SESSION 2018

CAPES EXTERNE

MATHÉMATIQUES 2

Problème n° 1

Partie A : premiers essais

I. La lettre E correspond au nombre 6. $6^3 = 216$ puis $216 = 7 \times 29 + 13$ avec $0 \leqslant 13 \leqslant 28$. Donc, $f_3(6) = 13$. Par la méthode de cryptage d'Albert, la lettre E est remplacée par la lettre L.

II. Soit $k \in \mathbb{N}^*$. Le point correspond au nombre 0. $0^k = 0 = 0 \times 29 + 0$ avec $0 \leqslant 0 \leqslant 28$. Donc, $f_k(0) = 0$.
De même, l'espace correspond au nombre 1. $1^k = 1 = 0 \times 29 + 1$ avec $0 \leqslant 1 \leqslant 28$. Donc, $f_k(1) = 1$.

Les symboles espace et point sont donc inchangés après cryptage.

III. La référence à la colonne de la case AE3 doit être absolue et pas relative.
On doit donc rentrer la formule =MOD(D2^$AE3;29) (ou aussi =MOD(D2^AE3;29), auquel cas c'est la référence de la case qui est absolue).

IV. CLE se code en 4 13 6 avec $(f_7(4), f_7(13), f_7(6)) = (28, 28, 28)$ et donc CLE se crypte en , , ,
LUC se code 13 22 4 avec $(f_7(13), f_7(22), f_7(4)) = (28, 28, 28)$ et donc CLE se crypte en , , ,

En particulier, les deux mots CLE et LUC, bien que différents, se cryptent de la même façon (ce qui ne convient pas).

V. Une fonction de cryptage f_k est correcte si et seulement si : $\forall (x, y) \in [\![0, 28]\!]^2,\ (x \neq y \Rightarrow f_k(x) \neq f_k(y))$ ou encore si et seulement si f_k est injective. Ensuite, puisque la fonction f_k va de l'ensemble fini $[\![0, 28]\!]$ dans lui-même, f_k est injective si et seulement si f_k est bijective.

Finalement, la fonction f_k est une bonne fonction de cryptage si et seulement si la fonction f_k est une permutation de $[\![0, 28]\!]$.

VI. L'affichage #NOMBRE ! vient du fait que les nombres obtenus sont trop grands pour la capacité d'Excel (ceci dit, le nombre $3^{19} = 1\,162\,261\,467$, écrit dans la case E3, n'est certainement pas hors format).

Partie B : choix de la fonction de cryptage

VII.

VII.1. Soit $k \in \mathbb{Z}$. Si p divise k, alors p divise ka. Inversement, supposons que p divise ka. Le nombre p ne divise pas a et donc $a \wedge p = 1$ car p est un nombre premier. Ainsi, p divise ka et p est premier à a. D'après le théorème de Gauss, p divise k.

On a montré que : $\forall k \in \mathbb{Z},\ (p \text{ divise } ka \Leftrightarrow p \text{ divise } k)$.

VII.2.a. Pour tout $i \in [\![1, p-1]\!]$, un diviseur de i étant inférieur ou égal à i, p ne divise pas i. D'après la question précédente, p ne divise pas l'entier ia et donc α_i, le reste de la division euclidienne de ia par p, n'est pas nul.

Soit $(i, j) \in [\![1, p-1]\!]^2$ tel que $i \leqslant j$. Si $\alpha_i = \alpha_j$, alors p divise $ja - ia = (j-i)a$ et donc p divise $j - i$ d'après la question précédente. Puisque $j - i \in [\![0, p-1]\!]$, ceci impose $j - i = 0$ (d'après le début de la question) puis $i = j$. Par contraposition, si $i \neq j$, alors $\alpha_i \neq \alpha_j$.

On a montré que les restes α_i, $i \in [\![1, p-1]\!]$, sont non nuls et deux à deux distincts.

VII.2.b. Pour tout $i \in [\![1, p-1]\!]$, $1 \leqslant \alpha_i \leqslant p-1$. Donc, $\{\alpha_i,\ i \in [\![1, p-1]\!]\} \subset [\![1, p-1]\!]$. Mais de plus, les restes α_i, $1 \leqslant i \leqslant p-1$, sont deux à deux distincts. Donc, $\text{card}\{\alpha_i,\ i \in [\![1, p-1]\!]\} = p - 1 = \text{card}[\![1, p-1]\!] < +\infty$. On en déduit que $\{\alpha_i,\ i \in [\![1, p-1]\!]\} = [\![1, p-1]\!]$.

VII.3. $P = \prod_{k=1}^{p-1}(ka) = a^{p-1}\prod_{k=1}^{p-1} k = a^{p-1}(p-1)!$. D'autre part, puisque l'application $i \mapsto \alpha_i$ est une permutation de $[\![1, p-1]\!]$ d'après la question précédente, modulo p on a :

$$P = \prod_{i=1}^{p-1}(ia) \equiv \prod_{i=1}^{p-1}\alpha_i = \prod_{k=1}^{p-1} k = (p-1)!.$$

VII.4. Ainsi, $P = a^{p-1}(p-1)!$ et aussi $P \equiv (p-1)!$ [p]. On en déduit que $a^{p-1}(p-1)! \equiv (p-1)!$ [p]. Le nombre premier p divise donc $\left(a^{p-1}-1\right)(p-1)!$. Maintenant, p est premier à chacun des entiers k, $1 \leqslant k \leqslant p-1$, et donc p est premier à $(p-1)!$. D'après le théorème de Gauss, p divise $a^{p-1}-1$ et finalement $a^{p-1} \equiv 1$ [p].

VII.5. Le nombre 29 est premier (car n'est divisible ni par 2, ni par 3, ni par 5, qui sont les nombres premiers inférieurs ou égaux à sa racine). Donc, pour tout élément a de $[\![1,28]\!]$, $a^{28} = a^{29-1} \equiv 1$ [29].
Ainsi, pour tout $a \in [\![1,28]\!]$, $f_{28}(a) = 1$ (et $f_{28}(0) = 0$). La fonction f_{28} n'est pas une bonne fonction de cryptage.

Soit $a \in [\![1,28]\!]$. En multipliant par a les deux membres de la congruence $a^{28} \equiv 1$ [29], on obtient $a^{29} \equiv a$ [29]. Cette dernière congruence reste vraie quand $a = 0$ et donc : $\forall a \in [\![0,28]\!]$, $f_{29}(a) = a$. L'application f_{29} est donc l'identité de $[\![0,28]\!]$. La fonction f_{29} est une fonction de codage correcte mais sans intêret.

VII.6. Soient k et l deux entiers naturels non nuls tels que $k \equiv l$ [28] et $k \leqslant l$. Posons $l = k + 28q$ où $q \in \mathbb{N}$.

Soit $a \in [\![1,28]\!]$ (donc a est premier à 29).

$$\begin{aligned} a^l &= a^{k+28q} = a^k \times \left(a^{28}\right)^q \\ &\equiv a^k \times 1^q \ [29] \text{ (d'après le petit théorème de Fermat)} \\ &\equiv a^k \ [29]. \end{aligned}$$

Ainsi, les restes de la division euclidienne de a^k et a^l par 29 sont les mêmes et donc $f_k(a) = f_l(a)$. Cette dernière égalité reste vraie quand $a = 0$ car $f_k(0) = f_l(0) = 0$.

Finalement, si $k \equiv l$ [28], pour tout $a \in [\![0,28]\!]$, $f_k(a) = f_l(a)$ puis $f_k = f_l$.

VIII.

VIII.1. Puisque x est premier à 29, $x^{28} \equiv 1$ [29] d'après le petit théorème de Fermat. Mais alors, $\mathscr{E} = \left\{k \in \mathbb{N}^* / \ x^k \equiv 1 \ [29]\right\}$ est une partie non vide de $\mathbb{N}$ (et même de $\mathbb{N}^*$). A ce titre, $\mathscr{E}$ admet un plus petit élément que l'on note $o(x)$. Par définition, $o(x) \in \mathbb{N}^*$ et $x^{o(x)} \equiv 1$ [29]. Enfin, $28 \in \mathscr{E}$ et donc $o(x) \leqslant 28$.

VIII.2. Soit k un entier naturel. La division euclidienne de k par $o(x)$ (qui n'est pas nul) s'écrit $k = o(x) \times q + r$ avec $q \in \mathbb{N}$ et $r \in [\![0, o(x)-1]\!]$.
Ensuite, $x^k = x^{o(x)\times q + r} = x^r \times \left(x^{o(x)}\right)^q$ puis $x^k \equiv x^r$ [29]. Si $r = 0$, $x^k \equiv 1$ [29] et si $r \in [\![1, o(x)-1]\!]$ (si $o(x) = 1$, il n'y a plus rien à faire), alors $x^k \not\equiv 1$ [29] par définition de $o(x)$.

En résumé, $x^k \equiv 1$ [29] si et seulement si $r = 0$ ce qui équivaut à $o(x)$ divise k.

VIII.3. Puisque $x^{28} \equiv 1$ [29], $o(x)$ est un diviseur de 28.

VIII.4. Algorithme en langage Python.

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

On note que ce programme est très peu économe en opérations car
1) il suffit juste de tester pour $k \in \{1,2,4,7,14,28\}$
2) on recalcule x^k à chaque fois alors qu'il faudrait garder la valeur de x^k en mémoire pour n'avoir plus qu'une multiplication à effectuer pour passer à x^{k+1}.

D'autre part, le programme ne contient pas de test d'arrêt si on a rentré par erreur une valeur de x divisible par 29.

VIII.5.

VIII.5.a. $28 = 2^2 \times 7$ a $(2+1)(1+1) = 6$ diviseurs à savoir 1, 2, 4, 7, 14 et 28.

VIII.5.b. Si $x^{14} \equiv 1$ [29], alors $o(x) \leqslant 14$ et en particulier, $o(x) \neq 28$. Si $x^4 \equiv 1$ [29], alors $o(x) \leqslant 4$ et en particulier, $o(x) \neq 28$.
Ainsi, si $x^{14} \equiv 1$ [29] ou $x^4 \equiv 1$ [29], alors $o(x) \neq 28$.

VIII.5.c. Supposons maintenant $x^{14} \not\equiv 1$ [29] et $x^4 \not\equiv 1$ [29]. L'ordre x ne peut plus être que 1, 2, 7 ou 28.
Si $o(x) = 1$, alors $x \equiv 1$ [29], puis $x^4 \equiv 1$ [29] ce qui est faux.
Si $o(x) = 2$, alors $x^2 \equiv 1$ [29], puis $x^4 = \left(x^2\right)^2 \equiv 1$ [29] ce qui est faux.
Si $o(x) = 7$, alors $x^7 \equiv 1$ [29], puis $x^{14} = \left(x^7\right)^2 \equiv 1$ [29] ce qui est faux.

Il ne reste plus que $o(x) = 28$. En résumé, $o(x) = 28 \Leftrightarrow x^4 \not\equiv 1\ [29]$ et $x^{14} \not\equiv 1\ [29]$.

VIII.5.d. $2^4 = 16 \not\equiv 1\ [29]$. $2^{14} = 16\,384 = 564 \times 29 + 28$ puis $2^{14} \equiv 28\ [29]$ et en particulier, $2^{14} \not\equiv 1\ [29]$. D'après la question précédente, $o(2) = 28$ ou encore 2 est primitif modulo 29.

IX. On pose $(\mathbb{Z}/29\mathbb{Z})^* = (\mathbb{Z}/29\mathbb{Z}) \setminus \{\overline{0}\}$.
Pour tout $k \in [\![1, 28]\!]$, 2^k n'est pas divisible par 29 et donc $\left\{\overline{2^k},\ 1 \leqslant k \leqslant 28\right\} \subset (\mathbb{Z}/29\mathbb{Z})^*$. Vérifions alors que les classes $\overline{2^k}$, $1 \leqslant k \leqslant 28$, sont deux à deux distinctes.

Soit $(k, l) \in [\![1, 28]\!]^2$ tel que $k \leqslant l$.

$$\begin{aligned}\overline{2^l} = \overline{2^k} &\Rightarrow 2^l \equiv 2^k\ [29] \Rightarrow 2^l - 2^k \equiv 0\ [29] \Rightarrow 2^k\left(2^{l-k} - 1\right) \equiv 0\ [29]\\ &\Rightarrow 29 \text{ divise } 2^k\left(2^{l-k} - 1\right).\end{aligned}$$

Puisque 29 est 2^k sont premiers entre eux, le théorème de Gauss permet d'affirmer que 29 divise $2^{l-k} - 1$ et donc que $2^{l-k} \equiv 1\ [29]$. Mais $l - k$ est un élément de $[\![0, 27]\!]$ et puisque 2 est d'ordre 28, il ne reste plus que $l - k = 0$ et donc $k = l$. Ceci montre que les classes $\overline{2}^k = \overline{2^k}$, $0 \leqslant k \leqslant 27$, sont deux à deux distinctes.

Ainsi, $\left\{\overline{2}^k,\ 0 \leqslant k \leqslant 27\right\} \subset (\mathbb{Z}/29\mathbb{Z})^*$ et d'autre part, $\text{card}\left\{\overline{2}^k,\ 0 \leqslant k \leqslant 27\right\} = 28 = \text{card}\,(\mathbb{Z}/29\mathbb{Z})^* < +\infty$. On en déduit que $\left\{\overline{2}^k,\ 0 \leqslant k \leqslant 27\right\} = (\mathbb{Z}/29\mathbb{Z})^*$. Ceci signifie que le groupe $\left((\mathbb{Z}/29\mathbb{Z})^*, \overline{\times}\right)$ est cyclique et que 2 est un générateur de ce groupe.

X. Tout ou presque a été établi à la question précédente :

X.1. Pour tout $k \in [\![1, 28]\!]$, $\beta_k \neq 0$ puis $\beta_k \in S$ et donc φ est une application de S dans S.

X.2. Déjà fait à la question IX.

X.3. Egalement fait dans la question IX. On a vu que si $(k, k') \in [\![1, 28]\!]^2$ est tel que $k \leqslant k'$ et $2^{k'-k} - 1$ est divisible par 29, alors $k = k'$.
Ainsi, $\forall (k, k') \in S^2$, $(\varphi(k) = \varphi(k') \Rightarrow k = k')$. φ est donc une application injective de l'ensemble fini S dans lui-même. On en déduit que φ est une bijection.

X.4. Mais alors, $\forall y \in S$, $\exists! x \in S /\ \varphi(x) = y$ ou encore $\forall y \in S$, $\exists! x \in S /\ y \equiv 2^x\ [29]$.

XI.

XI.1. Soient $y \in S$ puis $z \in \mathbb{Z}$. Si $z \equiv 0\ [29]$, alors $z^k \equiv 0\ [29]$ et donc $z^k \not\equiv y\ [29]$. Donc, $z \notin 29\mathbb{Z}$. Soit alors r le reste de la division euclidienne de z par 29. r est un élément de S et $z^k \equiv r^k\ [29]$ puis $z^k \equiv y\ [29] \Leftrightarrow r^k \equiv y\ [29]$. On se ramène donc au cas où $z \in S$.

XI.2. Soit $(x, t) \in S^2$ tel que $y \equiv 2^x\ [29]$ et $z = 2^t\ [29]$ (ou encore soient $x = \varphi^{-1}(y)$ et $t = \varphi^{-1}(z)$).

$$z^k \equiv y\ [29] \Leftrightarrow 2^{kt} \equiv 2^x\ [29] \Leftrightarrow 2^x\left(2^{kt-x} - 1\right) \equiv 0\ [29] \Leftrightarrow 29 \text{ divise } 2^x\left(2^{kt-x} - 1\right).$$

Ensuite, si 29 divise $2^{kt-x} - 1$, alors z divise $2^x\left(2^{kt-x} - 1\right)$. Inversement, si 29 divise $2^x\left(2^{kt-x} - 1\right)$, puisque $29 \wedge 2^x = 1$, d'après le théorème de Gauss, 29 divise $2^{kt-x} - 1$. En résumé,

$$z^k \equiv y\ [29] \Leftrightarrow 29 \text{ divise } 2^{kt-x} - 1 \Leftrightarrow 2^{kt-x} \equiv 1\ [29].$$

La division euclidienne de $kt - x$ par 28 s'écrit $kt - x = 28q + r$ avec $0 \leqslant r \leqslant 27$. Puisque 2 est d'ordre 28 modulo 29,

$$2^{kt-x} = \left(2^{28}\right)^q \times 2^r \equiv 2^r\ [29]$$

puis, par définition de l'ordre de 2,

$$2^{kt-x} \equiv 1\ [29] \Leftrightarrow 2^r \equiv 1\ [29] \Leftrightarrow r = 0 \Leftrightarrow kt - x \text{ est divisible par } 28.$$

XI.3.a. D'après le théorème de Bézout, l'équation $(*)$ admet au moins une solution (a_0, b_0) dans $\mathbb{Z}^2$ si et seulement si k et 28 sont premiers entre eux.

XI.3.b. On suppose donc $k \wedge 28 = 1$. Soit $(a, b) \in \mathbb{Z}^2$.

$$ak + 28b = 1 \Leftrightarrow ak + 28b = a_0k + 28b_0 \Leftrightarrow k(a - a_0) = 28(b_0 - b).$$

Si (a,b) est un couple solution de $(*)$, nécessairement 28 divise $28(b_0-b)=k(a-a_0)$. Puisque $28\wedge k=1$, le théorème de Gauss permet d'affirmer que 28 divise $a-a_0$. Donc, il existe nécessairement un entier relatif q tel que $a-a_0=28q$ puis $a=a_0+28q$. De même, il existe nécessairement un entier relatif q' tel que $b_0-b=kq'$ ou encore $b=b_0-28q'$.

Soient alors $(q,q')\in\mathbb{Z}^2$ puis $a=a_0+28q$ et $b=b_0-28q'$.

$$ak+28b=1\Leftrightarrow k(a-a_0)=28(b_0-b)\Leftrightarrow k\times 28\times q=28\times k\times q'\Leftrightarrow q=q'.$$

Les solutions de $(*)$ dans $\mathbb{Z}^2$ sont les couples de la forme (a_0+28q,b_0-kq), $q\in\mathbb{Z}$.

XI.3.c. Soient $q\in\mathbb{Z}$ puis $(a,b)=(a_0+28q,b_0-kq)$.

$$0\leqslant a\leqslant 28\Leftrightarrow 0\leqslant a_0+28q\leqslant 28\Leftrightarrow -\frac{a_0}{28}\leqslant q\leqslant -\frac{a_0}{28}+1.$$

Soit $q=\left\lfloor -\frac{a_0}{28}\right\rfloor+1$. Alors, q est un entier relatif tel que $-\frac{a_0}{28}\leqslant q\leqslant -\frac{a_0}{28}+1$ et donc (a,b) est une solution de $(*)$ telle que $0\leqslant a\leqslant 28$. De plus, si $a=0$ alors $28b=1$ ce qui est impossible. Donc, (a,b) est une solution de $(*)$ telle que $1\leqslant a\leqslant 28$. Ceci montre l'existence du couple (a_1,b_1).

Vérifions l'unicité du couple (a_1,b_1). Soit $(a,b)\in\mathbb{Z}^2$ une solution de $(*)$ telle que $1\leqslant a\leqslant 28$. Alors $ka+28b=ka_1+28b_1$ puis $k(a-a_1)=28(b_1-b)$. D'après le théorème de Gauss, $a-a_1$ est divisible par 28 et de plus $-27\leqslant a-a_1\leqslant 27$. Donc, $a-a_1\in 28\mathbb{Z}\cap[\![-27,27]\!]=\{0\}$ puis $a=a_1$ (puis $b=b_1$). Ceci montre l'unicité du couple (a_1,b_1).

XI.4. Soit $w\in R$. Si $w=0$, $f_{a_1}\circ f_k(w)=0=f_k\circ f_{a_1}(w)$. Dorénavant $w\in S$.
Posons $v=f_k(w)$ puis $u=f_k(v)$. $w^k\equiv v\ [29]$ puis $v^{a_1}\equiv u\ [29]$. Mais alors, $u\equiv w^{ka_1}\ [29]$. De plus, $ka_1\equiv 1\ [28]$ et donc il existe $q\in\mathbb{Z}$ (et même $\mathbb{N}$) tel que $ka_1=1+28q$. Mais alors, modulo 29, puisque $\overline{w}\in(\mathbb{Z}/28\mathbb{Z})\setminus\{\overline{0}\}$, $w^{28}\equiv 1\ [29]$ puis

$$u\equiv w^{ka_1}=w\times\left(w^{28}\right)^q\equiv w\times(1)^q=w.$$

Mais alors, $u=w$ (puisque u et w sont dans S). On a montré que $f_{a_1}\circ f_k(w)=w$ puis immédiatement, $f_k\circ f_{a_1}(w)=w$ car $\left(w^k\right)^{a_1}=(w^{a_1})^k$.

XI.5. Ainsi, $f_{a_1}\circ f_k=f_k\circ f_{a_1}=Id_R$. Ceci montre que f_k est bijective et que $f_k^{-1}=f_{a_1}$. La fonction f_{a_1} permet donc le décryptage d'un cryptage par f_k.

XII. $3\times 19-28\times 2=57-56=1$ avec $1\leqslant 19\leqslant 28$. Donc, si $k=3$, alors $a_1=19$ puis $f_3^{-1}=f_{19}$. Tout message crypté par f_3 peut être décrypté par f_{19}.

XIII. On sait déjà que si k est premier à 28, f_k est bijective puis que tout message crypté par f_k peut être décrypté par $f_k^{-1}=f_{a_1}$ (le cas $k=1$ est contenu dans ce cas mais le décyptage est assez facile à réaliser). Il reste à analyser le cas où k n'est pas premier à 28.

D'après la question VII.6., il suffit d'envisager le cas où $k\in[\![1,28]\!]$ et non premier à 28 (c'est-à-dire $k\in\{2,4,6,7,8,10,12,14,16,18,20,21,22,24,26,28\}$).
Soit $d\in[\![2,27]\!]$ un diviseur commun à k et 28. Posons $28=dq$ où $q\in[\![2,27]\!]$ et $k=dq'$ où $q'\in[\![2,27]\!]$.

$$\left(2^{q'}\right)^k=2^{dqq'}=\left(2^{dq'}\right)^q\equiv 1[29].$$

Donc, si w est l'élément de $[\![1,28]\!]$ tel que $2^{q'}\equiv w\ [29]$, $f_k(w)=1=f_k(1)$. Si de plus $w=1$, alors $2^{q'}\equiv 1\ [29]$ puis q' est un multiple de 28, l'ordre de 2, ce qui contredit $q'\in[\![1,27]\!]$. Donc, $w\neq 1$ et $f_k(w)=f_k(1)$. Dans ce cas, f_k n'est pas injective et ne permet donc pas de décrypter un message.

En résumé, on peut décrypter tout message crypté par f_k si et seulement si $k\wedge 29=1$. Si on se contente des entiers k de $[\![1,28]\!]$, l'ensemble de ces entiers k est $\{1,3,5,9,11,13,15,19,19,23,25,27\}$.

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

XIV. Première méthode.

XIV.1. Pour obtenir chaque ligne, on multiplie la précédente par la ligne 2 puis on effectue une division euclidienne. Dans les références à écrire, l'une des références à la ligne 2 est absolue. D'où la formule à recopier : =MOD(D2*D$2 ;29)

XIV.2. On a ainsi effectué 18 multiplications et 18 divisions euclidiennes.

XV. Deuxième méthode.

XV.1. La formule à recopier de la case D3 à la case AD6 est =MOD(D2^2 ;29).

XV.2. Soit $x \in \mathbb{R}$. Modulo 19,

$$f_{19}(x) \equiv x^{19} = x^{2^4+2+1} = \left(\left(\left(x^2\right)^2\right)^2\right)^2 \times x^2 \times x \equiv \left(\left(\left(x^2\right)^2\right)^2\right)^2 \times f_2(x) \times x,$$

où de plus, $f_2(x) \equiv x^2$ puis $f_2\left(f_2(x)\right) \equiv \left(x^2\right)^2$ puis ... $f_2 \circ f_2 \circ f_2 \circ f_2(x) \equiv \left(\left(\left(x^2\right)^2\right)^2\right)^2$. Finalement,

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

XV.3. En case D7, on rentre donc =MOD(D2*D3*D6 ;29), formule que l'on recopie ensuite sur la ligne 7.

XV.4. Dans chaque colonne, on a effectué 6 multiplication et 5 divisions euclidiennes.

XVI. Troisième méthode.

XVI.1. On remplit les lignes 3 et 4. En case D3, on écrit la formule =MOD(D2*D2*D2 ;29) que l'on recopie sur les lignes 3 et 4.

XVI.2. En case D5, on écrit alors =MOD(D4*D4*D2 ;29), formule que l'on recopie dans la ligne 5.

XVI.3. Dans chaque colonne, on a effectué 6 multiplications et 3 divisions euclidiennes.

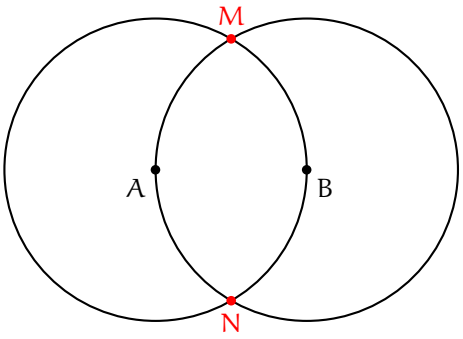
XVI.4. La troisième méthode semble la plus performante. On peut penser qu'une seule division euclidienne en dernière ligne doit être suffisante mais ce serait oublier que les puissances successives dépassent la capacité du tableur. Faire des divisions euclidiennes intermédiaires permet, comme annoncé en VI. de ne pas avoir l'affichage ♯NOMBRE !.

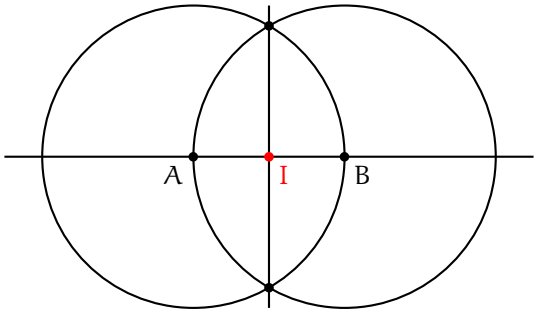
Problème n° 2

Partie A : constructions à la règle et au compas

I.

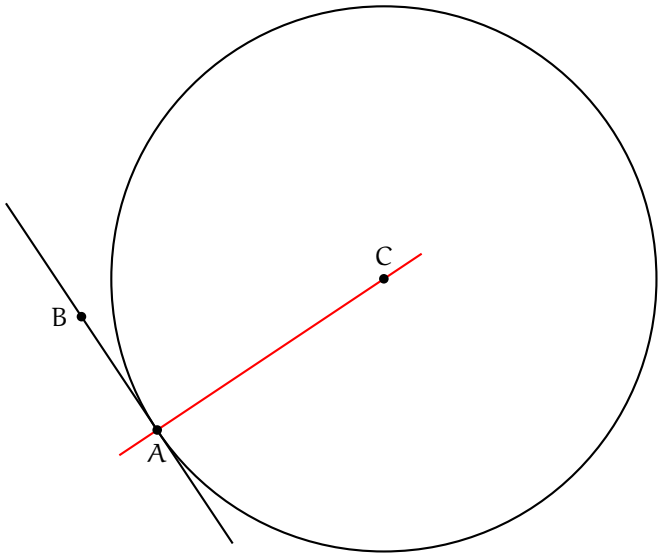
I.1. On trace le cercle de centre A et de rayon AB et le cercle de centre B et de rayon AB.
Ces cercles se coupent en deux points distincts M et N (les points M et N sont les deux points du plan tels que les triangles AMB et ANB soient équilatéraux).
Les points M et N sont deux nouveaux points constructibles puis la droite (MN) est constructible. Puisque les points M et N sont distincts et à égale distance des points A et B (car AM = BM = AB et AN = BN = AB), la droite (MN) est la médiatrice du segment [AB] qui est donc constructible à la règle et au compas.
Enfin, le milieu I du segment [AB] est le point d'intersection des deux droites constructibles (MN) et (AB). Le milieu I du segment [AB] est donc constructible.



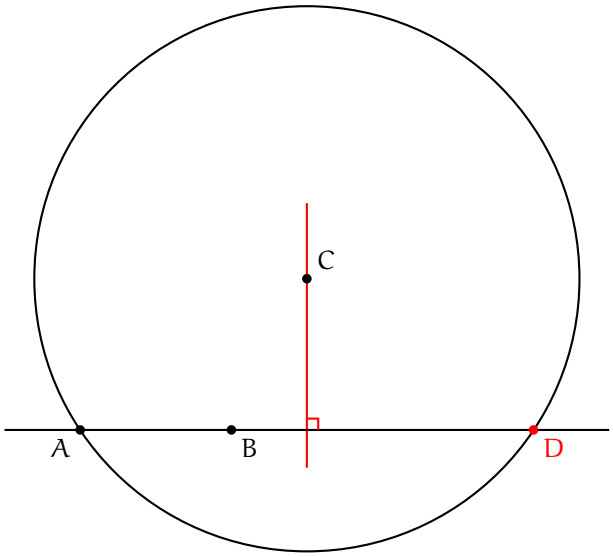


I.2. Puisque A ≠ B, l'un des deux points A ou B est distinct de C. On supposera sans perte de généralité que A ≠ C.
On trace le cercle $\mathscr{C}$ de centre C et de rayon AC puis la droite (AB). La droite (AB) et le cercle $\mathscr{C}$ ont en commun le point A. Deux cas de figure se présentent alors :

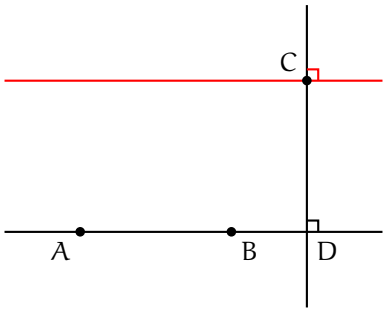
1er cas. A est l'unique point commun à la droite (AB) et au cercle $\mathscr{C}$. C'est le cas où la droite (AB) est tangente au cercle $\mathscr{C}$ en A. Dans ce cas, la droite (AC) (qui porte le rayon [AC]) est perpendiculaire à la tangente (AB) et est donc la perpendiculaire à (AB) passant par C. Les points A et C étant constructibles, il en est de même de la droite (AC).



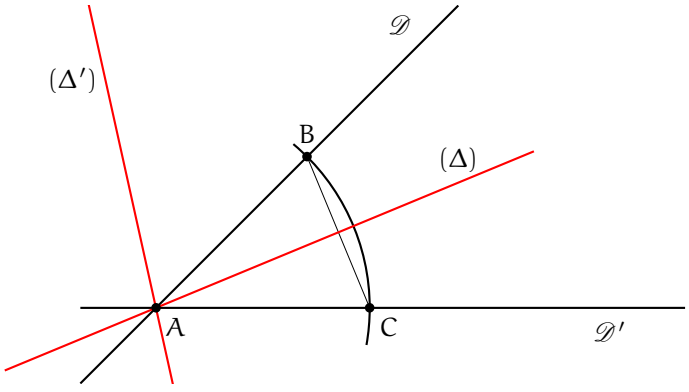
2ème cas. La droite (AB) et le cercle $\mathscr{C}$ ont un deuxième point en commun que l'on note D avec D ≠ A. Puisque les points A, B et C sont constructibles, le point D est constructible. Le point C est à égale distance de A et D et donc le point C est sur la médiatrice du segment [AB]. La médiatrice du segment [AB] est la perpendiculaire à la droite [AB] passant pas C. Cette perpendiculaire est donc constructible d'après la question I.1.



I.3. Si C appartient à la droite (AB), la parallèle à la droite (AB) passant par C est directement la droite (AB). Cette droite est constructible puisque les points A et B le sont.
Sinon, le point C n'appartient pas à la droite (AB). La perpendiculaire à (AB) passant par C est constructible d'après la question précédente. Elle coupe la droite (AB) en un point D, distinct de C. Le point D est constructible en tant qu'intersection de deux droites constructibles.
La parallèle à (AB) passant par C est la perpendiculaire à (CD) (avec $C \neq D$) passant par C. Cette droite est constructible car C et D le sont. Mais alors, la parallèle à (AB) passant par C, qui est la perpendiculaire à (CD) passant par C, est constructible.

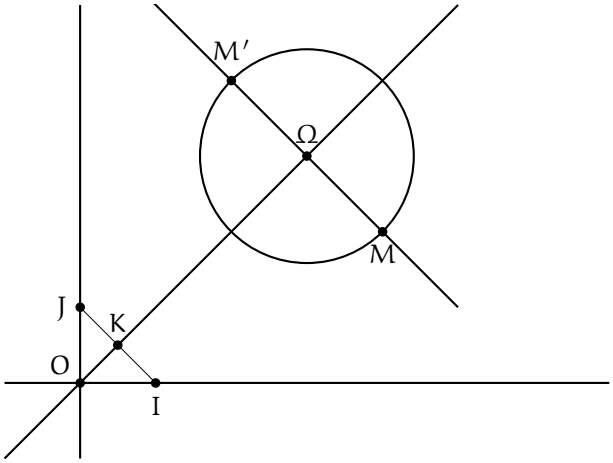


I.4. Puisque $\mathcal{D}$ est une droite constructible, il existe un point constructible B distinct de A tel que $\mathcal{D} = (AB)$. Le cercle $\mathscr{C}$ de centre A et de rayon AB est constructible. Il coupe la droite $\mathcal{D}'$ en un point C qui est constructible puisque $\mathcal{D}'$ et $\mathscr{C}$ le sont. Puisque $AB = AC$, la médiatrice du segment [BC] est l'une des deux bissectrices (Δ). Cette bissectrice est donc constructible. L'autre bissectrice (Δ') est la perpendiculaire à (Δ) passant par A. Elle est constructible.



II. Soit $M(x,y)$ un point constructible. Puisque x est l'abscisse de M, x est un nombre constructible. Vérifions que y est l'abscisse d'un point constructible. Pour cela, vérifions que le symétrique de M par rapport à la droite d'équation $y=x$, à savoir le point $M'(y,x)$, est constructible. On note (D) la droite d'équation $y=x$.

La médiatrice du segment [IJ], à savoir la droite (D) est constructible. Le point d'intersection K de cette médiatrice et de la droite (IJ) est donc constructible puis la perpendiculaire (Δ) à la droite (OK) passant par M est constructible d'après la question I.2. Le point d'intersection Ω de (Δ) et (D) est constructible puis le cercle de centre Ω et de rayon ΩM est constructible. Le point M' appartient à l'intersection de ce cercle et de la droite (Δ). Le point M' est donc constructible.



Mais alors, l'abscisse y de M' est un nombre constructible.

III. Soit x un réel constructible. x est l'abscisse d'un point constructible $M(x,y)$. La parallèle à la droite constructible (OJ) passant par M est constructible d'après I.3. L'intersection de cette parallèle avec la droite constructible (OI), à savoir le point $M_0(x,0)$, est constructible. Mais alors, le point de coordonnées $(0,x)$ est aussi constructible d'après la question II.

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

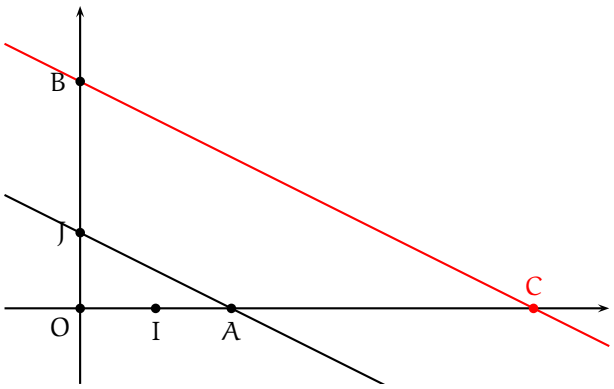
IV.1. Puisque x est constructible, le point A de coordonnées $(x,0)$ est constructible d'après la question III. Le cercle de centre O et de rayon OA est donc constructible. Ce cercle coupe la droite constructible (OI) en A et en le point B de coordonnées $(-x,0)$. Le point B est donc constructible puis le réel $-x$ est constructible.

IV.2. Les points A et B de coordonnées respectives $(x,0)$ et $(y,0)$ sont constructibles. Le cercle de centre A et de rayon OB est donc constructible. Ce cercle coupe la droite constructible (OI) en les points de coordonnées respectives $(x-y,0)$ et $(x+y,0)$. Ces deux points sont ainsi constructibles puis les réels $x+y$ et $x-y$ sont constructibles.

IV.3. Si $x=1$ ou $y=1$, le résultat est immédiat. Dorénavant, $x\neq 1$ et $y\neq 1$.

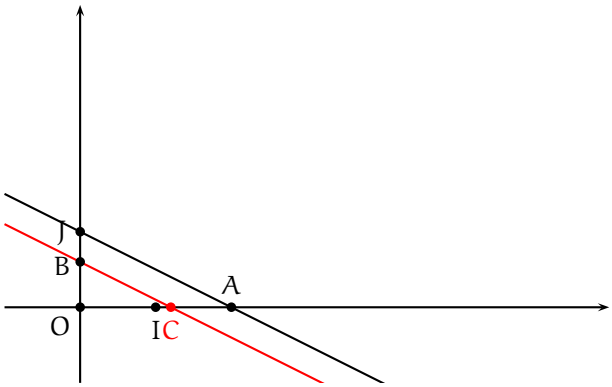
On construit (Δ), la parallèle à la droite constructible (JA) passant par la point constructible B. Puisque le point A appartient à la droite (OI) et pas le point J, la droite (AJ) n'est pas parallèle à la droite (OI) et il en est de même de la droite (Δ). Mais alors la droite constructible (Δ) coupe la droite constructible (OI) en un point C. Le point C est ainsi constructible puis son abscisse x_C est un nombre constructible. Il y a deux cas de figure.

1er cas. On suppose $y>1$.



Dans le triangle OBC, le point J appartient au segment [OB] (car $y > 1$), le point A appartient à la droite (OC) et la droite (AJ) est parallèle à la droite (BC). D'après le théorème de Thales, $\dfrac{OC}{OA} = \dfrac{OB}{OJ}$ ce qui fournit $\dfrac{x_C}{x} = \dfrac{y}{1}$ puis $x_C = xy$. Le réel xy est donc constructible.

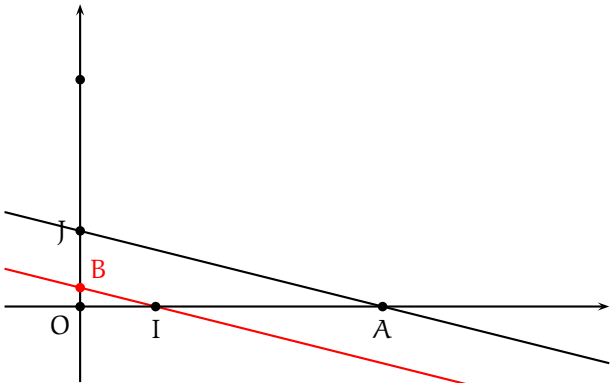
2ème cas. On suppose $0 < y < 1$.



Dans le triangle OAJ, le point B appartient au segment [OJ] (car $y < 1$), le point C appartient à la droite (OA) et la droite (BC) est parallèle à la droite (AJ). D'après le théorème de Thales, $\dfrac{OC}{OA} = \dfrac{OB}{OJ}$ ce qui fournit $\dfrac{x_C}{x} = \dfrac{y}{1}$ puis $x_C = xy$. Le réel xy est donc constructible.

Dans tous les cas, le réel xy est constructible.

IV.4. Soit x un réel strictement constructible. Vérifions que $\dfrac{1}{x}$ est constructible. On note A le point de coordonnées $(x, 0)$. On construit la parallèle à (AJ) passant par I. Elle coupe la droite (OJ) en un point B



Sans détailler les cas $0 < x < 1$ et $x > 1$, le théorème de Thales permet d'affirmer que $\dfrac{OB}{OJ} = \dfrac{OI}{OA}$ et donc $OB = \dfrac{1}{x}$. Le réel $\dfrac{1}{x}$ est donc constructible.

Si maintenant, x et y sont deux réels strictement positifs constructibles, alors $\dfrac{x}{y} = x \times \dfrac{1}{y}$ est constructible d'après ce qui précède.

V. Soient x et y deux réels constructibles. Si $x = 0$ ou $y = 0$, alors $x + y$, $x - y$ et xy sont constructibles. Si $x = 0$ et $y \neq 0$, $\dfrac{x}{y}$ est constructible. Dorénavant, $x \neq 0$ et $y \neq 0$.

On note que si x est strictement négatif et constructible, alors $-x$ est constructible par une construction analogue à celle de IV.1.

• Si $x > 0$ et $y > 0$, $x + y$, $x - y$, xy et $\dfrac{x}{y}$ sont constructibles d'après les questions IV.2., IV.3. et IV.4.

• Si $x < 0$ et $y < 0$, $-x$ et $-y$ sont deux réels strictement positifs constructibles. Donc, $-(x + y) = (-x) + (-y)$, $-x + y = (-x) - (-y)$, $xy = (-x)(-y)$ et $\dfrac{x}{y} = \dfrac{-x}{-y}$ sont constructibles puis $x + y = -(-(x + y))$ et $x - y = -(-x + y)$ (et toujours xy et $\dfrac{x}{y}$) sont constructibles.

• Si $x > 0$ et $y < 0$, x et $-y$ sont deux réels strictement positifs constructibles. Mais alors $x-y = x+(-y)$, $x+y = x-(-y)$, $-xy = x(-y)$ et $-\dfrac{x}{y} = \dfrac{x}{-y}$ sont constructibles puis $x+y$, $x-y$, xy et $\dfrac{x}{y}$ sont constructibles en prenant l'opposé de certains des nombres précédents.

• Si $x < 0$ et $y > 0$, $-x$ et y sont deux réels strictement positifs constructibles. Mais alors $-x+y$, $-(x+y) = -x-y$, $-xy = (-x)y$ et $-\dfrac{x}{y} = \dfrac{-x}{y}$ sont constructibles puis $x+y$, $x-y$, xy et $\dfrac{x}{y}$ sont constructibles en prenant l'opposé de certains des nombres précédents.

On a montré que pour tous nombres constructibles x et y, les réels $x+y$, $x-y$, xy et, si $y \neq 0$, $\dfrac{x}{y}$, sont constructibles.

VI.

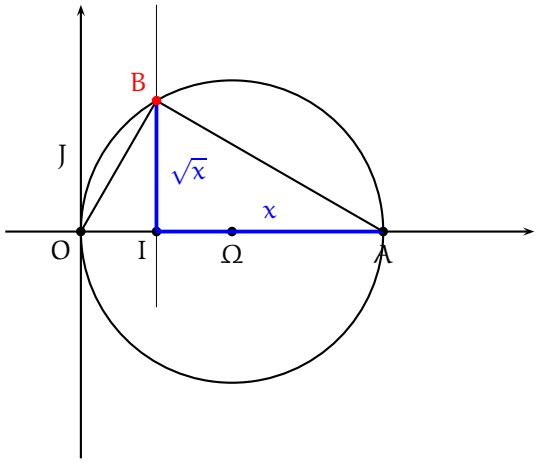
VI.1. Soit x un réel strictement positif constructible. 1 est constructible (car 1 est l'abscisse du point I) et x est constructible. Donc, $x+1$ est constructible d'après V. puis le point $A(x+1, 0)$ est constructible d'après III.

VI.2. Le milieu Ω du segment [OA] est constructible d'après I.1. Le cercle $\mathcal{C}$ de diamètre [OA] est encore le cercle de centre Ω et de rayon ΩA. On en déduit que ce cercle est constructible.

VI.3. Le cercle $\mathcal{C}$ est constructible et la perpendiculaire à la droite (OI) passant par I est constructible. Donc, B est constructible.

VI.4. Dans le triangle OIB, rectangle en I, $\tan(\theta) = \dfrac{BI}{OI} = BI$.

Ensuite, puisque B appartient au cercle de diamètre [OA], le triangle OAB est rectangle en B. Donc, $\widehat{IAB} = \pi - \left(\dfrac{\pi}{2} + \widehat{IOB}\right) = \dfrac{\pi}{2} - \theta$. Dans le triangle BIA, rectangle en I, $\tan\left(\dfrac{\pi}{2} - \theta\right) = \dfrac{BI}{IA} = \dfrac{BI}{x}$.



L'égalité, $\tan(\theta) = \dfrac{1}{\tan\left(\dfrac{\pi}{2} - \theta\right)}$ fournit $BI = \dfrac{x}{BI}$ puis $BI^2 = x$ puis $BI = \sqrt{x}$.

VI.5 Le point constructible B a pour coordonnées $\left(1, \sqrt{x}\right)$. D'après V., son ordonnée, à savoir $\sqrt{x}$, est un nombre constructible.

VII. Montrons par récurrence que pour tout $n \in \mathbb{N}^*$, n est constructible.
- 1 est constructible car abscisse du point constructible I.
- Soit $n \geqslant 1$. Supposons n constructible. Alors le point de coordonnées $(n+1, 0)$ est constructible d'après VI.1. et donc $n+1$ est constructible d'après II.

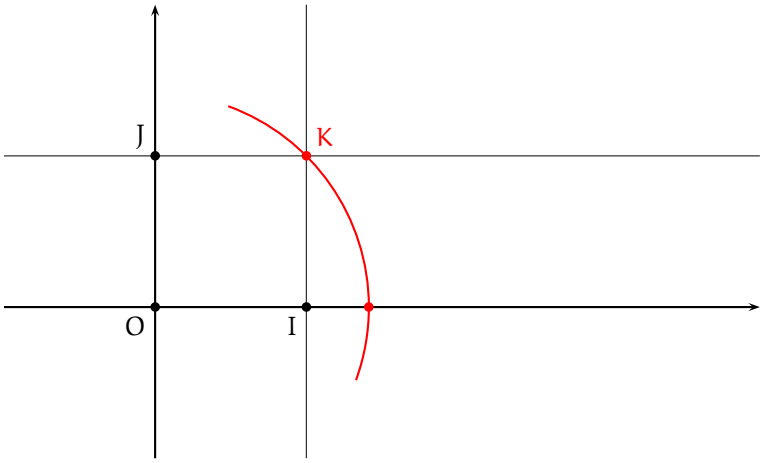
On a montré par récurrence que pour tout $n \in \mathbb{N}^*$, n est constructible.

On en déduit encore que pour tout $n \in \mathbb{N}^*$, $-n$ est constructible d'après IV.1. puis, en tenant compte du fait que 0 est constructible, on a montré que pour tout $p \in \mathbb{Z}$, p est constructible.

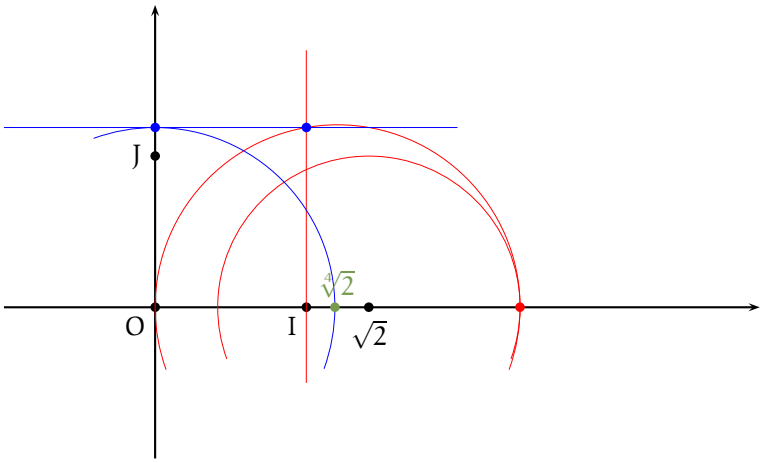
D'après V., pour tout $p \in \mathbb{Z}$ et tout $q \in \mathbb{N}^*$, $\dfrac{p}{q}$ est constructible et finalement, tout nombre rationnel est constructible.

VIII. 2 est constructible et donc $\sqrt{2}$ est constructible puis $\sqrt[4]{2} = \sqrt{\sqrt{2}}$ est constructible.

Pour construire $\sqrt{2}$ puis le point $\left(\sqrt{2},0\right)$, on part des points O, I et J. La parallèle à (OJ) passant par I et la parallèle à (OI) passant par I se coupe en le point $K(1,1)$. Le cercle de centre O passant par K a pour rayon $OK=\sqrt{2}$. Le cercle de centre O et de rayon OK coupe la droite (OI) en le point de coordonnées $\left(\sqrt{2},0\right)$.



Le point de coordonnées $\left(\sqrt{2},0\right)$ est maintenant construit. On construit ensuite le point de coordonnées $\left(\sqrt{2}+1,0\right)$ puis le point de coordonnées $\left(1,\sqrt[4]{2}\right)$ (avec $\sqrt[4]{2}=\sqrt{\sqrt{2}}$) en suivant les étapes de la question VI. On obtient le point de coordonnées $\left(1,\sqrt[4]{2}\right)$. On construit ensuite le point de coordonnées $\left(0,\sqrt[4]{2}\right)$ puis on rabat au compas pour obtenir de point de coordonnées $\left(\sqrt[4]{2},0\right)$.



Partie B : polygones réguliers

IX.

IX.1. Soit $n\geqslant 3$. Soit z un nombre complexe non nul (0 n'est pas solution). Posons $z=re^{i\theta}$ où $r\in]0,+\infty[$ et $\theta\in\mathbb{R}$.

$$z^n=1\Leftrightarrow r^ne^{in\theta}=1\times e^0\Leftrightarrow r^n=1 \text{ et } \exists k\in\mathbb{Z}/\ n\theta=0+2k\pi\Leftrightarrow r=1 \text{ et } \exists k\in\mathbb{Z}/\ \theta=\frac{2k\pi}{n}$$
$$\Leftrightarrow \exists k\in\mathbb{Z}/\ z=e^{\frac{2ik\pi}{n}}.$$

Les solutions dans $\mathbb{C}$ de l'équation $z^n=1$ sont les nombres de la forme $\omega_k=e^{\frac{2ik\pi}{n}}$, $k\in\mathbb{Z}$.

Soit $k\in\mathbb{Z}$. La division euclidienne de k par n s'écrit $k=nq+r$ où $q\in\mathbb{Z}$ et $r\in[\![0,n-1]\!]$. Ensuite,

$$e^{\frac{2ik\pi}{n}}=e^{\frac{2i(qn+r)\pi}{n}}=e^{2iq\pi+\frac{2ir\pi}{n}}=e^{2iq\pi}\times e^{\frac{2ir\pi}{n}}=e^{\frac{2ir\pi}{n}}.$$

Donc, les solutions dans $\mathbb{C}$ de l'équation $z^n=1$ sont les nombres complexes de la forme $\omega_k=e^{\frac{2ik\pi}{n}}$, $k\in[\![0,n-1]\!]$.

Notons enfin que les nombres $e^{\frac{2ik\pi}{n}}$, $k \in [\![0, n-1]\!]$, sont deux à deux distincts par injectivité de l'application $\begin{array}{ccc} [0,2\pi[& \to & \mathbb{C} \\ \theta & \mapsto & e^{i\theta} \end{array}$.

Finalement, l'équation $z^n = 1$ admet dans $\mathbb{C}$ exactement n solutions deux à deux distinctes à savoir les nombres de la forme $\omega_k = e^{\frac{2ik\pi}{n}}$, $k \in [\![0, n-1]\!]$.

IX.2. Pour $k \in [\![0, n-1]\!]$, notons M_k le point d'affixe ω_k. Soit $k \in [\![0, n-1]\!]$.

$$OM_k = |\omega_k| = \left|e^{\frac{2ik\pi}{n}}\right| = 1.$$

Donc, $OM_0 = OM_1 = \ldots = OM_{n-1} = 1$. Ensuite, modulo 2π, en notant que $\omega_n = e^{2i\pi} = 1$ et donc que le point M_n d'affixe ω_n est le point M_0,

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

Donc, $\left(\widehat{\overrightarrow{OM_0}, \overrightarrow{OM_1}}\right) = \left(\widehat{\overrightarrow{OM_1}, \overrightarrow{OM_2}}\right) = \ldots = \left(\widehat{\overrightarrow{OM_{n-2}}, \overrightarrow{OM_{n-1}}}\right) = \left(\widehat{\overrightarrow{OM_{n-1}}, \overrightarrow{OM_0}}\right) = \frac{2\pi}{n}\ [2\pi]$.

On a montré que $M_0M_1 \ldots M_{n-1}$ est un polygone régulier.

X.

X.1. M_1 est le point de coordonnées $\left(\cos\left(\frac{2\pi}{n}\right), \sin\left(\frac{2\pi}{n}\right)\right)$. Si M_1 est constructible, ses coordonnées sont constructibles d'après II. et en particulier $\cos\left(\frac{2\pi}{n}\right)$ est constructible.

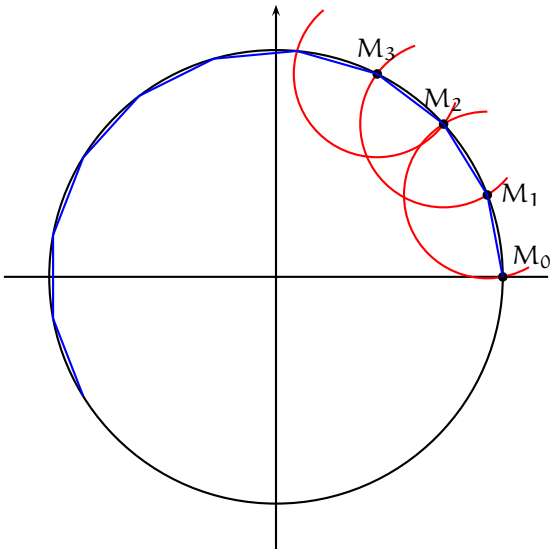
X.2. Si $\cos\left(\frac{2\pi}{n}\right)$ est constructible, alors le point B de coordonnées $\left(\cos\left(\frac{2\pi}{n}\right), 0\right)$ est constructible d'après III. Le point M_1 est alors constructible en tant que point commun au cercle de centre O et de rayon OI et de la perpendiculaire à (OI) passant par B.

XI. Si M_0, M_1, ..., M_{n-1}, sont constructibles, en particulier M_1 est constructible puis B est constructible d'après X.1. Inversement, supposons que B est constructible. Alors, M_1 est constructible d'après X.2. D'autre part, $M_0 = I$ est constructible. On note alors que pour $k \in [\![0, n-1]\!]$,

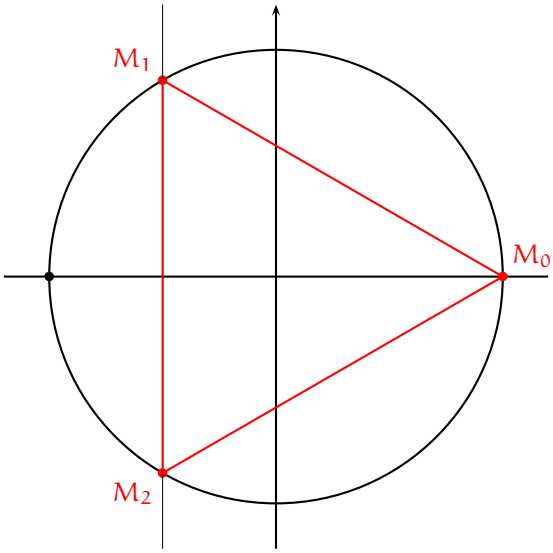
$$M_kM_{k+1} = \left|e^{\frac{2i(k+1)\pi}{n}} - e^{\frac{2ik\pi}{n}}\right| = \left|e^{\frac{(2k+1)i\pi}{n}}\left(e^{\frac{i\pi}{n}} - e^{-\frac{i\pi}{n}}\right)\right| = 2\sin\left(\frac{\pi}{n}\right).$$

Ainsi, pour tout $k \in [\![0, n-1]\!]$, $M_kM_{k+1} = M_0M_1 = IM_1$.

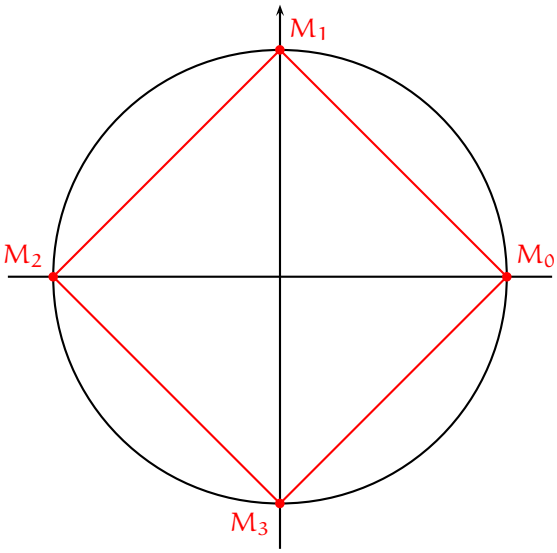
Par suite, M_2 est commun au cercle $\mathscr{C}_1$ de centre M_1 et de rayon IM_1 et au cercle $\mathbb{U}$ de centre O et de rayon OI. M_2 est donc constructible. Puis M_3 est commun au cercle $\mathscr{C}_2$ de centre M_2 et de rayon IM_1 et au cercle $\mathbb{U}$ de centre O et de rayon OI. M_3 est donc constructible. Puis, par récurrence, pour tout $k \in [\![0, n-1]\!]$, M_k est constructible à la règle et au compas en reportant à chaque fois au compas la distance IM_1.



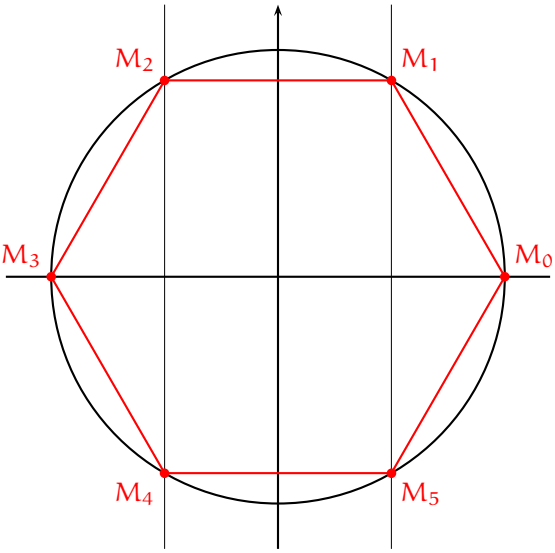
XII. Quand $n = 3$, B est le point de coordonnées $\left(-\frac{1}{2}, 0\right)$. Il est constructible car $-\frac{1}{2} \in \mathbb{Q}$. Donc, $M_0M_1M_2$ est constructible. On construit le point $I'(-1,0)$ puis la médiatrice du segment $[OI']$. Elle coupe le cercle de centre O et de rayon OI en M_1 et M_2.



Quand $n = 4$, B = O et donc B est constructible puis $M_0M_1M_2M_3$ est constructible. Sans autre commentaire, on obtient



Quand $n = 6$, B est le point de coordonnées $\left(\frac{1}{2}, 0\right)$. Il est constructible et donc, $M_0M_1M_2M_3M_4M_5$ est constructible. On construit la médiatrice de $[OI]$. Elle coupe $\mathbb{U}$ en M_1 et M_5. On construit le point $I'(-1,0)$, c'est-à-dire le point M_3 puis la médiatrice du segment $[OI']$. Elle coupe le cercle de centre O et de rayon OI en M_2 et M_4.



XIII.

XIII.1. D'après les formules d'Euler,

$$\omega + \overline{\omega} = e^{\frac{2i\pi}{5}} + e^{-\frac{2i\pi}{5}} = 2\cos\left(\frac{2\pi}{5}\right).$$

XIII.2. Puisque $\omega \neq 1$ (car $0 < \frac{2\pi}{5} < 2\pi$) et puisque $\omega^5 = 1$,

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

XIII.3. $\omega^4 = e^{\frac{8i\pi}{5}} = e^{\frac{8i\pi}{5}-2i\pi} = e^{-\frac{2i\pi}{5}} = \overline{\omega}$ puis $\alpha = \omega + \overline{\omega} = \omega + \omega^4$. Ensuite, en tenant compte de $\omega^5 = 1$,

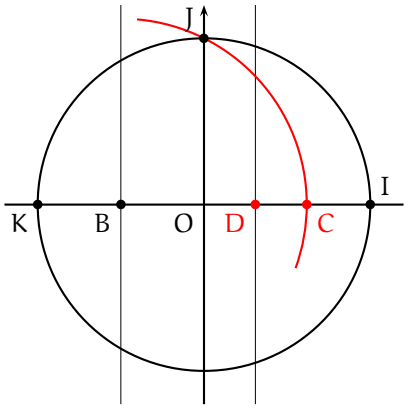
$$\alpha^2 = \left(\omega + \omega^4\right)^2 = \omega^2 + 2\omega^5 + \omega^8 = \omega^2 + 2 + \omega^3.$$

XIII.4. $\alpha + \alpha^2 = \omega + \omega^4 + \omega^2 + \omega^3 + 2 = -1 + 2 = 1$ et donc $-1 + \alpha + \alpha^2 = 0$. Ainsi, α est l'une des deux solutions de l'équation $z^2 + z - 1 = 0$. Les solutions dans $\mathbb{R}$ de cette équation sont $z_1 = \dfrac{-1+\sqrt{5}}{2}$ et $z_2 = \dfrac{-1-\sqrt{5}}{2}$.

Puisque $\alpha \geqslant 0$ car $\dfrac{2\pi}{5} \in \left[0, \dfrac{\pi}{2}\right]$, on a $\alpha = \dfrac{\sqrt{5}-1}{2}$ puis $\cos\left(\dfrac{2\pi}{5}\right) = \dfrac{\sqrt{5}-1}{4}$.

XIII.5. $\sqrt{5}$ est constructible d'après VI.5. 1 et 4 sont constructibles puis $\dfrac{\sqrt{5}-1}{4}$ est constructible d'après V. On en déduit que le point $B\left(\cos\left(\dfrac{2\pi}{5}\right), 0\right)$ est constructible et donc que le pentagone régulier $M_0M_1M_2M_3M_4$ est constructible.

XIV.



XIV.1. D'après le théorème de PYTHAGORE $BJ^2 = BO^2 + OJ^2 = \dfrac{5}{4}$ puis $BJ = \sqrt{\dfrac{5}{2}}$. Mais alors, $x_C = x_B + \dfrac{\sqrt{5}}{2} = \dfrac{\sqrt{5}-1}{2}$.
On en déduit que $x_D = \dfrac{x_C}{2} = \dfrac{\sqrt{5}-1}{4}$. D est le point de coordonnées $\left(\dfrac{\sqrt{5}-1}{4}, 0\right)$ ou encore le point d'affixe $\cos\left(\dfrac{2\pi}{5}\right)$.

XIV.2. Le point M_1 est le point d'intersection de la perpendiculaire à (OI) passant par D et du cercle $\mathbb{U}$, d'ordonnée strictement positive (et M_4 est celui d'ordonnée strictement négative). On reporte ensuite la distance IM_1 au compas pour obtenir les points M_2 et M_3