Avertissement : Ceci n'est pas une correction *in extenso* du problème de capes. Il s'agit plutôt d'une lecture personnelle des questions, avec des indications, des idées de preuve, des mises en garde d'erreurs à éviter. Ce n'est surtout pas une correction modèle à reproduire... Pour signaler toute erreur, merci d'écrire à `devgeolabo@gmail.com`

Le premier problème est un problème traitant de cryptographie et d'arithmétique. Il permet de travailler essentiellement ce dernier chapitre, ainsi que l'utilisation d'un tableur. A noter aussi quelques questions sur les groupes et un algorithme. Ce problème est extrêment long ! Le second problème porte sur les constructions à la règle et au compas. Beaucoup plus court, un peu répétitif, il ne nécessite que des connaissances très élémentaires !

Premier problème

Partie A

I. Puisque $6^3 = 216$ et que le reste de 216 dans la division par 29 est 13, la lettre E est transformée en L.

II. Puisque $0^k = 0$ et que $1^k = 1$, on a $f_k(0) = 0$ et $f_k(1) = 1$ pour tout entier naturel k non nul. Donc les symboles espace et point sont inchangés.

III. Il ne faut pas oublier le symbole `$` qui permet de ne pas décaler $AE3$ lorsque la cellule est dupliquée vers la gauche. On rentre donc `=MOD(D2^$AE3;29)`.

IV. Les mots CLE et LUC sont tous les deux cryptés (en réalité, le vocabulaire employé en informatique serait plutôt chiffrés) par `,,,`. Ils sont donc cryptés de la même façon.

V. Pour pouvoir assurer le décryptage, il faut et il suffit que deux lettres ne soient jamais cryptés de la même façon. Autrement dit, il faut et il suffit que la fonction f_k soit injective (ce qui, puisque f_k est une application de l'ensemble fini R dans lui-même, est équivalent à dire que f_k est bijective).

VI. Le problème vient du mode de stockage des nombres dans le tableur. En général, un tableur classique comme Excel ou LibreOffice Calc stocke les nombres avec 14 chiffres significatifs (environ). Quand les nombres, même entiers, deviennent trop grands, il les arrondit. Par exemple, pour un tableur, les nombres 100 000 000 000 000 et 100 000 000 000 001 seront identiques. Les calculs faits alors ne seront plus justes. Cela dit, l'exemple donné par l'énoncé est clairement faux ! D'après l'énoncé, le tableur serait incapable de calculer $3^{19} = 1162261467$ ce qui n'est pas le cas (au moins pour LibreOffice) ! Il semble que cela foire à partir de 7^{19} plutôt. Détaillons d'ailleurs un peu le fonctionnement d'Excel et de LibreOffice. Ce dernier affiche toujours un résultat, qui n'a pas de sens, sans prévenir qu'il n'a pas de sens ! (par exemple, pour anticiper la question suivante, les calculs effectués ne montrent pas du tout que f_{29} est l'identité). Excel est plus honnête puisqu'il affiche le fameux #NOMBRE ! donné par l'énoncé. Il signifie concrètement qu'en calculant 7^{19}, Excel a trouvé un nombre trop grand pour qu'il puisse être stocké comme un entier avec tous ses chiffres. Il est stocké en machine différemment (comme un nombre flottant). En affichant #NOMBRE !, Excel dit que cela n'a pas de sens de calculer le reste dans une division euclidienne d'un tel nombre.

Partie B

VII.1. La clé pour cette question comme pour beaucoup de questions qui vont suivre est le théorème de Gauss. Si $u|vw$ et si u et v sont premiers entre eux, alors $u|w$. Ici, comme p est premier et que p ne divise pas a, alors p est premier avec a. Le sens direct de l'équivalence demandée découle alors directement du théorème de Gauss : puisque p divise ka et que p est premier avec a, alors p divise k. La réciproque est triviale. Si p divise k, alors p divise tout multiple de k, en particulier ka.
Comme p ne divise aucun des entiers compris entre 1 et $p-1$, alors p ne divise aucun des ka pour k allant de 1 à $p-1$.

VII.2.a. Écrivons $ia = q_i p + \alpha_i$. Alors, si $\alpha_i = 0$, on aurait $p|ia$ ce qui n'est pas le cas. Si pour $i \neq j$, on avait $\alpha_i = \alpha_j$, alors en soustrayant les deux équations $ia = q_i p + \alpha_i$ et $ja = q_j p + \alpha_i$, on trouverait que $(i-j)a = (q_i - q_j)p$, et donc on déduirait que p divise $i-j$. C'est impossible, car $i-j$ est un élément de $-(p-1), -(p-2), \ldots, -1, 1, \ldots, p-2, p-1$ et p ne divise aucun de ces entiers.

VII.2.b. L'ensemble des α_i, pour i de 1 à $p-1$, est un ensemble à $p-1$ éléments (puisque tous les α_i sont distincts) qui est contenu dans l'ensemble $\{1, \ldots, p-1\}$ (puisque $0 \leq \alpha_i \leq p-1$ d'après la caractérisation du reste dans la division euclidienne, et puisque $\alpha_i \neq 0$). Ce dernier ensemble contenant exactement $p-1$ éléments, on en déduit l'égalité demandée.

VII.3. D'une part (par commutativité du produit ? ? ?), on a

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

D'autre part, puisque $ia \equiv \alpha_i\ [p]$ et que la congruence est compatible avec les multiplications, on a

$$P \equiv \prod_{i=1}^{p-1} \alpha_i\ [29].$$

Mais, d'après la question précédente (et par commutativité du produit ? ? ?),

$$\prod_{i=1}^{p-1} \alpha_i = 1 \times 2 \times \cdots \times p-1 = (p-1)!.$$

VII.4. On vient de démontrer que $a^{p-1}(p-1)! \equiv (p-1)!\ [p]$. Autrement dit, p divise $(p-1)! \times (a^{p-1}-1)$. Un dernier coup de théorème de Gauss, et le tour est joué ! Puisque p est premier avec $(p-1)!$, on a $p|a^{p-1}-1$, qui est le résultat demandé.

VII.5. Puisque 29 est premier, et que $28 = 29 - 1$, la question précédente nous dit que si a est compris entre 1 et 28, alors $a^{28} \equiv 1\ [29]$. Autrement, f_{28} est identiquement égale à 1 sur R, sauf bien sûr $f_{28}(0) = 0$. Puisque $a^{29} = a \times a^{28}$, on en déduit que f_{29} est égale à l'identité.

VII.6. Supposons par exemple que $k \geq l$, et donc que $k = l + 28n$ avec $n \geq 0$. Alors pour $a = 0$, on a bien sûr $f_k(0) = f_l(0) = 0$. Pour $a \in \{1, \ldots, p-1\}$, on a

$$a^l = a^{k+28n} = a^k (a^{28})^n \equiv a^k \times 1^n\ [p]$$

ce qui prouve que $a^l \equiv a^k\ [p]$. Donc $f_k(a) = f_l(a)$.

VIII.1. Notons $E = \{k \geq 1;\ x^k \equiv 1\ [28]\}$. Alors E est une partie de $\mathbb{N}$ non vide (puisqu'elle contient 28). Elle possède donc un plus petit élément (qui est bien entendu inférieur ou égal à 28).

VIII.2. Un sens est très facile : si $o(x)$ divise k, alors $k = mo(x)$ et donc $x^k = (x^{o(x)})^m \equiv 1^m \equiv 1$ [29]. La réciproque est plus difficile, et il faut utiliser la division euclidienne : si $x^k \equiv 1$ [29], effectuons la division euclidienne de k par $o(x)$: $k = qo(x) + r$, avec $0 \leq r < o(x)$. Alors,

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

Donc $x^r \equiv 1$ [29]. Puisque $o(x)$ est le plus entier strictement positif possédant cette propriété, et que r est strictement plus petit que $o(x)$, on en déduit que $r = 0$. Ceci signifie que $o(x)$ divise k.

VIII.3. Conséquence directe de la question précédente et de $x^{28} \equiv 1$ [29].

VIII.4. Voici deux algorithmes possibles sous Python (qui ne testent pas si x est premier avec 29) :

```
def ordre(x):
    k=1
    while ( (x**k)%29!=1):
        k=k+1
    return k
```

```
def ordre(x):
    k=1
    y=x%29
    while (y!=1):
        k=k+1
        y=(y*x)%29
    return k
```

Le premier copie la définition de l'ordre. On regarde le reste modulo 29 de x^k jusqu'à la première valeur de k pour laquelle ce reste vaut 1. L'intérêt de travailler avec Python est que les calculs qu'il réalise sur les nombres entiers sont exacts et le problème qui se posait auparavant avec les tableurs n'apparait plus ici.
Le second algorithme fait la même chose, mais il est plus malin pour calculer le reste de x^k modulo 29. Il évite de recalculer x^k à chaque fois, en remarquant que si r_k est le reste de x^k modulo 29, alors r_{k+1} est le reste de $r_k \times x$ modulo 29, puisque si $x^k \equiv r_k$ [29], alors $x^{k+1} \equiv r_k \times x$ [29].

VIII.5.a. $\{1, 2, 4, 7, 14, 28\}$.

VIII.5.b. Dans le premier cas, l'ordre de x est inférieur ou égal à 14, dans le second, il est inférieur ou égal à 4.

VIII.5.c. L'ordre de x peut être $1, 2, 4, 7, 14, 28$. Il n'est ni 4, ni 14. Il ne peut pas être 2, sinon $x^2 \equiv 1$ [29] $\implies x^4 = (x^2)^2 \equiv 1$ [29]. Il ne peut pas être 7 sinon pour les mêmes raisons, $x^7 \equiv 1$ [29] $\implies x^{14} \equiv 1$ [29]. Il ne peut pas être 1, sinon $x^k \equiv 1$ [29] pour tous les $k \geq 1$. Il ne peut donc être égal qu'à 28.

VIII.5.d. D'après les questions précédentes, il suffit de vérifier que 2^4 et 2^{14} ne sont pas congrus à 1 modulo 29. Pour 2^4, c'est facile car $2^4 = 16$. Pour 2^{14}, il faut être malin et remarquer par exemple que $2^5 = 32 \equiv 3$ [29]. Il vient $2^{10} = (2^5)^2 \equiv 3^2 = 9$ [29]. D'où

$$2^{14} = 2^{10}2^4 \equiv 9 \times 16 = 144 \equiv 28 \equiv -1 \text{ [29]}.$$

IX. Puisqu'on démontre à la question VIII que 2 est primitif modulo 29, nous sommes incités à démontrer que $\bar{2}$ est un générateur du groupe $G = \{\bar{x} \in \mathbb{Z}/29\mathbb{Z};\ \bar{x} \neq \bar{0}\}$ (rappel sur la définition d'un groupe cyclique). Autrement dit, on doit prouver que pour tout $\bar{x} \in \mathbb{Z}/29\mathbb{Z}$ avec $\bar{x} \neq 0$, il existe un entier k tel que $\bar{2}^k = \bar{x}$. C'est une question difficile. Calculons d'abord le cardinal de G. On a clairement $G \subset \{\bar{1}, \bar{2}, \ldots, \overline{28}\}$ et on a même égalité car aucun des $\bar{x}$ pour $x = 1, \ldots, 28$ n'est égal à $\bar{0}$. Considérons ensuite l'application

$$\begin{aligned} \phi : \{1, \ldots, 28\} &\to G \\ k &\mapsto \bar{2}^k. \end{aligned}$$

Démontrons que cette application est injective. Si elle ne l'est pas, il existe $1 \leq k < l \leq 28$ tels que $\bar{2}^k = \bar{2}^l$. En particulier, on a

$$\bar{2}^{l-k} = \bar{1} \iff 2^{l-k} \equiv 1\ [29].$$

Mais $1 \leq l - k < 28$, et ceci contredit que 2 est primitif modulo 29.
Ainsi, ϕ est injective. Mais comme c'est une application entre deux ensembles finis qui ont le même nombre d'éléments, elle est aussi surjective. Ainsi, pour tout $\bar{x} \in G$, il existe un entier k tel que $\bar{2}^k = \phi(k) = \bar{x}$. Ceci prouve bien que 2 est un générateur de G, et donc que ce groupe fini est cyclique.

X. Je ne comprends pas bien l'ordre des questions. Essentiellement, à cette question, on fait à nouveau le raisonnement de la question précédente, mais on donne de multiples détails... Ai-je raté quelque chose à la queston IX. ? ? ? ? Ou bien est-ce l'auteur du sujet qui aurait du mettre la question X avant la question IX ?

X.1. Le plus dur est de comprendre ce que signifie "bien définie". Ici, il faut entendre que φ est bien à valeurs dans S, puisqu'a priori elle est à valeurs dans $\{0, 1, \ldots, 28\}$. Autrement dit, il faut prouver que pour tout k dans S, on n'a pas $\varphi(k) = 0$, ce qui signifie que 2^k n'est pas divisible par 29. C'est maintenant un raisonnement d'arithmétique simple....

X.2. Le point clé du raisonnement est le suivant. Puisque $\varphi(k)$ et $\varphi(k')$ sont tous les deux à valeurs dans $\{1, \ldots, 28\}$, on a $\varphi(k) = \varphi(k')$ si et seulement si $\varphi(k) \equiv \varphi(k')$ [29]. Tout le reste n'est alors que de l'arithmétique élémentaire :

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

X.3. Recopier le raisonnement de la question IX....

X.4. Il s'agit juste d'une réécriture du fait que φ est bijective !

XI.1. Si 29 divise z, alors 29 divise z^k et donc 29 divise y, ce qui est impossible puisque $y \in S$.

XI.2. Cela ressemble beaucoup à la question X.2. :

$$\begin{aligned} z^k \equiv y\ [29] &\iff (2^t)^k \equiv 2^x\ [29] \\ &\iff 2^{kt} \equiv 2^x\ [29] \\ &\iff 2^{kt-x} \equiv 1\ [29] \end{aligned}$$

Si $kt-x$ est positif, donc un entier naturel, on sait que ceci est équivalent à dire que $kt-x$ est un multiple de $o(2)$, c'est-à-dire 28 (cf question VIII.3.). Si $kt-x$ est négatif, on fait le même raisonnement avec $x-kt$.

XI.3.a. D'après le théorème de Bézout, l'équation $ak+28b=1$ admet un couple de solutions $(a,b)\in\mathbb{Z}^2$ si et seulement si k et 28 sont premiers entre eux.

XI.3.b. C'est très classique et presque du cours. Si (a,b) est une autre solution, alors on a à la fois

$$ak+28b=1$$
$$a_0k+28b_0=1.$$

En soustrayant ces deux égalités, on a

$$(a-a_0)k+28(b-b_0)=0 \iff (a-a_0)k=-28(b-b_0).$$

On a donc $k|28(b-b_0)$. Puisque $k\wedge 28=1$, on en déduit par le théorème de Gauss que $k|b-b_0$: ainsi, il existe un entier $m\in\mathbb{Z}$ tel que $b-b_0=km$, ie $b=b_0+km$. Si on reporte ceci dans l'identité précédente, on trouve

$$(a-a_0)k=-28mk \implies a=a_0-28m.$$

Attention !!! Ici, on n'a pas fait un raisonnement par équivalence, et on a simplement prouvé que, si (a,b) est une solution de (*), alors il existe $m\in\mathbb{Z}$ tel que $a=a_0-28m$ et $b=b_0+km$. Réciproquement, si (a,b) est un couple d'entiers tels que $a=a_0-28m$ et $b=b_0+km$, alors

$$ak+28b=(a_0-28m)k+28(b_0+km)=a_0k+28b_0=1,$$

et donc (a,b) est bien une solution de (*).

XI.3.c Partons de la solution (a_0,b_0). Soit $a_1\in R$ tel que $a_0\equiv a_1$ [28]. En particulier, il existe $m\in\mathbb{Z}$ tel que $a_1=a_0-28m$. Posons alors $b_1=b_0+km$. Alors le couple (a_1,b_1) est une solution de l'équation. De plus, a_1 ne peut pas être égal à 0 (sinon on aurait $28b_1=1$, impossible !). Puisque $a_1\in R$, on en déduit $a_1\in S$.
Supposons maintenant qu'il y ait deux solutions (a_1,b_1) et (a_2,b_2) à l'équation avec a_1 et $a_2\in S$. Alors, d'après la question précédente, on sait que $a_2-a_1=-28m$ pour un certain $m\in\mathbb{Z}$. Mais comme $|a_2-a_1|<28$ puisqu'ils sont tous les deux éléments de S, on a nécessairement $m=0$, et donc $a_1=a_2$.

XI.4. Fixons $w\in R$, et notons $v=f_k(w)$ et $u=f_{a_1}(v)$. Alors v est le reste de w^k dans la division par 29 et u est le reste de v^{a_1} dans la division par 29. Autrement dit,

$$w^k\equiv v\ [29] \text{ et } v^{a_1}\equiv u\ [29].$$

Par les propriétés des congruences,

$$w^{a_1k}\equiv v^{a_1}\equiv u\ [29].$$

Mais on sait que $a_1k=1-28b$ et donc

$$w^{a_1k}\equiv w\cdot(w^{28})^b\ [29].$$

Le résultat de la question VIII.3. nous dit que $w^{28}\equiv 1$ [29], et donc on a $w^{a_1k}\equiv w$ [29]. Ceci prouve que $f_{a_1}\circ f_k(w)=w$. Le même raisonnement prouve que $f_k\circ f_{a_1}(w)=w$.

XI.5. On en conclut que f_k est bijective, et que sa bijection réciproque est la fonction f_{a_1}. Autrement dit, la fonction f_{a_1} permet d'assurer le décryptage de la fonction f_k.

XII. On a $3 \times 19 - 2 \times 28 = 1$, et donc avec les notations précédentes, $a_1 = 3$. Je vous laisse terminer....

XIII. Dans la question XI. on a déjà prouvé que si k est premier avec 28, alors tout message crypté avec f_k peut être décrypté avec f_{a_1}. Réciproquement, si k n'est pas premier avec 28, on va prouver que f_k n'est pas injective, prouvant l'existence de messages cryptés avec f_k qui ne peuvent pas être décryptés. Soit d un diviseur commun de 28 et k, avec $d > 1$. Écrivons $28 = du$ et $k = dv$. Alors, posons $w \in R$ tel que $2^u \equiv w$ [29]. On n'a pas $w = 1$ sinon l'ordre de 2 serait inférieur strict à 28. De plus, on a

$$w^k \equiv (2^u)^{dv} \text{ [29]} \equiv (2^{ud})^v \text{ [29]} \equiv 1^v \text{ [29]} \equiv 1 \text{ [29]}.$$

Autrement dit, $f_k(1) = f_k(w)$, et donc, comme annoncé, la fonction f_w n'est pas injective.

Partie C

XIV.1. L'énoncé ne me semble pas extrêment clair sur ce qui est demandé. Je pense (cf la question suivante) qu'il faut comprendre remplir le tableau en effectuant uniquement des multiplications et des divisions euclidiennes (pas de puissances). La formule qui convient est alors : `=MOD(D2*D$2;29)`.

XIV.2. Sur chaque colonne, on a 18 multiplications et 18 divisions euclidiennes qui sont effectuées.

XV.1. On veut que chaque ligne soit le carré, modulo 29, de la précédente. La formule à rentrer est donc `=MOD(D2*D2;29)`.

XV.2. On a

$$f_{19}(x) \equiv x^{19} \text{ [29]} \equiv x^{2^4} \times x^{2^1} \times x^{2^0} \text{ [29]}.$$

Mais $f_2(x) \equiv x^2$ [29], $f_2(f_2(x)) \equiv (x^2)^2 = x^{2^2}$ [29], $f_2 \circ f_2 \circ f_2(x) \equiv (x^{2^2})^2 = x^{2^3}$ [29] et finalement $f_2 \circ f_2 \circ f_2 \circ f_2(x) \equiv (x^{2^3})^2 = x^{2^4}$ [29].

XV.3. On doit donc remplir `=MOD(D2*D3*D6;29)`.

XV.4. Pour chaque colonne, on réalise 6 multiplications (une par ligne de 3 à 6, deux pour la ligne 7), et 5 divisions euclidiennes (une par ligne de 3 à 7).

XVI./XVII. Je vais très vite, c'est presque la même chose et j'en ai marre ! Dans D4, on entre `=MOD(D3*D3*D3;29)`. Dans D5, on rentre `=MOD(D4*D4*D2;29)`. Sur chaque colonne, on effectue donc 4 multiplications et 2 divisions euclidiennes. C'est cette méthode qui a l'air le plus efficace !

Deuxième problème

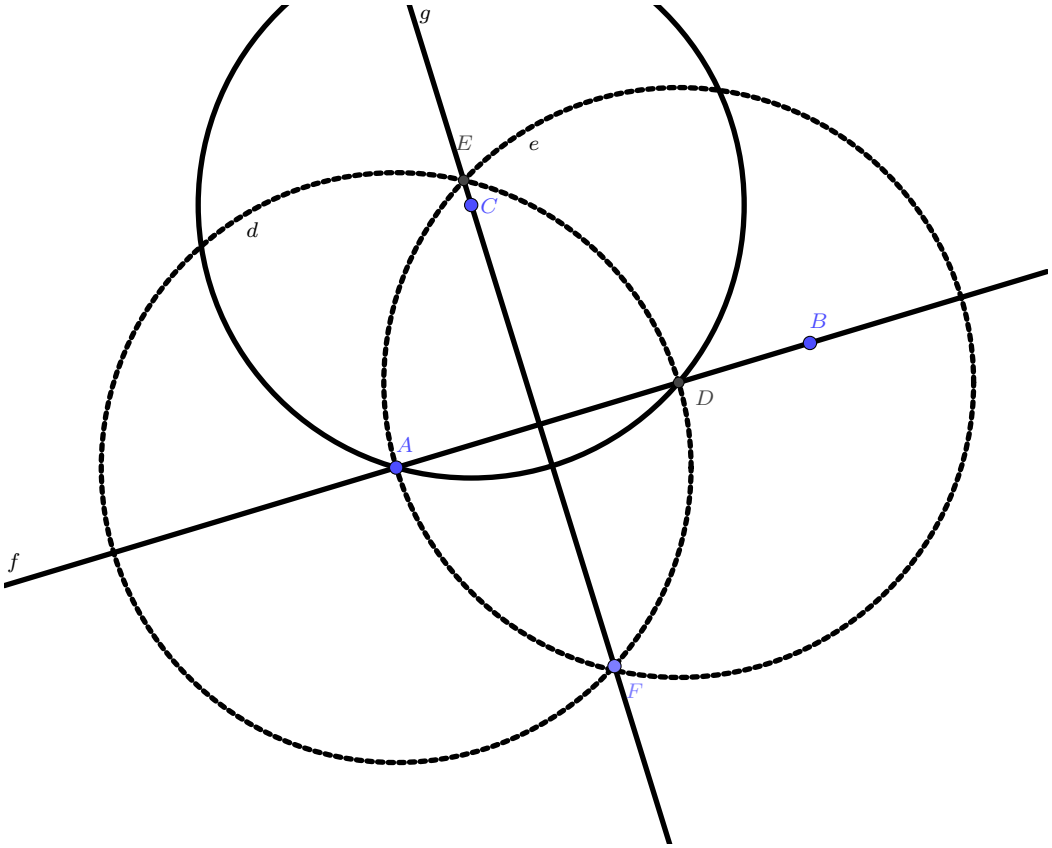
Partie A

I.1. On trace le cercle C_1 de centre A et de rayon AB et le cercle C_2 de centre B et de rayon AB. Ces deux cercles se coupent en deux points C et D. La droite (CD) est la médiatrice de $[AB]$. L'intersection de (CD) et de (AB) est le milieu de $[AB]$.

I.2. Supposons d'abord que $C \neq A$. On construit alors successivement :
— Le cercle C_1 de centre C et de rayon AC.

— Si la droite (AB) est tangente au cercle C_1, alors c'est que (AC) est perpendiculaire à (AB) et on a terminé. Sinon, le cercle C_1 coupe la droite (AB) en A et en un second point D.
— On construit comme précédemment la médiatrice à (AD). Cette médiatrice passe par C puisque $CA = CD$. C'est donc la perpendiculaire à (AB) passant par C.

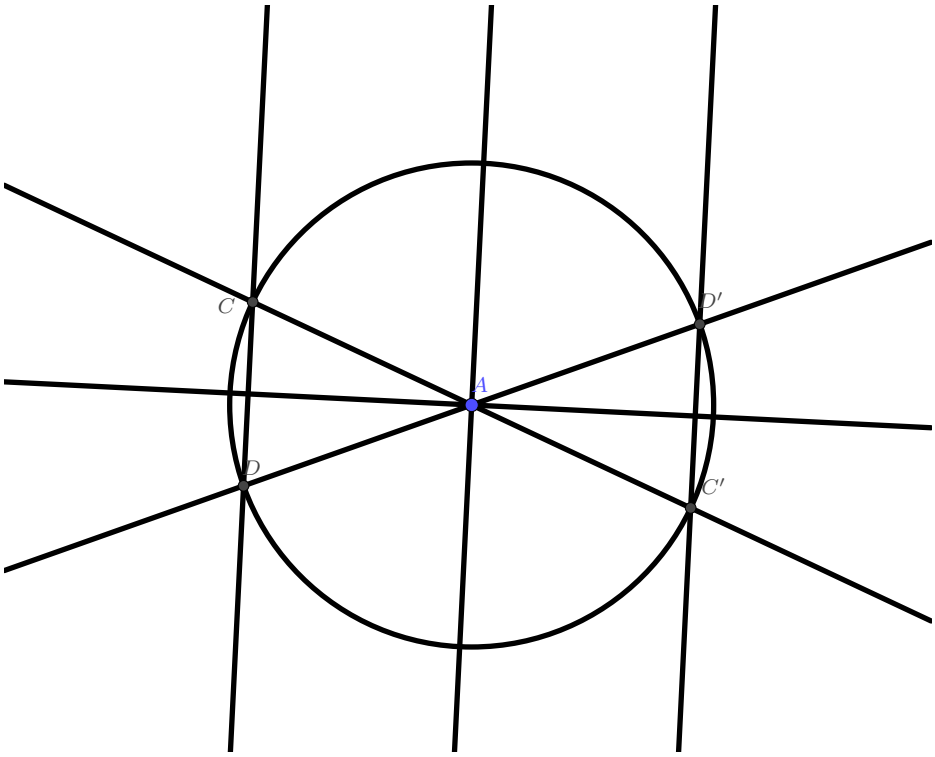
Si maintenant $C = A$, alors on fait la même construction en remplaçant le point A par le point B.



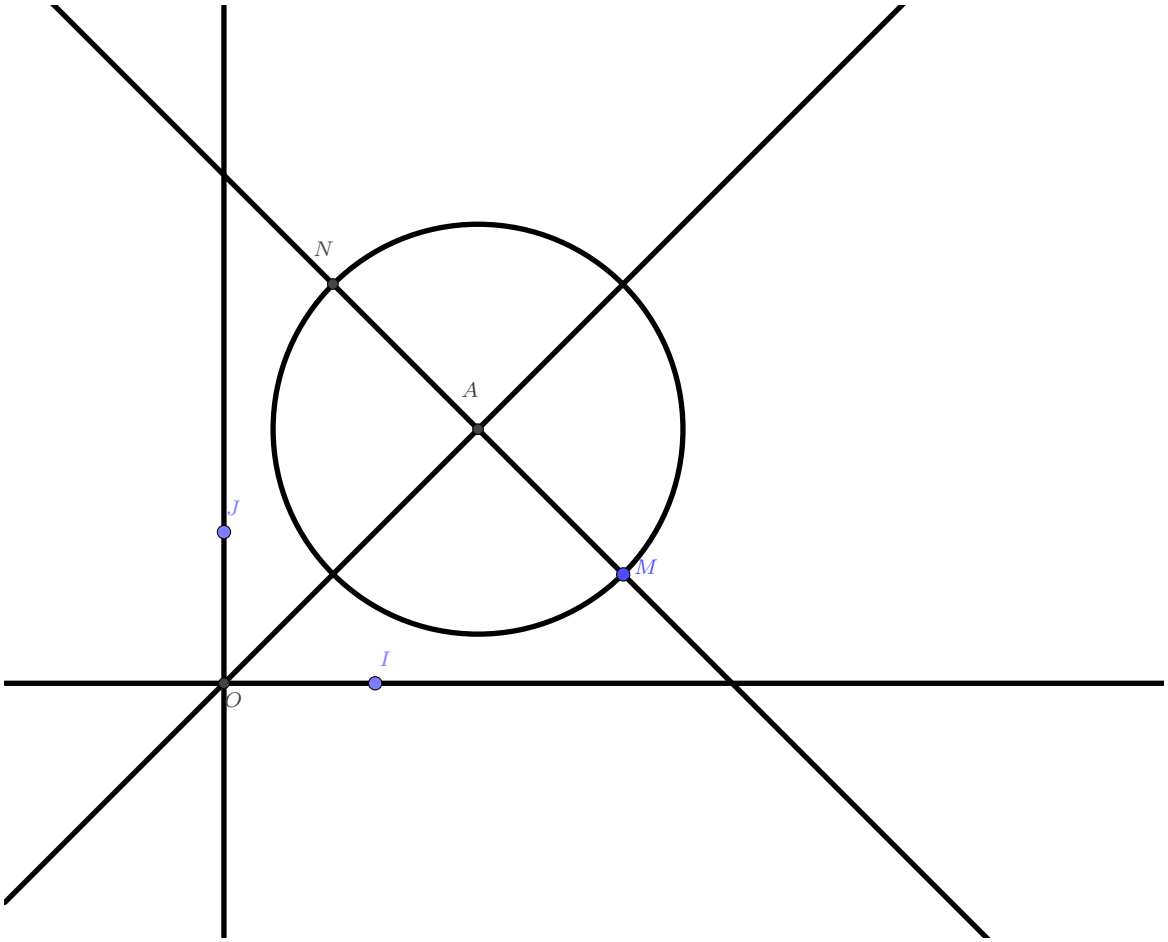
I.3. Rapidement, on construit la perpendiculaire à (AB) passant par C (on sait faire d'après la question précédente). Soit D un autre point de cette droite. Alors on construit la perpendiculaire à (CD) passant par C.

I.4. — On trace le cercle de centre A et de rayon OI.
— Ce cercle coupe $\mathcal{D}$ en C et C' et $\mathcal{D}'$ en D et D'.
— On trace (comme à la question I.2.) la perpendiculaire à (CD) passant par A. On obtient une des deux bissectrices qu'on note $\mathcal{D}_1$.
— On trace la perpendiculaire à $\mathcal{D}_1$ passant par A.

Dans la figure suivante, on a volontairement enlevé les traits de construction pour tracer les perpendiculaires (bon d'accord, j'ai utilisé l'outil Droites Perpendiculaires de Geogebra !)



II. Que le réel x soit constructible est simplement une application de la définition. Ensuite, il faut être capable de construire le point (y, x) (par exemple) pour obtenir que y est constructible. Le point (y, x) est le symétrique de (x, y) par rapport à la première bissectrice du repère. Successivement,
   - on construit cette première bissectrice, notée Δ ;
   - on trace la perpendiculaire à Δ passant par (x, y), notée D ;
   - on considère A le point d'intersection de Δ et de D ;
   - on considère le cercle de centre A et de rayon AM, où M est le point de coordonnées (x, y).
   - ce cercle coupe la droite (AM) en M et en un deuxième point N. Ce point N est le symétrique de M par rapport à Δ, il a pour coordonnées (y, x).



III. C'est facile ! Si x est constructible, c'est qu'il existe un réel y tel que (x, y) est constructible et on a vu d'après la première question que (y, x) est aussi constructible. On construit ensuite la parallèle à (OJ) passant par (x, y). Elle coupe (OI) en $(x, 0)$, qui est donc constructible...

IV.1. Si x est constructible, alors on peut construire le point d'abscisse x sur la droite (OI). Notons A ce point. Traçons le cercle de centre O et de rayon OA. Il coupe la droite (OI) en deux points : le point A et le point B dont l'abscisse est $-x$.

IV.2. Notons A le point de coordonnées $(x, 0)$ et B le point de coordonnées $(y, 0)$. Traçons ensuite le cercle de centre A et de rayon OB. Il coupe la droite (OI) en deux points : le point d'abscisse $x - y$ et le point d'abscisse $x + y$.

IV.3. Traçons (D) la parallèle à (AJ) passant par B. Elle coupe la droite (OI) en un point C (qui est donc constructible). Appliquons ensuite le théorème de Thalès au triangle OBC avec (AJ) parallèle à (BC). On a donc :

$$\frac{OC}{OA} = \frac{OB}{OJ} \text{ et donc } OC = \frac{OA \times OB}{OJ} = xy.$$

Ainsi, xy est constructible.

IV.4. Considérons $A(x, 0)$ et $B(y, 0)$, et traçons la droite (D) parallèle à (BJ) passant par A. Soit C son point d'intersection avec la droite (OJ). Je laisse conclure en utilisant le théorème de Thalès...

V. Si par exemple $x < 0$ et $y > 0$, alors on peut construire $-x > 0$, et donc on peut construire $-x+y$, $-x-y$, $-xy$, $-x/y$. Il suffit de reprendre l'opposé de ces nombres pour construire $x+y$, $x-y$,... C'est à peu près pareil si x et y sont tous les deux strictement négatifs (si l'un des deux est nul, c'est trivial !).

VI.1. Question IV.2.

VI.2. On peut construire le milieu de $[0A]$...

VI.3. ? ? ?

VI.4. Dans le triangle OIB rectangle en I, on a $\tan(\theta) = \frac{BI}{1}$. Dans le triable AIB, rectangle en I, on a $\tan(\frac{\pi}{2} - \theta) = \frac{IB}{IA} = \frac{IB}{x}$. Puisque $\tan(\frac{\pi}{2} - \theta) = \frac{1}{\tan\theta}$, on en déduit $IB^2 = x$.

VI.5. Tracer le cercle de centre O et de rayon IB...

VII. Très rapidement, on montre par récurrence que tous les entiers naturels sont constructibles, puis par des questions précédentes que tous les entiers relatifs et enfin tous les rationnels sont constructibles.

VIII. Puisque 2 est constructible, $\sqrt{2}$ est constructible. Puisque $\sqrt{2}$ est constructible, $\sqrt{\sqrt{2}} = \sqrt[4]{2}$ est constructible. Pour les construire pratiquement, tout est déjà décrit dans les questions précédentes....

Partie B

IX.1. C'est du cours. L'ensemble des solutions est $\{e^{2ik\pi/n};\ k = 0, \dots, n-1\}$.

IX.2. Rappelons que si A, B, C et D sont des points du plan d'affixes respectives a, b, c et d, alors

$$(\widehat{\overrightarrow{AB}, \overrightarrow{CD}}) = \arg\left(\frac{b-a}{d-c}\right)\ [2\pi].$$

Notons M_k le point d'affixe $e^{2ik\pi/n}$, $k = 0, \dots, n-1$. Alors on a

$$(\widehat{\overrightarrow{OM_k}, \overrightarrow{OM_{k+1}}}) = \arg\left(\frac{e^{2i(k+1)\pi/n} - 0}{e^{2ik\pi/n} - 0}\right) = \arg(e^{2i\pi/n}) = 2i\pi/n\ [2\pi].$$

Comme de plus $OM_k = 1$, $M_0 \dots M_{n-1}$ est bien un polygone régulier.

X.1. Le point B est constructible comme point d'intersection de (OI) et de la parallèle à (OJ) passant par M_1. L'énoncé aurait dû nous faire démontrer une propriété sur la constructibilité des projections plutôt que de nous demander trois fois d'écrire la même chose !

X.2. Le cercle unité est constructible à la règle et au compas, la droite parallèle à (OJ) passant par B est elle-aussi constructible. Le point M_1 est constructible comme intersection de ces deux objets.

XI. On a prouvé que B est constructible si et seulement M_1 est constructible. Il suffit donc de prouver que si B est constructible, alors $M_2, \dots, M_{n-1}$ sont constructibles (bien sûr, $M_0 = I$ est constructible). Puisque B est constructible, M_1 l'est. Traçons alors le cercle de centre M_1 et de rayon M_1I. Il intersecte le cercle unité en deux points : le point I, et le point C. Puisque $OC = OI = 1$ et que $M_0C = M_0I$, la droite (OM_0) est la médiatrice de $[IC]$. En particulier, on a

$$(\widehat{\overrightarrow{OI}, \overrightarrow{OM_1}}) = (\widehat{\overrightarrow{OM_1}, \overrightarrow{OC}}) = \frac{2\pi}{n}\ [2\pi].$$

On en tire que

$$(\widehat{\overrightarrow{OI},\overrightarrow{OC}}) = \frac{4\pi}{n}\ [2\pi]$$

et donc que $C = M_2$. En répétant la construction, on construit les autres points M_k.

XII. Il suffit de remarquer que $\cos(2\pi/3) = -1/2$, $\cos(\pi/2) = 0$ et $\cos(\pi/3) = 1/2$ sont constructibles.... La construction des polygones réguliers correspondants est très facile. Pour $n = 3$, on construit
— le point $C = (-1, 0)$ en traçant le cercle de centre O et de rayon OI
— la médiatrice de $[OC]$;
— cette médiatrice coupe le cercle unité en M_1 et en M_2.
Je vous laisse écrire des protocoles de construction pour les autres cas.

XIII.1. On écrit

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

XIII.2. Puisque $\omega \neq 1$, la formule donnant la somme d'une suite géométrique nous dit que

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

XIII.3. Il suffit de remarquer que

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

et que

$$\alpha^2 = \omega^2 + \bar{\omega}^2 + 2\omega\bar{\omega} = \omega^2 + \omega^3 + 2.$$

XIII.4. La première relation est une conséquence directe des deux questions précédentes. Ensuite, on résout l'équation du second degré et on utilise le résultat de la question XIII.1. pour obtenir le résultat.

XIII.5. D'après la partie A, $\cos(2\pi/5)$ est constructible... On utilise ensuite le résultat de la question X.2.

XIV. Le point B est d'affixe $-1/2$. Par le théorème de Pythagore dans le triangle BOJ rectangle en O, on a $BJ^2 = BO^2 + OJ^2 = 5/4$. On a donc $BC = \sqrt{5}/2$ et le point C est d'affixe $\frac{\sqrt{5}-1}{2}$. Le point D est d'affixe $\cos(2\pi/5)$. D'où la construction du polygone régulier à 5 côtés...