



Prénom :

Nom :

Note : / 20

I. (2 points)

Pour tout entier naturel $p \geq 2$, on pose $N_p = \overline{1\dots 1}$ où le chiffre 1 apparaît p fois.

Écrire l'égalité de la division euclidienne de N_{p+1} par N_p . Justifier sur les deux lignes qu'il s'agit bien de l'égalité de la division euclidienne de N_{p+1} par N_p .

.....

Dans la division euclidienne de N_{p+1} par N_p , le quotient est égal à et le reste est égal à

II. (4 points : 2 points + 2 points)

Les publications en série, comme les journaux et les périodiques, sont toutes identifiées par un numéro ISSN (International Standard Serial Number). En France, ce numéro est attribué par le Centre national d'enregistrement des publications en série. L'ISSN comporte huit caractères répartis en deux groupes de quatre, ces groupes étant séparés par un tiret. Le tableau ci-après donne les numéros ISSN de quelques journaux ou périodiques français.

| Journal ou périodique | Numéro ISSN |
|------------------------|-------------|
| Le Monde | 1950-6244 |
| Le Figaro | 1241-1248 |
| Le Nouvel Observateur | 0029-4713 |
| Les Échos | 0153-4831 |
| Libération | 0335-1793 |
| Le Canard Enchaîné | 0008-5405 |
| Courrier International | 1154-516X |

Les sept premiers caractères d'un numéro ISSN sont des chiffres qui caractérisent la publication. Le dernier caractère, situé en huitième position, sert de clé de contrôle et est pris dans l'ensemble $E = \{0; 1; 2; 3; 4; 5; 6; 7; 8; 9; X\}$ où les chiffres de 0 à 9 représentent le nombre correspondant et le caractère X représente le nombre 10.

Pour déterminer la clé de contrôle d'un numéro ISSN dont les sept premiers chiffres correspondent aux nombres a, b, c, d, e, f, g :

- on calcule le nombre $N = 8a + 7b + 6c + 5d + 4e + 3f + 2g$;
- on détermine le reste r de $-N$ dans la division euclidienne par 11 ;
- la clé de contrôle est le caractère de l'ensemble E correspondant au nombre r .

Par exemple, pour *Le Monde*, on a $N = 8 \times 1 + 7 \times 9 + 6 \times 5 + 5 \times 0 + 4 \times 6 + 3 \times 2 + 2 \times 4 = 139$. Le reste de la division euclidienne de $-N$ par 11 est 4. La clé de contrôle est donc bien égale à 4.

1°) En détaillant les étapes, retrouver la clé de contrôle du périodique *Courrier International*.

.....

.....

.....

.....

2°) Le deuxième caractère du numéro ISSN d'un journal est illisible. Si l'on note n ce caractère, le numéro ISSN est $3n08-2138$. Déterminer la valeur de n .

..... (écrire la valeur sans égalité et sans justifier)

III. (4 points)

À toute lettre de l'alphabet on associe un entier naturel x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

| | | | | | | | | | | | | |
|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|----------|
| A | B | C | D | E | F | G | H | I | J | K | L | M |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Le « chiffre de Rabin » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q . Le couple $(p; q)$ est sa clé privée qu'elle garde secrète.

Elle calcule ensuite $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leq B \leq n - 1$.

Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.

Le codage d'une lettre représentée par l'entier x est le nombre y tel que y soit le reste de la division euclidienne de $x(x+B)$ par n .

Dans l'exercice, on prend $p = 3$ et $q = 11$ donc $n = p \times q = 33$ et $B = 13$.

Coder le mot « ET » puis décoder la lettre A.

..... (une seule réponse)

Le « chiffre de Rabin » est-il utilisable pour décoder un message lettre par lettre ?

.....

IV. (2 points)

À l'aide de la calculatrice, déterminer tous les entiers naturels x inférieurs ou égaux à 29 tels que le reste de la division euclidienne de x^2 par 30 soit égal à 16.

..... (écrire les valeurs en les séparant par des virgules)

V. (2 points)

On considère la fonction f définie sur \mathbb{Z} par $f(n) = \frac{n}{3}$ si n est divisible par 3 et $f(n) = 3 - n$ si n n'est pas divisible par 3.

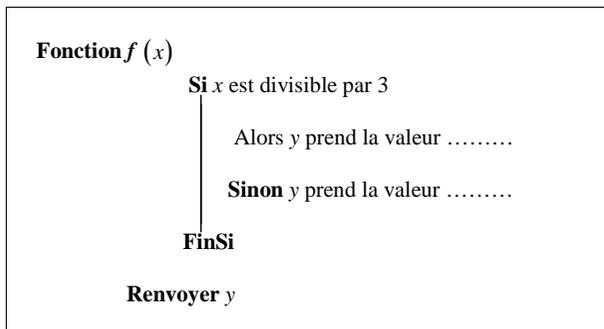
- Déterminer le(s) antécédent(s) de -2 par f ?

.....

- L'affirmation « Tout entier relatif admet deux antécédents par f » est-elle vraie ou fausse ? Justifier.

.....

- On considère la fonction écrite ci-dessous en langage naturel dans le cadre de gauche dont le script correspondant en langage Python est donné dans le cadre de droite. Compléter le cadre de gauche.



```

def f(x):
    if n%3 == 0 :
        y = x / 3
    else :
        y = 3 - x
    return y

```

VI. (6 points : 1°) 1 point ; 2°) 1 point ; 3°) 1 point ; 4°) 3 points)

On considère un entier relatif a tel que le reste de la division euclidienne de a par 20 soit égal à 13.

On note q le quotient de la division euclidienne. On a donc $a = 20q + 13$ (1).

Les questions sont indépendantes les unes des autres.

1°) Quelle est la parité de a ?

.....

2°) Le but de cette question est de déterminer le quotient et le reste de la division euclidienne de a par 10.

On reprend l'égalité (1) en effectuant les transformations successives suivantes : $a = 10 \times 2q + 13$;

$a = 10 \times 2q + 10 + 3$; $a = 10 \times (2q + 1) + 3$.

Expliquer pourquoi la dernière égalité correspond à la division euclidienne de a par 10.

.....
.....

Dans la division euclidienne de a par 10, le quotient est égal à et le reste est égal à

3°) Le but de cette question est de déterminer le quotient et le reste de la division euclidienne de $a + 5$ par 20.

On reprend l'égalité (1). En ajoutant 5 à chaque membre, on obtient : $a + 5 = 20q + 18$.

Expliquer pourquoi la dernière égalité correspond à la division euclidienne de $a + 5$ par 20.

.....
.....

Dans la division euclidienne de $a + 5$ par 20, le quotient est égal à et le reste est égal à

4°) En reprenant la même méthode qu'à la question précédente, déterminer le reste et le quotient de la division euclidienne de $a + 7$, $a + 8$ et $-a$ par 20. On effectuera le travail de recherche au brouillon.

- Dans la division euclidienne de $a + 7$ par 20, le quotient est égal à et le reste est égal à

- Dans la division euclidienne de $a + 8$ par 20, le quotient est égal à et le reste est égal à

- Dans la division euclidienne de $-a$ par 20, le quotient est égal à et le reste est égal à

Corrigé du contrôle du 4-11-2019

I.

Pour tout entier naturel $p \geq 2$, on pose $N_p = \overline{1\dots 1}$ où le chiffre 1 apparaît p fois.

Écrire l'égalité de la division euclidienne de N_{p+1} par N_p . Justifier sur les deux lignes qu'il s'agit bien de l'égalité de la division euclidienne de N_{p+1} par N_p .

$$N_{p+1} = N_p \times 10 + 1$$

Pour répondre à cette question, il faut raisonner dans le cas général et non en prenant une valeur particulière de p . Les valeurs particulières de p ne donnent qu'une idée du résultat.

$$N_p \times 10 + 1 = \underbrace{\overline{1\dots 1}}_{p \text{ fois}} \times 10 + 1 = \underbrace{\overline{11\dots 10}}_{p \text{ fois}} + 1 = \underbrace{\overline{11\dots 1}}_{p+1 \text{ fois}} = N_{p+1}$$

10 et 1 sont des entiers.

De plus, $1 < N_p$ puisque $p \geq 2$ par hypothèse (le reste d'une division euclidienne doit toujours être strictement inférieur au diviseur).

Dans la division euclidienne de N_{p+1} par N_p , le quotient est égal à 10 et le reste est égal à 1.

II.

Les publications en série, comme les journaux et les périodiques, sont toutes identifiées par un numéro ISSN (International Standard Serial Number). En France, ce numéro est attribué par le Centre national d'enregistrement des publications en série. L'ISSN comporte huit caractères répartis en deux groupes de quatre, ces groupes étant séparés par un tiret. Le tableau ci-après donne les numéros ISSN de quelques journaux ou périodiques français.

| Journal ou périodique | Numéro ISSN |
|------------------------|-------------|
| Le Monde | 1950-6244 |
| Le Figaro | 1241-1248 |
| Le Nouvel Observateur | 0029-4713 |
| Les Échos | 0153-4831 |
| Libération | 0335-1793 |
| Le Canard Enchaîné | 0008-5405 |
| Courrier International | 1154-516X |

Les sept premiers caractères d'un numéro ISSN sont des chiffres qui caractérisent la publication. Le dernier caractère, situé en huitième position, sert de clé de contrôle et est pris dans l'ensemble $E = \{0; 1; 2; 3; 4; 5; 6; 7; 8; 9; X\}$ où les chiffres de 0 à 9 représentent le nombre correspondant et le caractère X représente le nombre 10.

Pour déterminer la clé de contrôle d'un numéro ISSN dont les sept premiers chiffres correspondent aux nombres a, b, c, d, e, f, g :

- on calcule le nombre $N = 8a + 7b + 6c + 5d + 4e + 3f + 2g$;
- on détermine le reste r de $-N$ dans la division euclidienne par 11 ;
- la clé de contrôle est le caractère de l'ensemble E correspondant au nombre r .

Par exemple, pour *Le Monde*, on a $N = 8 \times 1 + 7 \times 9 + 6 \times 5 + 5 \times 0 + 4 \times 6 + 3 \times 2 + 2 \times 4 = 139$.

Le reste de la division euclidienne de $-N$ par 11 est 4. La clé de contrôle est donc bien égale à 4.

1°) En détaillant les étapes, retrouver la clé de contrôle du périodique *Courrier International*.

On applique la formule $N = 8a + 7b + 6c + 5d + 4e + 3f + 2g$ avec les chiffres a, b, c, d, e, f, g respectivement égaux à 1, 1, 5, 4, 5, 1, 6.

On calcule $N = 8 \times 1 + 7 \times 1 + 6 \times 5 + 5 \times 4 + 4 \times 5 + 3 \times 1 + 2 \times 6 = 100$.

L'égalité $-100 = 11 \times (-10) + 10$ donne la division euclidienne de $-N$ par 11.

Le reste est 10 donc la clé est bien X.

2°) Le deuxième caractère du numéro ISSN d'un journal est illisible. Si l'on note n ce caractère, le numéro ISSN est 3n08-2138. Déterminer la valeur de n .

3 (écrire la valeur sans égalité et sans justifier)

Le nombre N est égal à $8 \times 3 + 7 \times n + 6 \times 0 + 5 \times 8 + 4 \times 2 + 3 \times 1 + 2 \times 3 = 7n + 81$.

On cherche ensuite n tel que le reste de $-(7n + 81)$ soit égal à 8.

On teste les chiffres de 0 à 9 les uns après les autres. On a la chance de tomber rapidement sur 3.

III.

À toute lettre de l'alphabet on associe un entier naturel x compris entre 0 et 25 comme indiqué dans le tableau ci-dessous :

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|----|----|----|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Le « chiffre de Rabin » est un dispositif de cryptage asymétrique inventé en 1979 par l'informaticien Michael Rabin.

Alice veut communiquer de manière sécurisée en utilisant ce cryptosystème. Elle choisit deux nombres premiers distincts p et q . Le couple $(p; q)$ est sa clé privée qu'elle garde secrète.

Elle calcule ensuite $n = p \times q$ et elle choisit un nombre entier naturel B tel que $0 \leq B \leq n - 1$.

Si Bob veut envoyer un message secret à Alice, il le code lettre par lettre.

Le codage d'une lettre représentée par l'entier x est le nombre y tel que y soit le reste de la division euclidienne de $x(x+B)$ par n .

Dans l'exercice, on prend $p=3$ et $q=11$ donc $n=p \times q=33$ et $B=13$.
Coder le mot « ET » puis décoder la lettre A.

CO (une seule réponse)

J, L, U

On cherche donc le(s) entier(s) naturel(s) x tel(s) que $0 \leq x \leq 25$ et le reste de la division euclidienne de $x(x+13)$ par 33 soit égal à 0.

Le mieux est d'utiliser la calculatrice. On tape $Y1 = \text{reste}(X(X+13), 33)$.

On obtient la table.

On cherche dans la table les valeurs qui donnent 0.

On obtient : 9, 11, 20.

Les lettres correspondantes sont donc les lettres J, L, U.

Le « chiffre de Rabin » est-il utilisable pour décoder un message lettre par lettre ?

Une lettre peut être décodée par plusieurs lettres donc le chiffre de Rabin n'est pas utilisable pour décoder un message lettre par lettre.

IV.

À l'aide de la calculatrice, déterminer tous les entiers naturels x inférieurs ou égaux à 29 tels que le reste de la division euclidienne de x^2 par 30 soit égal à 16.

4, 14, 16, 26 (écrire les valeurs en les séparant par des virgules)

Le mieux est d'utiliser la calculatrice. On tape $Y1 = \text{reste}(X^2, 30)$.

On obtient la table.

On cherche dans la table les valeurs qui donnent 16.

V.

On considère la fonction f définie sur \mathbb{Z} par $f(n) = \frac{n}{3}$ si n est divisible par 3 et $f(n) = 3-n$ si n n'est pas divisible par 3.

• Déterminer le(s) antécédent(s) de -2 par f ?

5 et -6

On cherche les entiers relatifs n tels que $f(n) = -2$.

On raisonne par disjonction de cas.

1^{er} cas : n est divisible par 3

$$(1) \Leftrightarrow \frac{n}{3} = -2$$

$$\Leftrightarrow n = -6 \text{ qui convient}$$

2^e cas : n n'est pas divisible par 3

$$(1) \Leftrightarrow 3-n = -2$$

$$\Leftrightarrow n = 5 \text{ qui convient}$$

• L'affirmation « Tout entier relatif admet deux antécédents par f » est-elle vraie ou fausse ? Justifier.

En résolvant l'équation $f(n) = 0$ avec $n \in \mathbb{Z}$, on observe que 0 admet un seul antécédent, à savoir lui-même. L'affirmation est donc fausse.

• On considère la fonction écrite ci-dessous en langage naturel dans le cadre de gauche dont le script correspondant en langage Python est donné dans le cadre de droite. Compléter le cadre de gauche.

| | |
|---|--|
| <p>Fonction $f(x)$</p> <p>Si x est divisible par 3</p> <p> Alors y prend la valeur $\frac{x}{3}$</p> <p>Sinon y prend la valeur $3-x$</p> <p>FinSi</p> <p>Renvoyer y</p> | <pre>def f(x): if n%3 == 0 : y = x / 3 else : y = 3 - x return y</pre> |
|---|--|

VI.

On considère un entier relatif a tel que le reste de la division euclidienne de a par 20 soit égal à 13.

On note q le quotient de la division euclidienne. On a donc $a = 20q + 13$ (1).

Les questions sont indépendantes les unes des autres.

1°) Quelle est la parité de a ?

a est impair (somme d'un nombre pair et d'un nombre impair)

2°) Le but de cette question est de déterminer le quotient et le reste de la division euclidienne de a par 10.

On reprend l'égalité (1) en effectuant les transformations successives suivantes : $a = 10 \times 2q + 13$;

$$a = 10 \times 2q + 10 + 3 ; a = 10 \times (2q + 1) + 3.$$

Expliquer pourquoi la dernière égalité correspond à la division euclidienne de a par 10.

$2q + 1 \in \mathbb{Z}$ puisque $q \in \mathbb{Z}$.

De plus, $0 \leq 3 < 10$.

Dans la division euclidienne de a par 10, le quotient est égal à $2q+1$ et le reste est égal à 3.

3°) Le but de cette question est de déterminer le quotient et le reste de la division euclidienne de $a+5$ par 20.

On reprend l'égalité (1). En ajoutant 5 à chaque membre, on obtient : $a+5 = 20q+18$.

Expliquer pourquoi la dernière égalité correspond à la division euclidienne de $a+5$ par 20.

$$q \in \mathbb{Z} \text{ et } 0 \leq 18 < 20.$$

Dans la division euclidienne de $a+5$ par 20, le quotient est égal à q et le reste est égal à 18.

4°) En reprenant la même méthode qu'à la question précédente, déterminer le reste et le quotient de la division euclidienne de $a+7$, $a+8$ et $-a$ par 20. On effectuera le travail de recherche au brouillon.

- Dans la division euclidienne de $a+7$ par 20, le quotient est égal à $q+1$ et le reste est égal à 0.
- Dans la division euclidienne de $a+8$ par 20, le quotient est égal à $q+1$ et le reste est égal à 1.
- Dans la division euclidienne de $-a$ par 20, le quotient est égal à $-(q+1)$ et le reste est égal à 7.

$$a+7 = 20(q+1)+0$$

$$a+8 = 20q+21$$

$$= 20(q+1)+1$$

$$-a = -20q-13$$

$$= -20q+7-20$$

$$= -20 \times (q+1)+7$$