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 ?

II. Montrer que, quelle que soit la fonction de cryptagef_k choisie, les symboles espace et point 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.

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 ?

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

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.

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.

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.

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

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

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

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

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

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 $o(x)$.

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.

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

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

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

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

d. En déduire que 2 est primitif modulo 29.

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.

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.

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

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

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

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.

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.

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.

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

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

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 $w \in R$.

5. Que conclure pour f_k ?

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

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

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 ?

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

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

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

3. Quelle formule doit-on écrire en D7 pour remplir la ligne 7 en utilisant la poignée de recopie et obtenir ainsif_{19} ?
4. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

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 ?
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.
3. Quelle formule doit-on écrire en D5 pour remplir la ligne 5 en utilisant la poignée de recopie et obtenir ainsif_{19} ?
4. Pour remplir chaque colonne, combien de multiplications et combien de divisions euclidiennes par 29 sont-elles effectuées ?

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

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.

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.

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.

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.

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.

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.

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

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.
2. Montrer que le cercle $\mathcal{C}$ de diamètre $[OA]$ est constructible à la règle et au compas.
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.
4. Soit $\theta = (\widehat{\overrightarrow{OI}, \overrightarrow{OB}})$. Exprimer $\tan(\theta)$ et $\tan\left(\dfrac{\pi}{2} - \theta\right)$ en fonction de BI et de x. En déduire BI.
5. Montrer que $\sqrt{x}$ est un nombre constructible.

VII. Montrer que tous 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 $(\sqrt[4]{2};0)$.

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

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 $\cos\left(\dfrac{2\pi}{n}\right)$.

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

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

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.

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 $M_0, \ldots, M_{n-1}$.

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

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

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

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

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

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

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

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