CAPES Maths 2018, épreuve 2 problème 1 : Des fonctions de chiffrement

Voici quelques éléments de correction de certaines questions de l'épreuve 2, problème 1.

Les fonctions de chiffrement étudiées ici sont du type « fonctions puissances » implicitement définies sur $\mathbf{Z}/29\mathbf{Z}$ *. Lesquelles sont des bijections de cet ensemble ?*

Partie A : « Quelques essais »

La construction d'une fonction de chiffrement conformément à cette partie est la suivante :

- On choisit un entier *k* non nul.
- On considère la fonction : $x \in \{0, 1, ..., 28\} \xrightarrow{f_k} f_k(x) = r_x$ *défini par* : $\begin{cases} r_x \equiv x^k \mod 29 \\ 0 \leq r_x < 29 \end{cases}$

Vu que $0^k = 0$; $1^k = 1$ quel que soit l'entier naturel *k* non nul, 0 et 1 restent toujours invariants. Une telle fonction de chiffrement respecte les points et les espaces.

Le déchiffrement est assuré à condition que f_k admette une application réciproque f_k^{-1}. Une CNS pour cela est que f_k soit injective OU surjective (elle est alors injective ET surjective puisqu'elle applique l'ensemble fini $\{0, 1, ..., 28\}$ sur lui-même). Ce n'est pas le cas ni de f_2 ni de f_7 par exemple (voir fin de correction).

Partie B : choix de la fonction de chiffrement

VII. Soit *p* un nombre premier et *a* un entier relatif que *p* ne divise pas.
L'ensemble *A* est l'ensemble $\{k\,a \ ; \ k \in \{1, 2, ..., p-1\}\}$

1. *p* étant un nombre premier, il est premier avec tout nombre qu'il ne divise pas : *p* est premier avec *a*.
D'après le théorème de Gauss, *p* étant premier avec *a*, si *p* divise le produit $k\,a$, alors il divise *k*. Il revient au même de dire que *k* appartient à l'ensemble $p\,\mathbf{Z}$ des multiples de *p*.
$\{1, 2, ..., p-1\} \cap p\,\mathbf{Z} = \varnothing$, donc *p* ne divise aucun élément de *A*. ¨

2. Quel que soit l'entier relatif *i*, si α_i désigne le reste de la division euclidienne de $a\,i$ par *p*, l'égalité $\alpha_i = 0$ implique que *p* divise $a\,i$. Par contraposition, si *p* ne divise pas $a\,i$, alors $\alpha_i \neq 0$.

Quel que soit *i* appartenant à $\{1, 2, ..., p-1\}$, d'après la question précédente *p* ne divise pas $a\,i$. Donc, quel que soit *i* appartenant à $\{1, 2, ..., p-1\}$, $\alpha_i \neq 0$.

Supposons qu'il existe deux entiers *i* et *j* appartenant à $\{1, 2, ..., p-1\}$ tels que $\alpha_i = \alpha_j$. Alors l'entier *p* divise $a(i-j)$, donc il divise $(i-j)$. L'entier $(i-j)$ appartient à $p\,\mathbf{Z}$. Mais puisque *i* et *j* appartiennent tous les deux à $\{1, 2, ..., p-1\}$, $(i-j)$ appartient à $\{-(p-1), -(p-2), ..., 0, 1, 2, ..., p-1\}$ ensemble dont l'intersection avec $p\,\mathbf{Z}$ ne contient que 0. Par contraposition, si *i* et *j* appartiennent à $\{1, 2, ..., p-1\}$ et sont tels que $i \neq j$, alors $\alpha_i \neq \alpha_j$.

L'application : $i \in \{1, 2, ..., p-1\} \mapsto \alpha_i \in \{1, 2, ..., p-1\}$ est une application injective d'un ensemble fini sur lui-même. Elle est donc bijective. On va désigner par h cette application et h^{-1} son application réciproque.

3. D'une part, d'après les propriétés de commutativité et d'associativité ordinaires de la multiplication : $\prod_{i=1}^{i=p-1}(a\,i) = \left(\prod_{i=1}^{i=p-1} a\right) \times \left(\prod_{i=1}^{i=p-1} i\right) = a^{p-1} \times (p-1)!$.

D'autre part, α_i désignant le reste de la division euclidienne de $a\,i$ par p, pour tout i appartenant à $\{1, 2, ..., p-1\}$, $a\,i \equiv \alpha_i \ (p)$. D'après les propriétés de compatibilité des congruences avec la multiplication : $\prod_{i=1}^{i=p-1} a\,i \equiv \prod_{i=1}^{i=p-1} \alpha_i \ \ (p)$

Compte tenu de la bijectivité de l'application h^{-1} : $\prod_{i=1}^{p-1} \alpha_i = \prod_{i=1}^{p-1} h^{-1}(\alpha_i) \underset{gj\,2018}{=} \prod_{i=1}^{p-1} i = (p-1)!$

On obtient : $a^{p-1}(p-1)! \equiv (p-1)! \ (p)$ et ce, quel que soit l'entier relatif a que p de divise pas.

4. Il en résulte : $\left(a^{p-1}-1\right)((p-1)!) \equiv 0 \ (p)$. Le nombre premier p divise le produit $\left(a^{p-1}-1\right)((p-1)!)$. Il est premier avec chacun des entiers de la factorielle, donc avec la factorielle elle-même. D'après le théorème de Gauss, il divise $a^{p-1}-1$, propriété qui s'exprime de façon équivalente par $a^{p-1} \equiv 1 \ (p)$ et ce, quel que soit l'entier relatif a que p de divise pas.

En conséquence, si on construit la fonction $x \in \{0, 1, ..., p-1\} \mapsto f_k(x) = r_k(x) \in \{0, 1, ..., p-1\}$ où $r_k(x)$ est le reste de la division euclidienne de x^k par p, la fonction f_p est l'application identique, tandis que $f_{p-1}(x) = 1$ pour tout x de $\{1, ..., p-1\}$ et en outre $f_{p-1}(0) = 0$

VIII. L'entier 29 étant un nombre premier, il est conforme à l'étude menée dans les questions précédentes.

1. Si x désigne un entier naturel premier avec 29 (donc un entier qui n'est pas un multiple de 29 …), l'ensemble des entiers strictement positifs k tels que $x^k \equiv 1 \ (29)$ est une partie non vide de l'ensemble **N*** puisque cette partie contient 28. L'ensemble **N*** étant bien ordonné, cette partie non vide de **N*** admet un plus petit élément (noté $o(x)$), nécessairement inférieur ou égal à 28.

2 et 3. Si k est un multiple de $o(x)$, il existe m : $k = m\,o(x)$. Alors : $x^k = \left(x^{o(x)}\right)^m$.

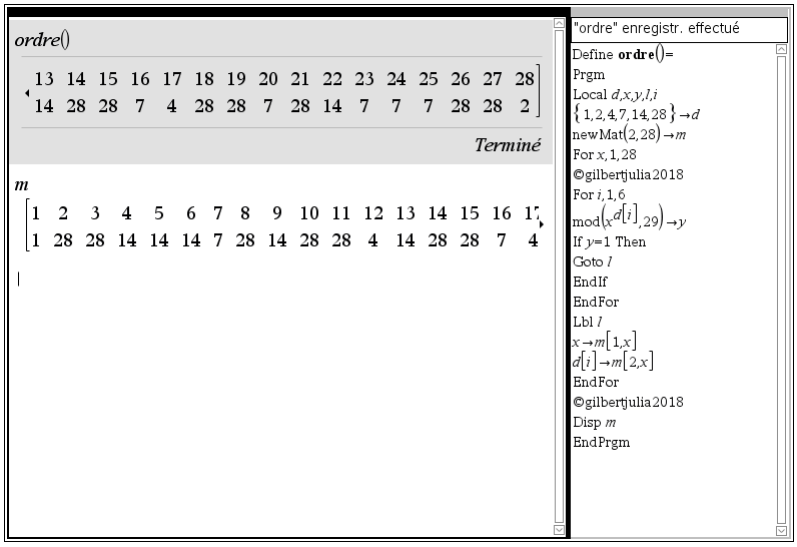
Compte tenu de la compatibilité des congruences avec les élévations à une puissance : $\underset{gj}{\begin{cases} x^k \equiv \left(x^{o(x)}\right)^m \ (29) \\ x^{o(x)} \equiv 1 \ (29) \end{cases}} \Rightarrow x^k \equiv 1 \ (29)$

Réciproquement, soit k tel que $x^k \equiv 1\,(29)$ et soient q le quotient et r le reste, $0 \le r < o(x)$, de la division euclidienne de k par $o(x)$: $\left.\begin{array}{l} x^k = x^{o(x)+r} \equiv 1\,(29) \\ x^{o(x)} \equiv 1\,(29) \end{array}\right\} \Rightarrow x^r \equiv 1\,(29)$. *gilbertjulia* 2018

Compte tenu du caractère de « plus petit élément strictement positif » que possède $o(x)$, l'entier r qui est strictement inférieur à $o(x)$ ne peut vérifier $x^r \equiv 1\,(29)$ que s'il est nul (sinon, ce serait lui le « plus petit élément strictement positif »). L'entier k est divisible par $o(x)$. Tel est le cas de 28.

5. Puisqu'il est question d'écrire un algorithme, autant s'en servir …

Le programme **ordre** affiche sous forme de matrice les entiers de 1 à 28 avec, dans la même colonne, leur ordre. Cet affichage fournit une solution exhaustive à la question **5**. On peut retenir que les éléments primitifs sont 2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26 et 27.



IX. Les classes des éléments primitifs cités ci-dessus sont autant de générateurs du groupe multiplicatif **Z**/29**Z***.

À titre d'information le programme **cycliste** ci-contre décrit, éventuellement plusieurs fois, le sous-groupe de **Z**/29**Z*** engendré par les puissances d'un de ses éléments.

Lorsque ce sous-groupe est **Z**/29**Z*** tout entier, l'élément considéré est générateur de **Z**/29**Z***.

X. L'application φ considérée est définie par : $k \in \{1,..., 28\} \mapsto \phi(k) = r_k(2)$ où $r_k(2)$ est le reste (conformément aux notations déjà utilisées) de la division euclidienne de 2^k par 29. Elle applique $\{1,..., 28\}$ sur lui-même car on a vu qu'aucun reste n'était nul. Elle est injective car 2 est primitif, donc surjective puisqu'elle applique un ensemble fini sur lui-même. Etant bijective, elle est inversible.

XI. *Une fonction de chiffrement f_k sera considérée comme une « bonne » fonction de chiffrement si deux éléments distincts de $\{0, 1,..., 28\}$ sont codés par deux éléments distincts, c'est-à-dire si f_k réalise une bijection de cet ensemble sur lui-même. La fonction permettant le déchiffrement est dans ce cas son application réciproque f_k^{-1}*

Rien ne prouve a priori qu'une fonction de chiffrement f_k admet une fonction réciproque du même type qu'elle. C'est pourtant une hypothèse implicite ici. La question qui se pose est :
Une fonction de chiffrement f_k étant donnée, en existe-t-il une autre f_m telle que : $f_m \circ f_k = I_d$?

C'est ce qu'on se propose d'examiner …

On note I_d la fonction identité définie sur $\{0, 1,..., 28\}$(elle coïncide avec f_1).

$f_m \circ f_k = I_d \Leftrightarrow_{gjulia} \forall x \in \{0, 1,..., 28\} : (x^k)^m \equiv x \ (29)$.

Les cas de 0 et de 1 n'amenant rien puisque $(0^k)^m = 0$ et $(1^k)^m = 1$ quels que soient *m* et *n*, il reste le cas des autres nombres, appartenant à $\{2,..., 28\}_{gjulia}$, tous premiers avec 29. De ce fait pour ces autres nombres :

$(x^k)^m - x \equiv 0 \ (29) \Leftrightarrow x^{k\,m-1} \equiv 1 \ (29)$.

$f_m \circ f_k = I_d \Leftrightarrow_{gjulia} \forall x \in \{2,..., 28\} : x^{k\,m-1} \equiv 1 \ (29)$.

Une condition nécessaire et suffisante pour que *m* convienne est que $k\,m-1$ soit un multiple de tous les entiers $o(x)$ lorsque *x* parcourt $\{2,..., 28\}_{gjulia}$. L'étude des ordres des différents éléments de **Z**/29**Z*** a montré que le PPCM de tous ces ordres était 28 : (on a vu que : $\exists x \in \{2,..., 28\} : x^{28} \equiv 1 \ (29)$, par exemple $x = 2$, mais on a vu aussi : $\forall x \in \{2,..., 28\} :_{gj} x^{28} \equiv 1 \ (29)$).

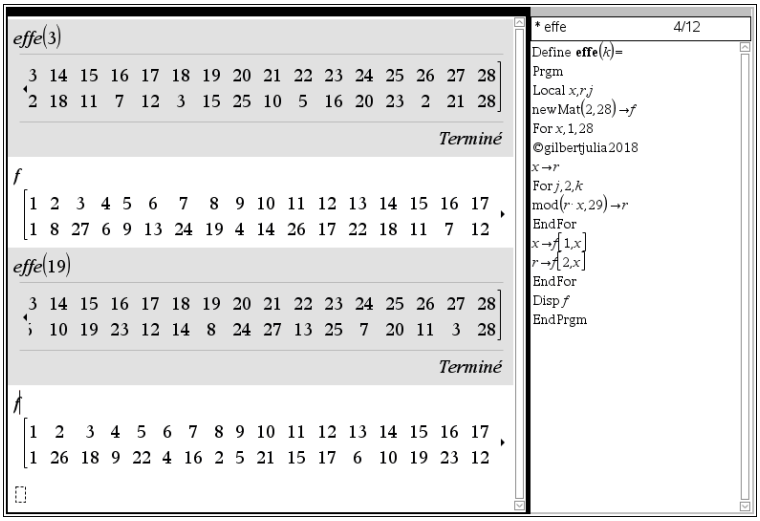
Ainsi, une condition nécessaire et suffisante pour que *m* convienne est que $k\,m-1$ soit un multiple de 28, c'est-à-dire qu'il existe un entier *u* vérifiant : $k\,m - 28\,u = 1$ **(E).**

D'après l'égalité de Bézout, l'équation diophantienne **(E)** admet des solutions (m, u) si et seulement si *k* est premier avec 28. Donc si et seulement si *k* appartient à la liste suivante : $\{3,5,9,11,13,_{gj} 15,17,19,23,25,27\}$.

En supposant que (m_0, u_0) est une solution particulière de **(E)**, les couples solutions de l'équation sont les couples : $(m = m_0 + 28\lambda,\ u = u_0 + k\,\lambda),\ \lambda \in \mathbf{Z}$. Un et un seul de ces couples est tel que $m \in \{0, 1,..., 28\}$ et nécessairement cet entier *m* n'est ni 0 ni 1.

Dans le cas où $k = 3$, il est immédiat que cet entier *m* est 19 car $3 \times 19 - 2 \times 28 = 1$

Le programme **effe** affiche la liste des images des entiers de 1 à 28 par la fonction de chiffrement f_k.

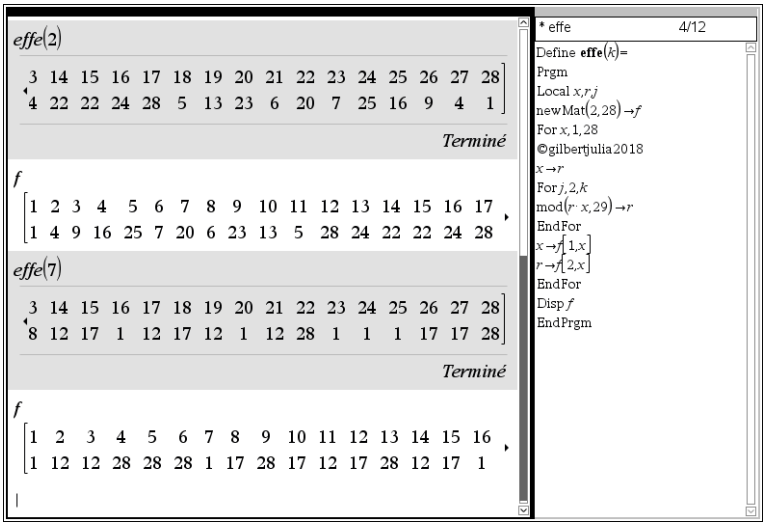


Afin d'éviter le risque de dépassement des capacités de calcul, l'image $r_k(x)$ de chaque x de 1 à 28 est calculée par récurrence, la fonction **mod** renvoyant le reste d'une division euclidienne :

$$\begin{cases} r_1(x) = \text{mod}(x,\ 29) \\ r_j(x) = \text{mod}\left(x \times r_{j-1}(x),\ 29\right) \end{cases}$$ *gilbertjulia 2018*

On vérifie que f_3 et f_{19} sont réciproques l'une de l'autre.

Pour le moment, on n'a pas démontré que lorsque k n'est pas premier avec 28 f_k n'est pas bijective ; on a juste démontré qu'alors f_k n'avait pas d'application réciproque du type « fonction puissance ».



Les listes en extension des images par f_2 et par f_7 des entiers non nuls, de 1 à 28, montrent que ni l'une ni l'autre de ces applications n'est bijective.

En notant $\text{Im}(f_k)$ l'ensemble des entiers de $_{gj}\{1,...,28\}$ qui sont images d'un entier de $_{gj}\{1,...,28\}$ par f_k :

Les inclusions $\text{Im}(f_2) \subset {}_{gj}\{1,...,28\}$ et $\text{Im}(f_7) \subset \{1,...,28\}$ sont toutes deux des inclusions strictes.

Si k n'est pas premier avec 28, alors k admet parmi ses diviseurs au moins un des deux entiers 2 ou 7 et dans ce cas une au moins des inclusions $\text{Im}(f_k) \subset \text{Im}(f_2)$ ou $\text{Im}(f_k) \subset \text{Im}(f_7)$ est vérifiée. $\text{Im}(f_k)$ est strictement inclus dans $_{gj}\{1,...,28\}$ et f_k est non surjective.

Ainsi, lorsque k n'est pas premier avec 28, il est avéré que f_k n'est pas bijective.

Voici, à titre d'exemple, ce qu'il en est de f_4, f_{14}, f_{21} .