Cette épreuve est constituée de deux problèmes indépendants.

Problème n° 1

Notations.
$\mathbb{N}$ désigne l'ensemble des entiers naturels.
Pour m et n deux entiers naturels, $[\![m, n]\!]$ désigne l'ensemble des entiers naturels k tels que $m \leqslant k \leqslant n$.

On souhaite crypter des messages, lettre à lettre. Pour écrire ces messages, on utilise 29 caractères différents : les 26 lettres de l'alphabet et les trois symboles espace, virgule et point. Pour faciliter le travail de cryptage, on code chacun de ces 29 caractères par un entier :

.	␣	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	13	14

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	,
15	16	17	18	19	20	21	22	23	24	25	26	27	28

On note R l'ensemble des entiers utilisés dans ce cryptage, c'est-à-dire l'ensemble $[\![0, 28]\!]$. Pour tout entier naturel k non nul, on note f_k l'application de R dans R qui à tout x de R associe le reste de la division euclidienne de x^k par 29.

Ces fonctions f_k, appelées *fonctions de cryptage*, sont utilisées pour crypter des messages.

Partie A : premiers essais

Albert souhaite utiliser comme fonction de cryptage l'application f_3. Benoît propose d'utiliser f_7. Camille choisit d'utiliser f_{19}.

I. Que devient la lettre E par la méthode de cryptage d'Albert ?

$6^3 = 216 = 7 \times 29 + 13$. Donc E devient L.

II. Montrer que, quelle que soit la fonction de cryptage f_k choisie, les symboles espace et point sont inchangés.

Le symbole point correspond à 0 et le symbole point à 1. Pour tout $k \geqslant 1$, comme $0^k = 0$ et $1^k = 1$, $f_k(0) = 0$ et $f_k(1) = 1$, donc les symboles points et espaces sont inchangés.

III. Un élève de troisième propose d'utiliser un tableur pour calculer les valeurs de f_k. Il prépare la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD	AE
1		.	␣	A	B	...	Z	,	
2	x	0	1	2	3	...	27	28	Exposant k
3	$f_k(x)$	0	1						3

Dans la cellule D3, il entre la formule =MOD(D2^AE3 ;29). Comment modifier cette formule afin de pouvoir la dupliquer en utilisant la poignée de recopie, sachant que le tableau doit rester correct lorsque le contenu de la cellule AE3 est modifié ?
On rappelle que MOD(a ;b) renvoie le reste de la division euclidienne de a par b.

Il doit entrer en D3 la formule =MOD(D21^AE3 ;29).

IV. Benoît utilise la feuille de calcul précédente pour son cryptage avec f_7. Il obtient le tableau suivant :

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f_k(x)$	0	1	12	12	28	28	28	1	17	28	17	12	17	28	12

x	15	16	17	18	19	20	21	22	23	24	25	26	27	28
$f_k(x)$	17	1	12	17	12	1	12	28	1	1	1	17	17	28

Crypter les mots CLE et LUC. Que constate t-on ?

CLE correspond à 4–13–6 donc est crypté par 28–28–28, soit « , , , ». LUC correspond à 13–22–4 donc est crypté par 28–28–28, soit « , , , ». Ces deux mots distincts sont cryptés de la même façon.

V. Quelle propriété doit vérifier la fonction f_k pour assurer le décryptage ?

Pour pouvoir décrypter les messages, il est nécessaire que deux lettres distinctes soient envoyées sur deux lettres distinctes, pour éviter ce qu'il se passe à la question IV. Autrement dit, la fonction f_k doit être injective. Comme f_k va d'un ensemble fini dans lui-même, l'injectivité de f_k est équivalente à sa bijectivité.

VI. Camille utilise la feuille de calcul de la question **III.** avec $k = 19$. Dans les cellules allant de E3 à AD3, il s'affiche ♯NOMBRE !. Comment expliquer ce résultat ? On verra dans la partie C comment contourner ce problème.

Pour calculer $f_k(3)$, le tableur calcule d'abord 3^{19} à l'aide de nombres flottants. La représentation de ce nombre en mémoire n'est plus exacte, ce nombre étant trop élevé. En conséquence, le tableur n'est pas capable de calculer son reste modulo 29.

Partie B : choix de la fonction de cryptage

On se propose dans cette partie de déterminer les valeurs de k pour lesquelles la fonction de cryptage f_k permet d'assurer le décryptage.

VII. On fixe un nombre premier p. Soit a un entier (relatif) tel que p ne divise pas a. Le but de cette question est de **démontrer** l'égalité suivante, connue sous le nom de petit théorème de Fermat :

$$a^{p-1} \equiv 1[p].$$

On désigne par A l'ensemble $\{a, 2a, 3a, \ldots, (p-1)a\}$.

1. Soit k un entier relatif. Montrer que p divise ka si, et seulement si, p divise k. En déduire que p ne divise aucun élément de A.

Supposons que p divise ka. Par le lemme de Gauss, p divise k ou p divise a. Comme p ne divise pas a, p divise k.

Supposons que p divise k. Comme k divise ka, par transitivité p divise ka.

Par contraposée, comme p ne divise pas k si $k \in [\![1, p-1]\!]$, p ne divise pas ka. Donc p ne divise aucun élément de A.

2. Pour $i \in [\![1, p-1]\!]$, on note α_i le reste modulo p de l'entier ia.

a. Établir que ces restes sont tous non nuls et deux à deux distincts.

Soient $i, j \in [\![1, p-1]\!]$ tels que $\alpha_i = \alpha_j$. Comme p divise $ia - \alpha_i$ et $ja - \alpha_j$, p divise $ja - \alpha_j - (ia - \alpha_i) = ja - ia = (j-i)a$. D'après la question VII.1, p divise $j-i$. De plus, $-(p-2) \leqslant j-i \leqslant p-2$, donc $j-i = 0$ et $j = i$. Les restes α_i sont donc deux-à-deux distincts. De plus, pout tout $i \in [\![1, p-1]\!]$, $\alpha_i \neq 0$ car p ne divise pas ia d'après la question VII. 1.

b. En déduire que $\{\alpha_i, i \in [\![1, p-1]\!]\} = [\![1, p-1]\!]$.

On a donc une application $f : [\![1, p-1]\!] \longrightarrow [\![1, p-1]\!]$ envoyant i sur α_i. Elle est injective d'après la question VII.2.a, donc bijective. Par suite, $\{\alpha_i, i \in [\![1, p-1]\!]\} = [\![1, p-1]\!]$.

3. On appelle P le produit de tous les éléments de A. Établir que $P = a^{p-1}(p-1)!$ et que $P \equiv (p-1)![p]$.

D'une part :

$$P = \prod_{i=1}^{p-1} ai = a^{p-1}(p-1)!.$$

D'autre part, pour tout i, ia est congru à α_i modulo p donc :

$$P \equiv \prod_{i=1}^{p-1} \alpha_i [p].$$

D'après la question VII.3.b. :

$$P \equiv \prod_{i=1}^{p-1} i \equiv (p-1)![p].$$

4. En déduire que pour tout entier relatif a premier avec p , $a^{p-1} \equiv 1[p]$.

On en déduit que p divise $a^{p-1}(p-1)! - (p-1)! = (a^{p-1}-1)(p-1)!$. Par le lemme de Gauss, p divise l'un des facteurs de ce produit. Aucun des facteurs $1, \ldots, p-1$ de $(p-1)!$ n'est divisible par p, donc $a^{p-1}-1$ est divisible par p. Par suite, $a^{p-1} \equiv 1[p]$.

5. Que peut-on en déduire pour f_{28} et f_{29} ?

Soit $i \in R$. Si $i = 0$ alors $f_{28}(i) = f_{29}(i) = 0$ d'après la question II. Sinon, p ne divise pas a. D'après la question VII. 4, comme 29 est un nombre premier, $a^{28} \equiv 1[29]$ et donc $a^{29} = a^{28} \times a \equiv a[p]$. Autrement dit, $f_{28}(a) = 1$ et $f_{29}(a) = a$. Par suite, $f_{29} = Id_R$ et pour tout $a \in R$:

$$f_{28}(a) = \begin{cases} 0 \text{ si } a = 0, \\ 1 \text{ sinon.} \end{cases}$$

6. Soit k et l deux entiers naturels non nuls. Montrer que si $k \equiv l[28]$, alors $f_k = f_l$.

quitte à permuter k et l, on peut supposer $l \geqslant k$. Alors $l = 28q + l$, avec $q \in \mathbb{N}$. Soit $i \in R$. Si $i = 0$, d'après la question II, $f_k(i) = f_l(i) = 0$. Sinon :

$$f_l(i) \equiv i^{28q+k} \equiv (i^{28})^q i^k \equiv 1^q i^k \equiv i^k \equiv f_k(i)[29],$$

donc $f_l(i) = f_k(i)$. En conséquence, $f_k = f_l$.

VIII. Dans cette question x désigne un entier naturel premier avec 29 .

1. Montrer qu'il existe un plus petit entier naturel non nul k tel que $x^k \equiv 1[29]$, et que cet entier k est inférieur ou égal à 28. Cet entier k est appelé *ordre de* x et est noté $o(x)$.

Soit $E = \{k \in \mathbb{N}^*, x^k \equiv 1[29]\}$. D'après VII.4, cet ensemble est non vide car il contient 28. Par suite, il contient un plus petit élément k, qui est donc inférieur ou égal à 28.

Définition. Soit x un entier premier avec 29.
On dit que x est primitif modulo 29 si $o(x) = 28$.

2. Soit k un entier naturel. Montrer que $x^k \equiv 1[29]$ si et seulement si $o(x)$ divise k.

Supposons que $o(x)$ divise k. Posons $k = o(x)q$, avec $q \in \mathbb{N}^*$. Alors :

$$x^k = (x^{o(x)})^q \equiv 1^q \equiv 1[29].$$

Supposons que $x^k \equiv 1[29]$. Soit $k = o(x)q + r$ la division euclidienne de k par $o(x)$, avec $0 \leqslant r \leqslant o(x)$ et $q \in \mathbb{N}$. Alors :

$$x^k = (x^{o(x)})^q x^r \equiv 1^q x^r \equiv x^r \equiv 1[29].$$

Si $r \neq 0$, ceci contredit la minimalité de $o(x)$. Donc $r = 0$ et $o(x)$ divise k.

3. En déduire que $o(x)$ est un diviseur de 28.

Comme $x^{28} \equiv 1[29]$, $o(x)$ divise 28.

4. Écrire un algorithme permettant de calculer l'ordre d'un nombre entier x premier avec 29.

```
o ← 1
N ← x mod 29
Tant que (N ≠ 1) faire
    | N ← N × x mod 29
    | o ← o + 1
Fin Tant que
Rendre o
```

5. a. Déterminer l'ensemble des diviseurs de 28.

La décomposition en nombres premiers de 28 est $28 = 2^2 \times 7$. Ses diviseurs sont donc les nombres de la forme $2^a \times 7^b$, avec $0 \leqslant a \leqslant 2$ et $0 \leqslant b \leqslant 1$. Il s'agit donc de 1, 2, 4, 7, 14, 28.

b. Montrer que si $x^{14} \equiv 1[29]$ ou $x^4 \equiv 1[29]$, alors l'ordre $o(x)$ ne peut pas valoir 28.

Si $x^{14} \equiv 1[29]$ ou $x^4 \equiv 1[29]$, d'après VIII.2, $o(x)$ divise 14 ou $o(x)$ divise 4, donc $o(x) \neq 28$.

c. Montrer que si $x^{14} \not\equiv 1[29]$ et $x^4 \not\equiv 1[29]$, alors $o(x) = 28$.

Comme $o(x)$ divise 28, $o(x) \in \{1, 2, 4, 7, 14, 28\}$. Supposons $x^{14} \not\equiv 1[29]$ et $x^4 \not\equiv 1[29]$. D'après VIII.2, $o(x)$ ne divise pas 14, donc est différent de 1, 2, 7 et 14. Par suite, $o(x) \in \{4, 28\}$. D'après VIII.2, $o(x)$ ne divise par 4, donc $o(x) = 28$.

d. En déduire que 2 est primitif modulo 29.

Par multiplication successives par 2 :

$$2^4 = 16 \equiv 16[29], \qquad 2^5 \equiv 32 \equiv 3[29],$$
$$2^6 \equiv 6[29], \qquad 2^7 \equiv 12[29].$$

En élevant au carré, $2^{14} \equiv 144 \equiv 28[29]$. D'après la question VIII.5.c, $o(2) = 28$.

IX. On rappelle que si p est un nombre premier, l'ensemble $\{\overline{x} \in \mathbb{Z}/p\mathbb{Z} \mid \overline{x} \neq \overline{0}\}$ muni de la loi $\overline{\times}$ induite par la multiplication de $\mathbb{Z}$ est un groupe. En utilisant les résultats de la question **VIII.**, vérifier que, pour $p = 29$, ce groupe est cyclique et donner un générateur de ce groupe.

Considérons $E = \{\overline{2}^k, k \in [\![1, 28]\!]\} \subseteq \{\overline{x} \in \mathbb{Z}/29\mathbb{Z} \mid \overline{x} \neq \overline{0}\}$. Soient $k, l \in [\![1, 28]\!]$ tels que $\overline{2}^k = \overline{2}^l$. Supposons par exemple $l \geqslant l$. Alors $\overline{2}^{l-k} = \overline{1}$, donc $o(2) = 28$ divise $l - k$. Comme $0 \leqslant l - k \leqslant 27$, $l - k = 0$ et $l = k$. Par suite, E comprend 28 éléments, donc est égal à $\{\overline{x} \in \mathbb{Z}/29\mathbb{Z} \mid \overline{x} \neq \overline{0}\}$. Ce groupe est donc cyclique, engendré par $\overline{2}$.

X. On considère l'application φ définie sur $S = [\![1, 28]\!]$ et à valeurs dans S qui à tout entier $k \in S$ associe $\varphi(k) = \beta_k$, où β_k désigne le reste de la division euclidienne de 2^k par 29.

1. Justifier que φ est bien définie.

Pour tout $k \in \mathbb{N}$, 29 ne divise pas 2^k, car 29 ne divise pas 2. Par suite, pour tout $k \in S$, $\beta_k \neq 0$ et donc $\beta_k \in S$.

2. Soient $k \leqslant k'$ deux éléments de S. Établir que $\varphi(k) = \varphi(k')$ si et seulement si 29 divise $2^{k'-k} - 1$.

$$\begin{aligned}\varphi(k) = \varphi(k') &\iff 2^k \equiv 2^{k'}[29] \\ &\iff (2^{k'-k} - 1)2^k \equiv 0[29] \\ &\iff 29 \mid (2^{k'-k} - 1)2^k.\end{aligned}$$

Comme 29 ne divise pas 2, par le lemme de Gauss :

$$\varphi(k) = \varphi(k') \Longleftrightarrow 29 \mid 2^{k'-k} - 1.$$

3. En déduire que φ est injective, puis que φ est bijective.

Soient k, k' deux éléments de S. On suppose par exemple que $k' \geqslant k$.

$$\begin{aligned}\varphi(k) = \varphi(k') &\Longleftrightarrow 29 \mid 2^{k'-k} - 1\\ &\Longleftrightarrow 2^{k'-k} \equiv 1[29]\\ &\Longleftrightarrow o(2) = 28 \mid k' - k\\ &\Longleftarrow k' = k,\end{aligned}$$

car $0 \leqslant k' - k \leqslant 27$. Par suite, φ est injective. Comme S est de cardinal fini, φ est bijective.

4. En déduire que, pour tout élément de $y \in S$, il existe un unique $x \in S$ tel que $y \equiv 2^x[29]$.

Soit $y \in S$. Comme φ est bijective, il existe un unique $x \in S$ tel que $\varphi(x) = y$, c'est-à-dire qu'il existe un unique $x \in S$ tel que $2^x \equiv y[29]$.

XI. Soit k un entier naturel non nul fixé. Étant donné $y \in S$, on cherche à trouver $z \in R$ tel que $z^k \equiv y[29]$.

1. Établir que 29 ne peut diviser z et que l'on peut se ramener à chercher z dans S.

Si 29 divise z, alors $z^k \equiv 0[29]$ et donc $z^k \neq y[29]$, car $y \in S$. Donc 29 ne divise pas z. Par suite, si $z \in R$ vérifie $z^k \equiv y[29]$, $z \neq 0$ et donc $z \in S$: on peut se ramener à chercher z dans S.

2. Soit z un élément de S et t (respectivement x) l'unique élément de S tel que $z \equiv 2^t\,[29]$ (respectivement $y \equiv 2^x\,[29]$). Démontrer que $z^k \equiv y\,[29]$ si et seulement si $kt - x$ est divisible par 28.

D'après X.2 :

$$z^k \equiv y[29] \Longleftrightarrow 2^{tk} \equiv 2^x[29] \Longleftrightarrow 28 \mid tk - x.$$

3. On considère l'équation diophantienne $(*)$ $ak + 28b = 1$, où les inconnues a et b sont des entiers relatifs.

a. Donner une condition nécessaire et suffisante (C) pour que $(*)$ admette des solutions.

$(*)$ admet des solutions si, et seulement si, a et 28 sont premiers entre eux.

b. On suppose cette condition (C) satisfaite. À partir d'une solution particulière (a_0, b_0), donner alors toutes les solutions de $(*)$.

Let solutions de $(*)$ sont les couples $(a_0 + 28n, b_0 - bn)$, où $n \in \mathbb{Z}$.

c. On suppose cette condition (C) satisfaite. Établir que $(*)$ a une unique solution (a_1, b_1) pour laquelle $a_1 \in S$.

Soit $a_0 = 28q + a_1$ la division euclidienne de a_0 par 28. Alors $a_1 \in S$ et de plus $(a_1, b_0 + qk)$ est une solution de $(*)$, ce qui prouve l'existence d'une telle solution.
Soit (a_2, b_2) une solution de $(*)$ avec $a_2 \in S$. Alors il existe $n \in \mathbb{Z}$ tel que $a_2 = a_0 + 28n$ et $b_2 = b_0 - bn$. Donc $a_2 = a_1 + 28(q + n)$.
Comme $-27 \leqslant a_2 - a_1 \leqslant 27$, nécessairement $a_2 = a_1$ et donc $n - q$. Par suite, $(a_2, b_2) = (a_1, b_1)$, ce qui prouve l'unicité d'une telle solution.

4. En déduire que si k et 28 sont premiers entre eux alors $f_{a_1} \circ f_k(w) = f_k \circ f_{a_1}(w) = w$ pour tout $w \in R$.

Si $w = 0$, alors $f_{a_1} \circ f_k(w) = f_k \circ f_{a_1}(w) = 0 = w$ d'après la question II. Si $w \in S$, il existe un unique $x \in S$ tel que $w \equiv 2^x [29]$. Comme 28 divise $ka_1x - x$, d'après XI.2 :

$$f_{a_1} \circ f_k(w) \equiv 2^{a_1 kx} \equiv 2^x \equiv w [29],$$

donc $f_{a_1} \circ f_k(w) = w$. De même, $f_k \circ f_{a_1}(w) = w$.

5. Que conclure pour f_k ?

f_k est donc bijective, d'inverse f_{a_1}.

XII. Montrer que tout message crypté par la fonction f_3 peut être décrypté à l'aide de la fonction f_{19}.

Une solution particulière de $(*)$: $3a + 28b = 1$ est donnée par $(-9, 1)$. Les solutions de $(*)$ sont donc les couples $(-9 + 28n, 1 - 3n)$, où $n \in \mathbb{Z}$. L'unique solution (a_1, b_1) avec $a_1 \in S$ est donnée pour $n = 1$, ce qui donne $(19, -2)$ Donc $f_{19} \circ f_3(w) = w$ pour tout $w \in S$: f_{19} permet donc de décrypter les messages cryptés par f_3.

XIII. Quelles sont les valeurs de k permettant le décryptage de tout message ayant été crypté par f_k ? Justifier votre réponse.

Le décryptage des messages cryptés par f_k est possible si, et seulement si, 28 et k sont premiers entre eux.
$\Longleftarrow$. D'après XI.3, dans ce cas, f_k est bijective, d'inverse f_{a_1}.
$\Longrightarrow$. Si 28 et k ne sont pas premiers entre eux, $(*)$ n'a pas de solution. D'après la question XI.2, il n'existe donc aucun $z \in R$ tel que $f_k(z) = 2$ (pour $t = 1$). Donc f_k n'est pas surjective et donc pas bijective.

Partie C : différents procédés de calcul de f_{19}

On décrit dans cette partie trois méthodes pour calculer f_{19} à l'aide d'un tableur.

XIV. Première méthode. On souhaite compléter la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD
1		.		A	B	...	Z	,
2	x	0	1	2	3	...	27	28
3	$f_2(x)$	0	1					
4	$f_3(x)$	0	1					
⋮	⋮	⋮	⋮					
20	$f_{19}(x)$	0	1					

1. Quelle formule doit-on écrire en D3 pour remplir le tableau en utilisant la poignée de recopie ?

=MOD(D2*D$2 ;29)

2. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

On effectue 18 multiplications et 18 divisions euclidiennes par 29.

XV. Seconde méthode. On souhaite compléter la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD
1		.		A	B	...	Z	,
2	x	0	1	2	3	...	27	28
3	$f_2(x)$	0	1					
4	$(f_2 \circ f_2)(x)$	0	1					
5	$(f_2 \circ f_2 \circ f_2)(x)$	0	1					
6	$(f_2 \circ f_2 \circ f_2 \circ f_2)(x)$	0	1					
7								

1. Quelle formule doit-on écrire en D3 pour remplir le tableau en utilisant la poignée de recopie ?

=MOD(D2^ 2 ;29)

2. En constatant que $19 = 2^4 + 2^1 + 2^0$, montrer que pour tout $x \in R$,

$$f_{19}(x) \equiv (f_2 \circ f_2 \circ f_2 \circ f_2)(x) \times f_2(x) \times x \,[29].$$

$2^4 + 2^1 + 2^0 = 16 + 2 + 1 = 19$. Donc, si $x \in R$:

$$\begin{aligned} f_{19}(x) &\equiv x^{2^4+2+1} \equiv (((x^2)^2)^2)^2 x^2 x[29] \\ &= (f_2 \circ f_2 \circ f_2 \circ f_2)(x) \times f_2(x) \times x \,[29] \end{aligned}$$

3. Quelle formule doit-on écrire en D7 pour remplir la ligne 7 en utilisant la poignée de recopie et obtenir ainsi f_{19} ?

=MOD(D4*D4*D2 ;29)

4. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

On effectue $4 + 2 = 6$ multiplications et 5 divisions euclidiennes pas 29.

XVI. Troisième méthode. On souhaite compléter la feuille de calcul suivante :

	A	B	C	D	E	...	AC	AD
1		.		A	B	...	Z	,
2	x	0	1	2	3	...	27	28
3	$f_3(x)$	0	1					
4	$(f_3 \circ f_3)(x)$	0	1					
5								

1. Quelle formule doit-on écrire en D3 pour remplir le tableau en utilisant la poignée de recopie ?

=MOD(D2^ 3 ;29)

2. En constatant que $19 = 2 \times 3^2 + 3^0$, donner une formule permettant de calculer $f_{19}(x)$ à partir de la feuille de calcul précédente.

$2 \times 3^2 + 3^0 = 18 + 1 = 19$. Pour tout $x \in R$:

$$f_{19}(x) \equiv ((x^3)^3)^2 x \equiv f_3 \circ f_3(x)^2 \times x[29].$$

3. Quelle formule doit-on écrire en D5 pour remplir la ligne 5 en utilisant la poignée de recopie et obtenir ainsi f_{19} ?

=MOD(D4^ 2*D2 ;29)

4. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

On effectue $2 + 2 + 3 = 7$ multiplications et 3 divisions euclidiennes par 29.

XVII. Laquelle de ces trois méthodes vous semble la plus performante ?

La première méthode nécessite le plus d'opérations : c'est la moins performante des trois. Soit m le temps nécessaire pour une multiplication et d le temps nécessaire pour une division euclidienne par 29. Le temps mis pour calculer une colonne est $6m + 5d$ avec la deuxième méthode et $7m + 3d$ avec la troisième méthode.

$$6m + 5d \leqslant 7m + 3d \iff 2d \leqslant m.$$

Par suite, si $2d < m$, la deuxième méthode est la plus performante ; si $2d > m$, la troisième méthode est la plus performante ; si $2d = m$, ces deux méthodes sont aussi performantes l'une que l'autre.

Problème n° 2

Notations.
$\mathbb{N}$ désigne l'ensemble des entiers naturels.
$\mathbb{C}$ désigne l'ensemble des nombres complexes.
Pour m et n deux entiers naturels, $[\![m, n]\!]$ désigne l'ensemble des entiers k tels que $m \leqslant k \leqslant n$.

Si z est un nombre complexe, son conjugué est noté $\overline{z}$.

Partie A : constructions à la règle et au compas

On se place dans un plan euclidien $\mathcal{P}$ muni d'un repère orthonormé (O, I, J), qu'on identifie avec le plan complexe $\mathbb{C}$. On construit des points de $\mathcal{P}$ à l'aide d'une règle non graduée et d'un compas de la façon suivante :

— au départ, seuls O, I et J sont construits ;
— à chaque étape, on peut :

- construire le cercle de centre A et de rayon BC si A, B et C sont des points déjà construits ;
- construire la droite (AB) si A et B sont des points déjà construits.

On obtient ainsi de nouveaux points, intersections des cercles et des droites qui ont été construits. Ces points pourront être utilisés aux étapes suivantes. Les droites, cercles et points ainsi obtenus sont dits *constructibles à la règle et au compas*.

Soit x un nombre réel. On dit que x est un nombre *constructible* s'il est l'abscisse dans le repère (O, I, J) d'un point constructible.

I. Dans toutes les questions qui suivent, on attend à la fois la représentation d'une construction à la règle et au compas laissant apparaître les traits de construction et la rédaction d'un programme de construction tel qu'il figurerait comme trace écrite dans les cahiers des élèves.

1. On suppose que A et B sont deux points distincts constructibles à la règle et au compas. Montrer que la médiatrice de $[AB]$ et le milieu de $[AB]$ sont constructibles à la règle et au compas.

(La figure est laissée au lecteur). Soient $\mathcal{C}_1$ et $\mathcal{C}_2$ les cercles de centres respectifs A et B et de rayon AB. Comme A et B sont constructibles, $\mathcal{C}1$ et $\mathcal{C}_2$ sont des cercles constructibles, donc leurs deux points d'intersection I et J sont constructibles. De plus, $IA = IB = AB$ et $JA = JB = AB$, donc I et J sont sur la médiatrice $\mathcal{D}$ de $[AB]$. En conséquence, $\mathcal{D}$ est constructible. Le point d'intersection de $\mathcal{D}$ et de (AB) est donc lui aussi constructible : c'est le milieu de $[AB]$.

2. On suppose que A, B et C sont trois points constructibles à la règle et au compas, avec $A \neq B$. Montrer que la droite perpendiculaire à (AB) passant par C est constructible à la règle et au compas.

(La figure est laissée au lecteur). Soit $\mathcal{C}$ le cercle de centre C et de rayon AC. Comme A et C sont constructibles, $\mathcal{C}$ est constructible. Ce cercle coupe la droite (AB) en A. Deux cas se présentent :

— Si A est le seul point d'intersection de $\mathcal{C}$ et (AB), alors (AB) et $\mathcal{C}$ sont tangents en A. Par suite, (AC) est perpendiculaire à (AB). La perpendiculaire à (AB) passant par C est donc (AC), qui est constructible.
— Sinon, $\mathcal{C}$ coupe (AB) en un second point D. Alors $CA = CD$, donc C est sur la médiatrice à $[AD]$. En conséquence, la perpendiculaire à (AB) passant par C est la médiatrice de $[AD]$. D'après la question I.1, cette droite est constructible.

3. On suppose que A, B et C sont trois points constructibles à la règle et au compas, avec $A \neq B$. Montrer que la droite parallèle à (AB) passant par C est constructible à la règle et au compas.

(La figure est laissée au lecteur). D'après la question I.2, la perpendiculaire $\mathcal{D}$ à (AB) passant par C est constructible. On considère le cercle $\mathcal{C}$ de centre C et de rayon AB : ce cercle est constructible et coupe $\mathcal{D}$ en deux points constructibles D et E, de sorte que $\mathcal{D} = (DE)$. La droite recherchée est la perpendiculaire à (DE) passant par C : en effet, cette droite passe par C et est parallèle à (AB) car (DE) est perpendiculaire à (AB). D'après la question I.2, cette droite est constructible.

4. Soient $\mathcal{D}$ et $\mathcal{D}'$ deux droites constructibles à la règle et au compas, sécantes en un point A. Montrer que les bissectrices de ces deux droites sont constructibles à la règle et au compas.

(La figure est laissée au lecteur). Comme $\mathcal{D}$ est constructible, elle contient un point I constructible différent de A. Le cercle $\mathcal{C}$ de centre A et de rayon AI est constructible et coupe $\mathcal{D}$ en un autre point J et $\mathcal{D}'$ en deux point I' et J'. Par construction, I', J et J' sont constructibles. Le triangle AII' est isocèle en A, donc la bissectrice Γ issue de A est aussi la médiatrice du segment $[II']$: d'après la question I.1, Γ est constructible. On obtient ainsi l'une des bissectrices des droites $\mathcal{D}$ et $\mathcal{D}'$. On obtient la seconde en considérant le triangle AIJ'.

On pourra désormais utiliser ces constructions sans en préciser tous les détails.

II. Soit M un point constructible à la règle et au compas. On note $(x; y)$ ses coordonnées dans le repère (O, I, J). Montrer que x et y sont des nombres constructibles.

Par définition, x est un nombre constructible. La perpendiculaire à (OI) passant par M est constructible, donc le point d'intersection $N(x; 0)$ de cette droite avec (OI) est constructible. Le cercle $\mathcal{C}$ de centre O et de rayon $MN = |y|$ coupe la droite (OI) en les points de coordonnées $(-y; 0)$ et $(y; 0)$, qui sont donc constructibles. Par suite, y (ainsi que $-y$) est un nombre constructible.

III. Soit x un nombre réel constructible. Montrer que les points de coordonnées $(x; 0)$ et $(0; x)$ dans le repère (O, I, J) sont constructibles à la règle et au compas.

Par définition, O et I sont constructibles. La perpendiculaire à (OI) passant par M est donc elle aussi constructible et le point d'intersection N de cette droite avec (OI) est constructible : il s'agit du point de coordonnées $(x; 0)$, qui est donc constructible. En utilisant la perpendiculaire à (OJ) passant par M, on obtient de même que le point $P(0; y)$ est constructible. Le cercle $\mathcal{C}$ de centre O et de rayon OP est constructible et coupe la droite (OI) en les points de coordonnées $(-y; 0)$ et $(0; y)$, qui sont donc constructibles.

IV. Soient x et y deux nombres réels constructibles strictement positifs.

1. Montrer que $-x$ est un nombre réel constructible. La réponse à cette question doit être rédigée telle que vous la présenteriez à une classe de collège.

D'après la question III, le point $M(x;0)$ est constructible. Le cercle de centre O et de rayon OM est donc constructible. Il coupe la droite (OI) en M et en le point de coordonnées $(-x;0)$, qui est donc constructible. Par suite, $-x$ est un nombre constructible.

2. Montrer que $x+y$ et $x-y$ sont constructibles. La réponse à cette question doit être rédigée telle que vous la présenteriez à une classe de collège.

D'après III, les points $M(x;0)$ et $N(y;0)$ sont constructibles. Le cercle $\mathcal{C}$ de centre M et de rayon $ON = y$ est donc constructibles. Il coupe (OI) en les points de coordonnées $(x-y;0)$ et $(x+y;0)$, qui sont donc constructibles. Par suite, $x-y$ et $x+y$ sont des nombres constructibles.

3. En utilisant les points J, $A(x;0)$ et $B(0;y)$ et la droite parallèle à (AJ) passant par B, montrer que xy est constructible. La réponse à cette question doit être rédigée telle que vous la présenteriez à une classe de collège.

D'après la question III, A et B sont constructibles. D'après la question I.3, la parallèle à (AJ) passant par B est constructible. L'intersection de cette droite avec (OI) est un point constructible C, de coordonnées $(z;0)$. D'après le théorème de Thalès, comme (AJ) est parallèle à (BC), $\frac{x}{z} = \frac{1}{y}$, donc $z = xy$ et z est un nombre constructible.

4. Montrer que $\dfrac{x}{y}$ est constructible.

Soit $\mathcal{D}$ la parallèle à (AB) passant par J : cette droite est constructible d'après I.3. Son intersection avec (OI) est un point C constructible, de coordonnées $(z;0)$. D'après le théorème de Thalès, comme (JD) est parallèle à (AB), $\frac{z}{x} = \frac{1}{y}$, donc $z = \frac{x}{y}$ et z est constructible.

V. Montrer que si x et y sont des nombres réels constructibles, alors $x+y$, $x-y$, xy et, si y est non nul, $\dfrac{x}{y}$ sont des nombres constructibles.

Le résultat est évident si $x = 0$ ou $y = 0$. On suppose donc x et y non nuls. D'après la question IV.1, x, y, $-x$ et $-y$ sont constructibles, donc $|x|$ et $|y|$ sont constructibles. D'après la question IV, $|x|+|y|$, $|x|-|y|$, $|y|-|x|$, $-|x|-|y|$, $|x||y|$, $-|x||y|$, $\frac{|x|}{|y|}$ et $-\frac{|x|}{|y|}$ sont constructibles. Donc $x+y$, $x-y$, xy et $\frac{x}{y}$ sont constructibles.

VI. Soit x un nombre réel constructible strictement positif.

1. Montrer que le point $A(1+x;0)$ est constructible à la règle et au compas.

1 et x sont constructibles, donc $1+x$ aussi d'après la question VI.1. D'après la question III, A est constructible.

2. Montrer que le cercle $\mathcal{C}$ de diamètre $[OA]$ est constructible à la règle et au compas.

D'après $I.1$, le milieu de K de $[OA]$ est constructible. Alors $\mathcal{C}$ est le cercle de centre K et de rayon OK, donc est constructible.

3. Soit B le point d'intersection d'ordonnée positive de $\mathcal{C}$ et de la droite $\mathcal{D}$ perpendiculaire à (OI) passant par I. Montrer que B est constructible à la règle et au compas.

D'après a question I.2, $\mathcal{D}$ est constructible. Comme $\mathcal{C}$ est constructible, les points d'intersection de $\mathcal{C}$ et $\mathcal{D}$ sont constructibles. En particulier, B est constructible.

4. Soit $\theta = (\widehat{\overrightarrow{OI}, \overrightarrow{OB}})$. Exprimer $\tan(\theta)$ et $\tan\left(\frac{\pi}{2} - \theta\right)$ en fonction de BI et de x. En déduire BI.

$\tan(\theta) = \frac{IB}{OI} = IB$. Comme B est sur le cercle de diamètre OA, OAB est rectangle en B, donc $(\widehat{\overrightarrow{AB}, \overrightarrow{AI}}) = \frac{\pi}{2} - \theta$. On a donc :

$$\tan\left(\frac{\pi}{2} - \theta\right) = \frac{IB}{AI} = \frac{IB}{x}.$$

De plus :

$$\tan\left(\frac{\pi}{2} - \theta\right) = \frac{\sin\left(\frac{\pi}{2} - \theta\right)}{\cos\left(\frac{\pi}{2} - \theta\right)} = \frac{\cos(\theta)}{\sin(\theta)} = \frac{1}{\tan(\theta)}.$$

Donc :

$$BI = \tan(\theta) = \frac{x}{\tan(\theta)}.$$

On obtient $x = \tan(\theta)^2$, donc $BI = \tan(\theta) = \sqrt{x}$.

5. Montrer que $\sqrt{x}$ est un nombre constructible.

Comme $B(1; \sqrt{x})$ est constructible, $\sqrt{x}$ est un nombre constructible d'après II.

VII. Montrer que tous les nombres rationnels sont constructibles.

0 et 1 sont constructibles. Supposons n constructible, pour un certain $n \in \mathbb{N}$. D'après V., $n + 1$ est constructible. Par le principe de récurrence, tous les entiers naturels sont constructibles. D'après V, leurs opposés aussi, donc tous les entiers relatifs sont constructibles. Par suite, si $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$, non nul, d'après V., a/b est constructible. Donc les nombres rationnels sont constructibles.

VIII. Montrer que $\sqrt{2}$ et $\sqrt[4]{2}$ sont des nombres constructibles. Proposer une construction à la règle et au compas des points de coordonnées $(\sqrt{2}; 0)$ et $(\sqrt[4]{2}; 0)$.

D'après VII., 2 est constructible. D'après VI.5, $\sqrt{2}$ est constructible et $\sqrt{\sqrt{2}} =^4 \sqrt{2}$ est constructible.
On trace la perpendiculaire à (OI) passant par I et la perpendiculaire à (OJ) passant par J : ces deux droites se coupent en le point K de coordonnées $(1; 1)$, et $OK = \sqrt{2}$. Le cercle de centre O er de rayon OK coupe la droite (OI) en les points de coordonnées $A = (\sqrt{2}; 0)$ et $(-\sqrt{2}; 0)$. À l'aide de la construction de la question VI.4, on trace le point de coordonnées $(1; \sqrt[4]{2})$ puis le point de coordonnées $(\sqrt[4]{2}; 0)$.

Partie B : polygones réguliers

Dans toute cette partie, n est un entier naturel supérieur ou égal à 3.

Soit $M_0 \dots M_{n-1}$ un polygone. On dit qu'il est régulier s'il existe un point O, appelé le centre du polygone, tel que

$$OM_0 = OM_1 = \dots = OM_{n-1},$$
$$(\widehat{\overrightarrow{OM_0}, \overrightarrow{OM_1}}) = (\widehat{\overrightarrow{OM_1}, \overrightarrow{OM_2}}) = \dots = (\widehat{\overrightarrow{OM_{n-2}}, \overrightarrow{OM_{n-1}}}) = (\widehat{\overrightarrow{OM_{n-1}}, \overrightarrow{OM_0}}).$$

IX. 1. Résoudre dans $\mathbb{C}$ l'équation $z^n = 1$.

Si $z^n = 1$, alors $z \neq 0$. Soit z un complexe non nul. On note r son module et soit θ un argument de z.

$$\begin{aligned} z^n = 1 &\iff r^n e^{in\theta} = 1 \\ &\iff \begin{cases} r = 1, \\ n\theta \equiv 0[2\pi], \end{cases} \\ &\iff \begin{cases} r = 1, \\ \theta \equiv 0\left[\frac{2\pi}{n}\right], \end{cases} \\ &\iff \exists k \in \mathbb{Z},\ z = e^{\frac{2i\pi k}{n}}. \end{aligned}$$

Comme $e^{2i\pi} = 1$, les solutions de $z^n = 1$ sont donc les nombres complexes $e^{\frac{2i\pi k}{n}}$, avec $0 \leqslant k < n$.

2. Montrer que les points d'affixe les solutions de l'équation $z^n = 1$ forment un polygone régulier.

Pour tout $k \in [\![0, n-1]\!]$, sont M_k le point d'affixe $e^{\frac{2i\pi k}{n}}$. Pour simplifier la rédaction, on pose aussi $M_n = M_0$, point d'affixe $e^{\frac{2i\pi n}{n}} = 1$. Pour tout $k \in [\![0, n-1]\!]$, $OM_k = |e^{\frac{2i\pi k}{n}}| = 1$. De plus, $(\widehat{\overrightarrow{OM_k}, \overrightarrow{OM_{k+1}}})$ est un argument du nombre complexe

$$\frac{e^{\frac{2i\pi(k+1)}{n}}}{e^{\frac{2i\pi k}{n}}} = e^{\frac{2i\pi}{n}},$$

donc est égal à $\frac{2\pi}{n}$.

X. Pour tout $k \in [\![0, n-1]\!]$, on note M_k le point d'affixe $e^{\frac{2i\pi k}{n}}$. En particulier, $M_0 = I$. Soit B le point d'affixe $\cos\left(\frac{2\pi}{n}\right)$.

1. Montrer que si M_1 est constructible à la règle et au compas, alors B est constructible à la règle et au compas.

M_1 a pour abscisse $\cos\left(\frac{2\pi}{n}\right)$. D'après III, B est constructible car M_1 est constructible.

2. Montrer que si B est constructible à la règle et au compas, alors M_1 est constructible à la règle et au compas.

Soit $\mathcal{D}$ la perpendiculaire à (OI) passant par B : cette droite est constructible. Elle coupe le cercle de centre O et de rayon OI en les points M_1 et M_{n-1}, qui sont donc constructibles.

XI. Montrer que $M_0, \ldots, M_{n-1}$ sont constructibles à la règle et au compas si, et seulement si, B est constructible à la règle et au compas.

Supposons $M_0, \ldots, M_{n-1}$ constructibles. D'après X.1, B est constructible.

Supposons B constructible. $M_0 = I$ est constructible. D'après X.2, M_1 est constructible. Les deux cercles $\mathcal{C}$ et $\mathcal{C}_1$ (constructibles) de centre respectifs O et M_1 et de rayons respectifs OI et M_0M_1 se coupent en M_0 et M_2, qui est donc constructibles. En utilisant les cercles $\mathcal{C}_i$ de centre M_i et de rayon M_0M_1, on obtient successivement $M_2, \ldots, M_{n-1}$, qui sont donc tous constructibles.

XII. En utilisant le point B, montrer que $M_0, \ldots, M_{n-1}$ sont constructibles à la règle et au compas lorsque $n = 3$, $n = 4$ ou $n = 6$. Dans chacun de ces cas, on proposera une construction des points $M_0, \ldots, M_{n-1}$.

Pour $n = 3$: $B(-\frac{1}{2}; 0)$. À l'aide du cercle unité, on obtient le point $I'(-1; 0)$. Alors B est le milieu de $[I'O]$ et on l'obtient par la construction de I.1. On construit la perpendiculaire à (OI) passant par B. L'intersection de cette droite et du cercle unité donne M_1 et M_2.

Pour $n = 4$: $B = O$ L'intersection du cercle unité avec les axes (OI) et (OJ) détermine les points $M_0 = I$, $M_1 = J$, $M_2 = I'$ et $M_3 = J'$.

Pour $n = 6$: $B(\frac{1}{2}; 0)$, donc B est le milieu de $[OI]$. On construit alors la perpendiculaire à (OI) passant par B et l'intersection de cette droite avec le cercle unité donne M_1 et M_5. À l'aide de cercles de rayon M_1I, on obtient M_2, puis M_3, puis M_4.

XIII. On suppose maintenant $n = 5$. On pose $\omega = e^{\frac{2i\pi}{5}}$, et on note $\alpha = \omega + \overline{\omega}$.

1. Justifier que $\alpha = 2\cos\left(\dfrac{2\pi}{5}\right)$.

$$\alpha + \overline{\alpha} = 2Re(\alpha) = 2\cos\left(\frac{2\pi}{5}\right).$$

2. Montrer que $1 + \omega + \omega^2 + \omega^3 + \omega^4 = 0$.

Comme $\omega \neq 1$ et $\omega^5 = 1$:

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 = \frac{1 - \omega^5}{1 - \omega} = 0.$$

3. Montrer que $\alpha = \omega + \omega^4$ et que $\alpha^2 = \omega^2 + \omega^3 + 2$.

$$\overline{\omega} = e^{-\frac{2i\pi}{5}} = e^{-\frac{2i\pi}{5} + 2i\pi} = e^{\frac{8i\pi}{5}} = \omega^4,$$

donc $\alpha = \omega + \omega^4$. Par suite :

$$\alpha^2 = \omega^2 + 2\omega^5 + \omega^8 = \omega^2 + 2 + \omega^3.$$

4. En déduire que $-1+\alpha+\alpha^2=0$ puis que

$$\cos\left(\frac{2\pi}{5}\right)=\frac{-1+\sqrt{5}}{4}.$$

$$0=1+\omega+\omega^2+\omega^3+\omega^4=1+\alpha+\alpha^2-2=-1+\alpha+\alpha^2.$$

Donc $\alpha=\frac{-1+\sqrt{5}}{2}$ ou $\alpha=\frac{-1-\sqrt{5}}{2}$. Comme $\alpha>0$, $\alpha=\frac{-1+\sqrt{5}}{2}$. On obtient :

$$\cos\left(\frac{2\pi}{5}\right)=\frac{\alpha}{2}=\frac{-1+\sqrt{5}}{4}.$$

5. En déduire que $M_0,\dots,M_4$ sont des points constructibles.

D'après VII., 1, 5 et 4 sont des nombres constructibles. D'après VI.5, $\sqrt{5}$ est constructible. D'après V., $\frac{-1+\sqrt{5}}{4}$ est constructible. D'après III., B est constructible. D'après XII., $M_0,\dots,M_4$ sont constructibles.

XIV. On considère la construction suivante.

— Tracer le cercle $\mathbb{U}$ de centre O et de rayon 1. Soit K le point d'affixe -1.
— Construire le milieu B de $[KO]$ et tracer le cercle Γ de centre B et de rayon BJ. On note C le point intersection de Γ et de $[OI]$.
— Construire le milieu de D de $[OC]$.

1. Calculer l'affixe de D.

$$JB=\sqrt{\frac{1}{4}+1}=\frac{\sqrt{5}}{2}.$$

Donc l'affixe de D est $\frac{-1+\sqrt{5}}{4}=\cos\left(\frac{2\pi}{5}\right)$.

2. En déduire une construction du pentagone $M_0M_1M_2M_3M_4$ à la règle et au compas.

En traçant la perpendiculaire à (OI) passant par D, on obtient M_1 et M_4. En traçant les cercles de centre M_1 et M_4 et de rayon IM_1, on obtient M_2 et M_3 par intersection avec le cercle unité.