 5^2$ et $36 = 6^2 = 2^2 \times 3^2$ donc ils n'ont pas de facteur commun autre que 1. D'après l'identité de Bézout il existe $u, v \in \mathbb{Z}$ tels que $25u + 36v = 1$. On peut en trouver en appliquant l'algorithme de Bézout étendu. On trouve par exemple $25 \times 13 - 36 \times 9 = 1$.

2. On a

$$25x \equiv 4 \mod 36 \Leftrightarrow \underbrace{13 \times 25}_{=1} x \equiv 13 \times 4 \equiv 52 \equiv 16 \mod 36.$$

Donc $x \equiv 16 \mod 36$ est la seule solution.

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 $n \in \mathbb{Z}, 5 \mid A_n$.

Correction :

1. On a $A_0 = 0, A_1 = 5$ et $A_2 = 40$.
2. D'après le petit théorème de Fermat on a pour tout $n \in \mathbb{Z}$ non divisible par 5

$$n^4 \equiv 1 \mod 5$$

donc $n^5 \equiv n \mod 5$. Lorsque $5 \mid n$ alors cette dernière relation est vraie car cela donne $0^5 \equiv 0 \mod 5$. Donc pour tout $n \in \mathbb{Z}$ on a $n^5 \equiv n \mod 5$ donc

$$n^5 - n \equiv n^5 + 4n \equiv 0 \mod 5$$

car $-1 \equiv 4 \mod 5$. Ceci signifie bien que $5 \mid A_n$.

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 $2024^{2024} + 2023^{2023}$?

Correction :

1. On a $3^2 = -1 \mod 10$ et $3^4 \equiv 1 \mod 10$
2. On pose $P(n)$: $4^{2n} \equiv 6 \mod 10$ pour $n \geq 1$.

Initialisation : On prouve $P(1)$. On a $4^2 = 16 \equiv 6 \mod 10$.

Hypothèse de récurrence : Soit $n \geq 1$ tel que $P(n)$ est vraie, i.e. $4^{2n} \equiv 6 \mod 10$.

Hérédité : Montrons que $P(n+1)$ est vraie en utilisant $P(n)$. On a

$$4^{2(n+1)} = 4^{2n+2} = 4^{2n} \times 4^2 \equiv \underbrace{6}_{\text{HR}} \times 6 \equiv 36 \equiv 6 \mod 10.$$

Ceci conclut la récurrence.

3. Le chiffre des unités correspond au reste de la division euclidienne par 10. On a $2024^{2024} + 2023^{2023} = 4^{2024} + 3^{2023} \mod 10$. D'après la première question $3^{2023} = 3^{2020+3} = 3^3 = 7 \mod 10$. D'après la deuxième question on a $4^{2024} \equiv 6 \mod 10$. Finalement, $2024^{2024} + 2023^{2023} = 6 + 7 = 3 \mod 10$. Donc le chiffre des unités est 3.

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.*

Correction :

L'an 3000 est 1000 ans plus tard que l'an 2000. Tous les 4 ans $3\times365+366$ jours s'écoulent (attention aux années bissextiles). Donc en 1000 ans $N=250\times(3\times365+366)$ jours s'écoulent. Tous les 7 jours on retombe sur un samedi donc ce qui nous intéresse c'est le reste modulo 7 de N. Pour cela, pas besoin de le calculer ! Il suffit de calculer indépendamment les restes de chacun des entiers qui le composent.

- On a $250\equiv \underbrace{210}_{7\times30}+30\equiv30\equiv2 \mod 7$.
- D'autre part, $365\equiv \underbrace{350}_{7\times50}+15\equiv15\equiv1 \mod 7$ donc $366\equiv2 \mod 7$ et $3\times365+366\equiv5 \mod 7$.

On en déduit que $N\equiv2\times5\equiv3 \mod 7$. Donc en l'an 3000 un certain nombre de semaines plus 3 jours se seront écoulés depuis l'an 2000. Ce sera donc un mercredi !

Puisque N représente 1000 ans écoulé alors N^2 représente $1000^2=1000000$ ans écoulés ce qui correspond donc à $N^2\equiv3^2\equiv2 \mod 7$ jours modulo 7. Il suffit donc de déterminer quel jour était le 1^{er} Janvier de l'an 0. C'était 2000 ans avant l'an 2000 donc $-2N$ jours écoulés. Or $-2N\equiv-6\equiv1 \mod 7$. Donc le premier Janvier de l'an 0 était un dimanche et le premier janvier de l'an 1000000 sera donc un mercredi aussi.

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. $(4C)_{16}$

Correction :

1. $(101)_2=5$
2. $(101010)_2=42$
3. $(1011101)_2=93$
4. $(11011010)_2=218$
5. $(10)_{16}=16$
6. $(135)_{16}=309$
7. $(F2)_{16}=242$
8. $(4C)_{16}=76$

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. $(6D)_{16}$

Correction :

1. $14 = (1110)_2$
2. $16 = (10000)_2$
3. $71 = (1000111)_2$
4. $238 = (11101110)_2$
5. $(E)_{16} = (1110)_2$ (c'est 14).
6. $(B4)_{16} = (10110100)_2$
7. $(30A)_{16} = (1100001010)_2$
8. $(6D)_{16} = (1101101)_2$

Exercice 25 (★☆☆☆☆)

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

Correction :

On peut factoriser par 2^n ce qui donne $2^{n+1} - 2^n = 2^n(2-1) = 2^n$. Par ailleurs, $2^n + 2^n = 2 \times 2^n = 2^{n+1}$.

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 $b = (1100)_2$.

Correction :

1. On a
   - $a + b = (100011)_2$
   - $a - b = (1001)_2$
   - Puisque $0 \leq (1001)_2 < b$ on a $a = b + (1001)_2$.
2. On a
   - $a + b = (10111001)_2$
   - $a - b = (10100001)_2$
   - On a $a = (1110)_2 b + (101)_2$.

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 $2^{n+1} - 2^n = 2^n$.

Correction :

1. Par définition $n = 8^k a_k + \dots + 8a_1 + a_0$. Puisque pour tout $n \in \mathbb{N}, 8^n \equiv 1^n \equiv 1 \mod 7$ on a
$$n \equiv a_k + \dots + a_1 + a_0 \mod 7.$$
2. En base 8 on a $n = (1033)_8$ et $1 + 0 + 3 + 3 = 7 \equiv 0 \mod 7$ donc n est divisible par 7.

3. Comme indiquer on commence par essayer de se débarrasser du $-$. On a $-2^3 = 2^3 - 2^4$ donc

$$n = 3\times 2^6 + \underbrace{2^5 - 2^4}_{=2^4} + 2^3 + 1 = 3\times 2^6 + 2^4 + 2^3 + 1.$$

On essaie ensuite de faire apparaître des puissance de 8.

$$n = 3\times (2^3)^2 + 2\times 2^3 + 2^3 + 8^0 = 3\times 8^2 + 3\times 8 + 1 = (331)_8$$

donc encore une fois cet entier est divisible par 7.

Indicatrice d'Euler et protocole RSA

Exercice 28 (★☆☆☆☆)

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

Correction :

Puisque m est impair il est premier avec 2 donc $\varphi(2m) = \varphi(2)\varphi(m) = (2-1)\varphi(m) = \varphi(m)$.

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

Correction :

1. $\varphi(30) = 4\times 2 = 8$
2. $\varphi(64) = \varphi(2^6) = 2^5 = 32$
3. $\varphi(102) = \varphi(3\times 34) = 2\times(17-1)\times 1 = 32$.
4. $\varphi(13\times 17\times 19) = \varphi(13)\varphi(17)\varphi(19) = 12\times 16\times 18$.
5. $\varphi(2^{11}) = 2^{10} = 1024$.
6. $\varphi(pq) = (p-1)(q-1)$

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 $(21, 5)$.

Correction :

1. $2^7 \equiv 8 \mod 15$ donc le message codé est 8. On a $15 = 3\times 5$ donc $\varphi(n) = 2\times 4$. L'inverse modulaire de 7 est -1 car $7\times -1 \equiv 1 \mod 8$ donc pour décoder 11 on calcule $11^{-1} = 11$ car $11\times 4 = 44 \equiv -1$ donc $11^{-1} \equiv -4 \equiv 11 \mod 15$.
2. $3^5 \equiv 3^3\times 9 \equiv 6\times 9 \equiv 6\times 3\times 3 \equiv -3\times 3 \equiv 12 \mod 21$. On a $21 = 3\times 7$ donc $\varphi(21) = 2\times 6 = 12$ et l'inverse modulaire de 5 modulo 12 est 5 car $5\times 5 = 2\times 12 + 1$. On en déduit que le message déchiffré de $N = 2$ est $2^5 \equiv 32 \equiv 11 \mod 21$.

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).

Correction :

Si on connaît la factorisation $n = pq$ alors on peut calculer $\varphi(n) = (p-1)(q-1)$. On peut alors calculer une relation de Bézout $ed + \varphi(n)v = 1$. Par définition d est l'inverse de e modulo $\varphi(n)$. Si on considère un message chiffré M^e on a alors

$$(M^e)^d \times \underbrace{M^{\varphi(n)v}}_{\equiv 1 \mod n} = M^{ed+\varphi(n)v} = M^1 \equiv M \mod n.$$

Garder la factorisation de n secrète est donc primordial pour la sécurité du protocole.

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.

Correction :

Ceci signifie que M n'est pas premier avec $n = pq$ et puisque $M < n$ alors M est soit divisible par p soit par q. Donc $\text{pgcd}(M, n) = p$ ou q. Un pgcd se calcule très rapidement à l'aide de l'algorithme d'Euclide donc on peut déterminer la factorisation de n en trouvant p ou q et en déduire la clé privée.

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 $11^{11} \equiv 7 \mod n$.

Correction :

1. On considère une relation de Bézout $ue + vf = 1$ pour $u, v \in \mathbb{Z}$. Si on a à dispositions les messages chiffrés M^e et M^f on peut alors calculer

$$(M^e)^u (M^f)^v = M^{eu+vf} = M^1 = M \mod n.$$

   On retrouve donc bien le message M sans avoir utilisé la clé privée qui nous est toujours inconnue.

2. (a) On a $M^5 = 22$ et $M^7 = 198$.
   (b) On a $3 \times 5 - 2 \times 7 = 1$.
   (c) D'après la première question on peut déchiffrer le message M en effectuant les opérations

$$M \equiv M^1 \equiv M^{3\times 5 - 2\times 7} \equiv \left(M^5\right)^3 \left(M^7\right)^{-2} \equiv 22^3 \times 198^{-2} \mod n.$$

On a

$$22^3 = 2^3 \times 11^3 \equiv 8 \times 121 \times 11 \equiv 4 \times 242 \times 11 \equiv 4 \times 21 \times 11 \equiv 4 \times 231 \equiv 4 \times 10 \equiv 40 \mod n$$

et

$$198^2 = (9 \times 11 \times 2)^2 = 81 \times \underbrace{121 \times 2}_{\equiv 21} \times 2 \equiv 81 \times 21 \times 2 \equiv \underbrace{81 \times 3}_{\equiv 22} \times 7 \times 2 \equiv 11 \times 28 \equiv 308 \equiv 87 \mod n.$$

Enfin, on a

$$94 \times 87 \equiv 47 \times 6 \times 29 \equiv 61 \times 29 \equiv 1 \mod n.$$

Pour conclure on a

$$22^3 \times 198^{-2} \equiv 40 \times 94 \equiv 10 \times 2 \times \underbrace{4 \times 47}_{\equiv -33} \equiv -330 \times 2 \equiv -109 \times 2 \equiv 3 \mod n$$

Donc le message codé était 3.

(d) On a alors $\varphi(n) = 12 \times 16 = 192$, 5 possède pour inverse modulaire 77. On calcule $22^{77} = 2^{77}11^{77} \equiv 32 \times 7 \equiv 224 \equiv 3 \mod n$.