Jour 1

PUISSANCES ET CONGRUENCES

solutions

Question 1

Si $x \equiv 0$ [2] alors $x^n \equiv 0$ pour tout $n \geqslant 1$, donc dans ce cas la suite est constante, égale à 0. Si $x \equiv 1$ [2] alors $x^n \equiv 1$ pour tout $n \geqslant 1$, donc dans ce cas la suite est constante, égale à 1.

Question 2

Si $x \equiv 0$ [3] (resp. $x \equiv 1$ [3]) alors comme précédemment $x^n \equiv 0$ (resp. $x^n \equiv 1$) pour tout $n \geqslant 1$, donc dans ce cas la suite est constante, égale à 0 (resp. à 1). Si $x \equiv 2 \equiv -1$ [3], on va donc avoir alternativement -1 (c'est-à-dire 2 modulo 3) et 1, puisque $u_n \equiv (-1)^n$ [3]. Autrement dit, lorsque $x \equiv 2$ [3], on a

$$u_n = \begin{cases} 2 & \text{si } n \text{ est impair,} \\ 1 & \text{si } n \text{ est pair.} \end{cases}$$

Question 3

Soient n et n' deux entiers strictement positifs, avec $n < n'$. On suppose que $u_n = u_{n'}$. On considère la propriété $\mathscr{P}(k)$: « $u_{n+k} = u_{n'+k}$ ». Montrons, par récurrence sur k, qu'elle est tout le temps vraie.

Initialisation. Pour $k = 0$ la propriété revient à $u_n = u_{n'}$, qui est vrai : c'est l'hypothèse de l'exercice.

Hérédité. Fixons un entier k et supposons que $\mathscr{P}(k)$ est vraie. Alors

$$u_{n'+k+1} \equiv x^{n'+k+1} \equiv x^{n'+k} \times x \equiv u_{n'+k} \times x \equiv \underset{\substack{\uparrow \\ \text{car } u_{n'+k} = u_{n+k}}}{u_{n+k}} \times x \equiv x^{n+k} \times x \equiv x^{n+k+1} \equiv u_{n+k+1}\ [m].$$

De plus, on sait que $u_{n'+k+1}$ et u_{n+k+1} sont tous les deux entre 0 et $m-1$, donc s'ils sont congrus modulo m, ils sont égaux. Ainsi $\mathscr{P}(k+1)$ est vraie.

Conclusion. La propriété est initialisée et héréditaire, donc elle est vraie pour tout $k \in \mathbf{N}$.

Question 4

Puisque u_n ne peut prendre que m valeurs différentes, il y a, parmi les termes u_1, u_1, u_2, etc., u_{m+1}, au moins deux valeurs égales (on doit prendre $m+1$ termes parmi m valeurs, il faut qu'il y ait un double). Donc il existe deux indices distincts n et n', entre 1 et $m+1$, tels que $u_n = u_{n'}$. Quite à les échange, on peut dire que $n < n'$; notons alors $\mathrm{T} = n' - n$. On a $n' = n + \mathrm{T}$ et $u_n = u_{n+\mathrm{T}}$. D'après la question précédente, on a alors $u_{n+k} = u_{n+\mathrm{T}+k}$, et donc la suite est périodique de période T à partir du rang n.

Exercice A

a) On suppose donc qu'il y a un y tel que $x \times y \equiv 1$ [m]. On peut, quite à le réduire modulo m, supposé que ce y est entre 0 et $m-1$, et même entre 1 et $m-1$ (puisque $x \times 0$ sera toujours égal à zéro). Maintenant reprenons les notations de la **Question 4**. On a prouvé l'existence d'un entier T entre 1 et m tel que $x^{n+\mathrm{T}} \equiv x^n$ pour un certain indice n. Multiplions chaque membre par y^n : on obtient

$$x^{n+\mathrm{T}} \times y^n \equiv x^n \times y^n \qquad \text{c'est-à-dire} \qquad x^{\mathrm{T}} \equiv 1$$

puisque $x^n \times y^n \equiv (x \times y)^n \equiv 1^n$ et que $x^{n+\mathrm{T}} = x^n \times x^{\mathrm{T}}$. Sauf qu'on peut écrire $x^{\mathrm{T}} = x \times x^{\mathrm{T}-1}$, et on a donc

$$x \times x^{\mathrm{T}-1} \equiv 1\ [m],$$

avec $\mathrm{T}-1 \in \{0\,;\,1\,;\,\ldots\,;\,m-1\}$, et comme $x^{\mathrm{T}-1} \equiv u_{\mathrm{T}-1}\ [m]$, on a bien $y = u_{\mathrm{T}-1}$, comme il était demandé.

b) Dans les questions précédentes, on a vu que lorsqu'on trouve une valeur déjà rencontrée, la suite se répète à partir de là. Donc pour $m = 7$ et $x = 2$ on trouve $u_1 = 2$, $u_2 = 4$, $u_3 = 1$, $u_4 = 2$ et donc $u_5 = 4$, $u_6 = 1$, etc., soit en résumé

$$u_n = \begin{cases} 2 & \text{si } n \equiv 1\ [3], \\ 4 & \text{si } n \equiv 2\ [3], \\ 1 & \text{si } n \equiv 0\ [3]. \end{cases}$$

c) On a déjà tout dit dans la question **a** : on a $u_{\mathrm{T}-1} = y$ (l'inverse de x modulo m) donc $u_{\mathrm{T}} \equiv y \times x \equiv 1\ [m]$ et enfin $u_{\mathrm{T}+1} \equiv 1 \times x \equiv x \equiv u_1$, et donc $u_{\mathrm{T}+1} = u_1$.

d) Pour construire un contre-exemple on doit choisir une situation où x n'est pas inversible. Prenons $m = 20$ et $x = 2$. On obtient la suite

$$2\,;\,4\,;\,8\,;\,16\,;\,12\,;\,4\,;\,8\,;\,\ldots$$

qui continue en répétant la période 4, 8, 16, 12, mais on ne revient jamais à $u_1 = 2$.

Question 5

Donc ici $m = 14$ et $x = 5$. On commence à énumérer les termes de la suite :

$$u_1 = 5\,;\,u_2 = 11\,;\,u_3 = 13\,;\,u_4 = 9\,;\,u_5 = 3\,;\,u_6 = 1$$

et donc la suite se répète à partir de là. La période est de longueur 5, donc tout dépend du reste dans la division euclidienne de l'exposant par 5. On a $2\,024 \equiv 4\ [5]$ donc $u_{2\,024} = u_4 = 9$.

Question 6

Supposons qu'on a $u_n = 0$ pour un certain indice n. Cela veut dire que $x^n \equiv 0\ [m]$ (puisque $u_n \equiv x^n$) et donc que m divise x^n. Donc tous les facteurs premiers p apparaissant dans la décomposition de m apparaissent aussi dans la décomposition de x^n, et donc de x (car x^n et x ont les mêmes facteurs premiers, bien que pas en même quantité). Réciproquement, supposons que tout facteur premier p de m soit aussi un facteur de x. Pour fixer les idées, disons que

$$m = p_1^{v_1} \times p_2^{v_2} \times \ldots \times p_r^{v_r} \qquad \text{et} \qquad x = p_1 \times p_2 \times \ldots \times p_r \times \mathrm{P}$$

avec P un nombre quelconque. Soit v le maximum de v_1, v_2, etc., v_r. Alors m divise $p_1^v \times p_2^v \times \ldots \times p_r^v$ (car tous les exposants sont au moins aussi grands que ceux de m) et donc m divise

$$x^v = p_1^v \times p_2^v \times \ldots \times p_r^v \times \mathrm{P}^v.$$

On a donc $x^v \equiv 0\ [m]$, et donc $u_v = 0$ (et tous les termes suivants aussi sont nuls, puisqu'en multipliant 0 par n'importe quoi, même modulo m, on obtient toujours zéro).

Résumons : la suite $(u_n)_{n \geqslant 1}$ est identiquement nulle à partir d'un certain rang si et seulement si tous les facteurs premiers de m sont des facteurs premiers de x. Exemple : $m = 48 = 2^4 \times 3^1$ et $x = 90 = 2 \times 3^2 \times 5$ (les facteurs premiers de m sont 2 et 3, et ils apparaissent bien dans x).