

PARTIEL DU 08/11/2021 (2H)

Ordinateurs et téléphones portables interdits.

Calculatrice autorisée. Feuille recto-verso A4 manuscrite autorisée.

Toutes les réponses doivent être justifiées. La qualité de la rédaction sera prise en compte.

Exercice n° 1. (5 pts) On code des entiers en base 27 à l'aide de l'alphabet et du caractère "espace", selon la correspondance suivante : $_ = 0$, $A = 1$, $B = 2$, ..., $Z = 26$. Par exemple, le code Q correspond à 17 en base 10, et le code AE correspond à $1 \times 27 + 5 = 32$ en base 10.

1. Dans quel intervalle se situe un entier dont le code en base 27 comprend exactement cinq caractères ?
2. Ecrire en base 10 l'entier dont le code en base 27 est BRAVO.
3. Coder en base 27 l'entier s'écrivant 10695 en base 10.
4. Comment pourrait-on facilement passer de la base 27 à la base 3 et inversement ? (On ne demande pas de l'appliquer sur les exemples précédents.)
5. Donner un critère de divisibilité par 9 pouvant se lire facilement sur l'écriture d'un entier en base 27.

Exercice n° 2. (5 pts)

1. Résoudre dans \mathbb{Z} le système de congruences suivant :

$$(S) \quad \begin{cases} x \equiv 1986 & [76] \\ x \equiv 1998 & [33] \end{cases}$$

2. La comète de Halley est observable tous les 76 ans, et a été observée pour la dernière fois en 1986. La comète de Tempel-Tuttle est observable tous les 33 ans, et a été observée pour la dernière fois en 1998.
 - a) Quel est le rapport entre ces deux comètes et le système (S) ?
 - b) Quelle est la prochaine année où ces deux comètes seront observables en même temps ?
 - c) La comète de Grigg-Skjellerup est observable tous les 5 ans. Quel est l'écart minimal entre deux années où nos trois comètes sont observables en même temps ?

Exercice n° 3. (5 pts) On se propose de calculer le reste dans la division euclidienne de 2021^{1321} par 21, de deux manières différentes. (Attention, les deux méthodes sont demandées !)

1. Méthode 1 : effectuer le calcul par exponentiation rapide.
2. Méthode 2.
 - a) Calculer $\varphi(21)$.
 - b) Sans calcul de puissances, que vaut $\overline{2021}^{\varphi(21)}$ dans $\mathbb{Z}/21\mathbb{Z}$?
 - c) Conclusion.

Exercice n° 4. (3 pts)

1. Donner la liste des éléments inversibles de $\mathbb{Z}/18\mathbb{Z}$.
2. Calculer l'inverse de $\bar{5}$ dans $\mathbb{Z}/18\mathbb{Z}$.
3. Résoudre l'équation $\bar{5}\bar{x} = \bar{3}$ dans $\mathbb{Z}/18\mathbb{Z}$.

Exercice n° 5. (2 pts) Soient a et b des entiers.

1. Montrer que si un nombre premier p divise ab et $a + b$ alors il divise a et b (on rappelle le lemme d'Euclide : si un nombre premier divise un produit d'entiers alors il divise au moins l'un des facteurs).
2. En déduire que si a et b sont premiers entre eux alors ab et $a + b$ sont premiers entre eux.

CORRIGÉ DU PARTIEL DU 08/11/2021

Le barème final est sur 24 points, avec une note gardée à l'identique sur 20.

Exercice n° 1. (5 points : 1+1+1+1+1)

1. D'une manière générale, les entiers dont l'écriture en base b comporte exactement k chiffres sont ceux de l'intervalle $[b^{k-1}, b^k - 1]$. La réponse est donc $[27^4, 27^5 - 1]$.
2. On a B=2, R=18, A=1, V=22, O=15. Par conséquent, l'entier dont le code en base 27 est BRAVO est $2 \times 27^4 + 18 \times 27^3 + 1 \times 27^2 + 22 \times 27 + 15 = 1418514$.
3. Le code est donné par les restes (lus de bas en haut) dans l'algorithme de conversion :

$$\begin{aligned} 10695 &= 27 \times 396 + 3 \\ 396 &= 27 \times 14 + 18 \\ 14 &= 27 \times 0 + 14 \end{aligned}$$
 Comme 3=C, 18=R et 14=N, on obtient le code NRC.
4. Comme $27 = 3^3$, on peut convertir "par blocs de trois". Passer de la base 27 à la base 3 se fait en remplaçant chaque caractère par un bloc de trois chiffres correspondant à son écriture en base 3. Passer de la base 3 à la base 27 se fait en regroupant les chiffres par blocs de trois (partant de la droite) et en convertissant chaque bloc en un caractère en base 27.
5. Si $n = (a_k a_{k-1} \dots a_1 a_0)_{27}$, on a $n = a_k \times 27^k + a_{k-1} \times 27^{k-1} + \dots + a_1 \times 27 + a_0$. Tous les termes de cette somme sont multiples de 9 sauf peut-être a_0 , ainsi $n \equiv a_0 [9]$. Par conséquent, n est divisible par 9 si et seulement si a_0 est divisible par 9. On en conclut que n est divisible par 9 si et seulement si le dernier caractère est ◡ (=0), I (=9) ou R (=18).

Exercice n° 2. (6 points : 3+1+1+1)

1. Comme 33 et 76 sont premiers entre eux et $33 \times 76 = 2508$, le théorème des restes chinois assure que l'ensemble des solutions de (S) est $\{x_0 + 2508k, k \in \mathbb{Z}\}$ où x_0 est n'importe quelle solution particulière de (S). Celle-ci est de la forme $x_0 = 1986 + 76\alpha = 1998 + 33\beta$ ce qui donne $76\alpha - 33\beta = 12$. Un tel couple (α, β) s'obtient grâce à l'algorithme d'Euclide étendu :

$$\begin{array}{l} L_1 \\ L_2 \\ L_3 = L_1 - 2 \times L_2 \\ L_4 = L_2 - 3 \times L_3 \\ L_5 = L_3 - 3 \times L_4 \\ L_6 = L_4 - 3 \times L_5 \end{array} \begin{array}{l} \left[\begin{array}{ccc} 76 & 1 & 0 \\ 33 & 0 & 1 \\ 10 & 1 & -2 \\ 3 & -3 & 7 \\ 1 & 10 & -23 \\ 0 & -33 & 76 \end{array} \right] \end{array} \quad \begin{array}{l} 76 = 33 \times 2 + 10 \\ 33 = 10 \times 3 + 3 \\ 10 = 3 \times 3 + 1 \\ 3 = 1 \times 3 + 0 \end{array}$$

L'avant-dernière ligne de la matrice donne la relation de Bézout $1 = 76 \times 10 + 33 \times (-23)$. En multipliant par 12, on obtient $76 \times 120 - 33 \times 276 = 12$, donc le couple $(\alpha, \beta) = (120, 276)$ convient, ce qui donne la solution particulière $x_0 = 1986 + 76 \times 120 = 1998 + 33 \times 276 = 11106$. En conclusion, l'ensemble des solutions de (S) est $\{11106 + 2508k, k \in \mathbb{Z}\}$.

2. a) Les solutions de la première (resp. deuxième) congruence sont les années en lesquelles on peut observer la comète de Halley (resp. de Tempel-Tuttle). Par conséquent les solutions du système sont précisément les années en lesquelles on peut observer ces deux comètes en même temps.
- b) La prochaine année en laquelle on pourra observer ces deux comètes en même temps est donc la plus petite solution de (S) supérieure à 2021. Comme $11106 + 2508k > 2021$ si et seulement si $k \geq -3$, celle-ci s'obtient en prenant $k = -3$: il s'agit de l'année 3582.
- c) Les années en lesquelles on peut observer les trois comètes en même temps sont les solutions du système suivant :

$$\begin{cases} x \equiv 1986 & [76] \\ x \equiv 1998 & [33] \\ x \equiv a & [5] \end{cases},$$

où a est n'importe quelle année où on a pu observer la comète de Grigg-Skjellerup. Comme 33, 76 et 5 sont deux-à-deux premiers entre eux et $33 \times 76 \times 5 = 12540$, le

théorème chinois (appliqué deux fois d'affilée) assure que l'ensemble des solutions de ce système est de la forme $\{y_0 + 12540k, k \in \mathbb{Z}\}$, ce qui signifie que les trois comètes sont observables en même temps tous les 12540 ans.

Exercice n° 3. (6 points : 3+1+1+1)

1. On commence par convertir 1321 en base 2 :

$$\begin{aligned} 1321 &= 2 \times 660 + 1 \\ 660 &= 2 \times 330 + 0 \\ 330 &= 2 \times 165 + 0 \\ 165 &= 2 \times 82 + 1 \\ 82 &= 2 \times 41 + 0 \\ 41 &= 2 \times 20 + 1 \\ 20 &= 2 \times 10 + 0 \\ 10 &= 2 \times 5 + 0 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \\ 1 &= 2 \times 0 + 1 \end{aligned}$$

En lisant les restes de bas en haut, on obtient $1321 = (10100101001)_2$, ce qui signifie que $1321 = 2^{10} + 2^8 + 2^5 + 2^3 + 2^0 = 1024 + 256 + 32 + 8 + 1$. D'autre part, on calcule dans $\mathbb{Z}/21\mathbb{Z}$:

$$\begin{aligned} \overline{2021} &= \overline{5} \\ \overline{2021}^2 &= \overline{25} = \overline{4} \\ \overline{2021}^4 &= \overline{16} \\ \overline{2021}^8 &= \overline{256} = \overline{4} \\ \overline{2021}^{16} &= \overline{16} \\ \overline{2021}^{32} &= \overline{4} \\ \overline{2021}^{64} &= \overline{16} \\ \overline{2021}^{128} &= \overline{4} \\ \overline{2021}^{256} &= \overline{16} \\ \overline{2021}^{512} &= \overline{4} \\ \overline{2021}^{1024} &= \overline{16} \end{aligned}$$

Ainsi $\overline{2021}^{1321} = \overline{2021}^{1024} \times \overline{2021}^{256} \times \overline{2021}^{32} \times \overline{2021}^8 \times \overline{2021} = \overline{16} \times \overline{16} \times \overline{4} \times \overline{4} \times \overline{5} = \overline{5}$, donc le reste dans la division euclidienne de 2021^{1321} par 21 est 5.

2. a) Comme $21 = 3 \times 7$ où 3 et 7 sont premiers entre eux, on a $\varphi(21) = \varphi(3)\varphi(7)$. On sait que $\varphi(p) = p - 1$ pour tout nombre premier p donc on peut conclure que $\varphi(21) = 2 \times 6 = 12$.
- b) On peut commencer par la simplification $\overline{2021} = \overline{5}$ dans $\mathbb{Z}/21\mathbb{Z}$. Comme 5 est premier avec 21, $\overline{5}$ est inversible dans $\mathbb{Z}/21\mathbb{Z}$ d'après le critère d'inversibilité du cours. Le théorème de Lagrange assure alors que $\overline{2021}^{\varphi(21)} = \overline{5}^{\varphi(21)} = \overline{1}$.
- c) D'après les deux questions précédentes, on a $\overline{5}^{12} = \overline{1}$. Pour conclure, il suffit d'écrire $\overline{2021}^{1321} = \overline{5}^{1321} = \overline{5}^{12 \times 110 + 1} = (\overline{5}^{12})^{110} \times \overline{5} = \overline{1} \times \overline{5} = \overline{5}$.

Exercice n° 4. (4 points : 1+2+1)

1. D'après le critère d'inversibilité du cours, les éléments inversibles de $\mathbb{Z}/18\mathbb{Z}$ sont les classes des entiers premiers avec 18. Les entiers entre 0 et 17 qui sont premiers avec 18 sont : 1, 5, 7, 11, 13, 17. Ainsi $(\mathbb{Z}/18\mathbb{Z})^* = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}, \overline{13}, \overline{17}\}$.
2. La méthode générale pour calculer l'inverse de $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$ est d'établir une relation de Bézout entre a et n :

$$\begin{array}{l} L_1 \\ L_2 \\ L_3 = L_1 - 3 \times L_2 \\ L_4 = L_2 - 1 \times L_3 \\ L_5 = L_3 - 1 \times L_4 \\ L_6 = L_4 - 2 \times L_5 \end{array} \begin{array}{l} \left[\begin{array}{ccc} 18 & 1 & 0 \\ 5 & 0 & 1 \\ 3 & 1 & -3 \\ 2 & -1 & 4 \\ 1 & 2 & -7 \\ 0 & -5 & 18 \end{array} \right] \end{array} \quad \begin{array}{l} \\ \\ 18 = 5 \times 3 + 3 \\ 5 = 3 \times 1 + 2 \\ 3 = 2 \times 1 + 1 \\ 2 = 1 \times 2 + 0 \end{array}$$

L'avant-dernière ligne de la matrice donne la relation de Bézout $1 = 18 \times 2 + 5 \times (-7)$ (remarque : on pouvait trouver cette identité de tête sans détailler l'algorithme). En passant cette égalité dans $\mathbb{Z}/18\mathbb{Z}$, on obtient $\overline{1} = \overline{5} \times (\overline{-7})$, donc $\overline{5}^{-1} = \overline{-7} = \overline{11}$.

3. On multiplie à gauche et à droite par l'inverse de $\bar{5}$ calculé dans la question précédente. On a $\bar{5}\bar{x} = \bar{3} \iff \bar{5}^{-1}\bar{5}\bar{x} = \bar{5}^{-1}\bar{3} \iff \bar{x} = \bar{5}^{-1}\bar{3} = \bar{11}\bar{3} = \bar{33} = \bar{15}$. Ainsi l'unique solution de cette équation est $\bar{x} = \bar{15}$.

Exercice n° 5. (3 points : 1,5+1,5)

1. Soit p un nombre premier divisant ab et $a + b$. Comme p divise ab , on sait d'après le lemme d'Euclide que p divise a ou b .
 - Si p divise a , puisque p divise aussi $a + b$, alors p divise la différence $(a + b) - a = b$.
 - Si p divise b , puisque p divise aussi $a + b$, alors p divise la différence $(a + b) - b = a$.Dans tous les cas, on voit que p divise à la fois a et b .
2. Il est équivalent de montrer la contraposée, c'est-à-dire que si ab et $a + b$ ne sont pas premiers entre eux alors a et b ne sont pas premiers entre eux. Supposons donc que ab et $a + b$ ne sont pas premiers entre eux, alors il existe un nombre premier p qui divise à la fois ab et $a + b$. D'après la question 1, p divise a et b , donc a et b ne sont pas premiers entre eux.