

Restes modulo p

Énoncé

Le but de cet exercice est d'étudier les restes modulo p (p entier strictement supérieur à 1) des suites $(u_n)_{n \in \mathbb{N}}$ définies par : $u_n = an + b$, a et b étant deux entiers naturels donnés.

1. Construire une feuille de calcul donnant les restes modulo 20 des 20 premiers termes de la suite $(u_n)_{n \in \mathbb{N}}$ définie par $u_n = 12n + 5$.

Appeler l'examineur

2. Adapter la feuille de calcul de façon à obtenir les restes modulo p des 20 premiers termes de la suite définie par $u_n = an + b$, $n \in \mathbb{N}$, de telle manière qu'on puisse modifier les valeurs de a , b et p . Notez sur votre feuille les restes obtenus dans les cas particuliers suivants :

(a) $p = 20$ et $u_n = 5n - 3$;

(b) $p = 7$ et $u_n = 5n - 3$.

Quelle conjecture peut-on formuler quant aux suites formées par ces restes euclidiens ?

Appeler l'examineur pour vérifier la conjecture émise

3. Démonstration de la conjecture :

(a) Montrer que, parmi les nombres u_0, u_1, \dots, u_p , il existe deux nombres ayant le même reste dans la division euclidienne par p , pour p entier naturel non nul.

(b) Soient n_0 et $n_0 + T$ les rangs de ces deux nombres ($T \neq 0$).
Montrer que aT est un multiple de p .


(c) En déduire que pour tout entier naturel k , u_{T+k} et u_k ont le même reste dans la division euclidienne par p .

(d) Démontrer alors la conjecture.

Production demandée

- Feuille de calcul correspondant aux diverses suites.
- Les démonstrations de la question 3.

Proposition de corrigé avec le Classpad

1. On entre dans l'application tableur par un appui du stylet sur l'icône  dans l'écran d'accueil du Classpad.

On crée une nouvelle feuille de calcul par « Fich/Nouveau ».

On choisit « Edit/Remplir suite » puis on renseigne la fenêtre comme indiqué (fig1).

Après validation, les vingt premiers entiers, de 0 à 19, apparaissent dans la colonne A.

On place ensuite le curseur sur la cellule B1. On choisit la fonction « Edit/Remplir échelle » et on renseigne la fenêtre comme indiqué fig2.

Ainsi on copie la formule $=\text{mod}(12A1+5, 20)$ de B1 jusqu'à B20.

Comme il s'agit d'*adressage relatif*, cela signifie qu'on place $=\text{mod}(12A[k]+5, 20)$ dans la cellule B[k], pour $1 \leq k \leq 20$.

On valide, et on obtient la liste des entiers $r_n = \text{mod}(u_n, 20)$, pour $0 \leq n \leq 19$ (fig3).

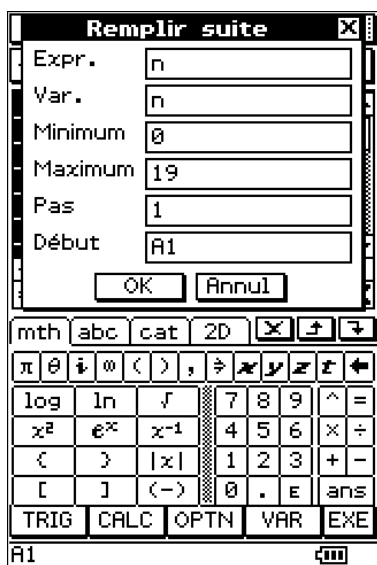


fig1 : entiers n de 0 à 19

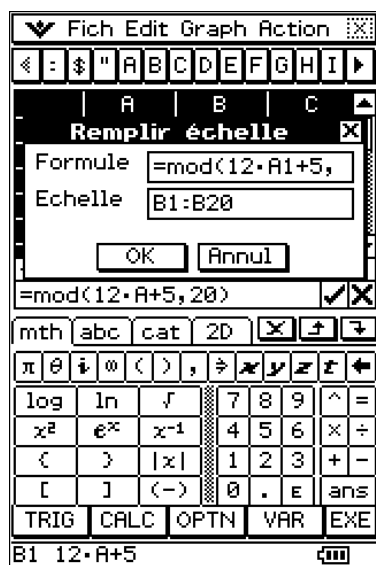


fig2 : formule de calcul

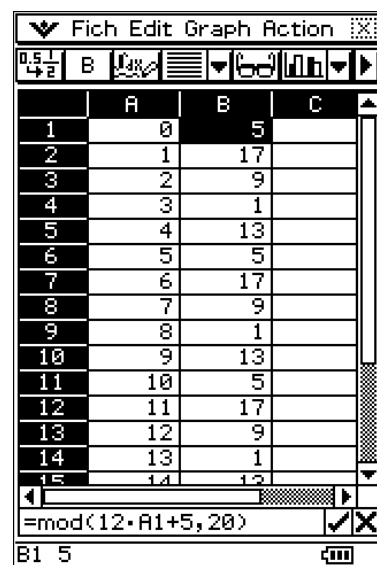


fig3 : le résultat

2. On va adapter la fenêtre de calcul de façon à pouvoir modifier les paramètres a, b, p .

Dans les cellules C1, C3, C5, on met respectivement les chaînes "a", "b", "p".

Dans les cellules C2, C4, C6, on place respectivement les valeurs 5, -3 et 20.

On revient ensuite sur la cellule B1. On choisit la fonction « Edit/Remplir échelle » et on place, sur la plage B1:B20, la formule $=\text{mod}(\$C\$2*A1+\$C\$4, \$C\$6)$.

Un référence comme $\$C\6 est dite *absolue*, alors que C6 est une référence *relative*. La première est invariable dans toute copie d'une formule sur une plage de cellules, et désigne donc toujours la même cellule origine.

Quand on a validé la fenêtre copiant la formule dans B1:B20, on voit apparaître dans la colonne B, les vingt premiers $r_n = \text{mod}(an + b, p)$ avec $a = 5$, $b = -3$ et $p = 20$ (fig4).

Il suffit de modifier C2, C4 et C6 (pour y placer respectivement 5, -3 et 7) : la feuille est automatiquement recalculée et la colonne B contient maintenant les vingt premiers $r_n = \text{mod}(an + b, p)$ avec $a = 5$, $b = -3$ et $p = 7$ (fig5).

On peut évidemment vérifier que tout fonctionne bien en redonnant les valeurs $a = 12$, $b = 5$, $p = 20$ pour retrouver la colonne B obtenue dans la question 1 (fig6).

	A	B	C
1	0	17	"a="
2	1	2	5
3	2	7	"b="
4	3	12	-3
5	4	17	"p="
6	5	2	20
7	6	7	
8	7	12	
9	8	17	
10	9	2	
11	10	7	
12	11	12	
13	12	17	
14	13	2	
15	14	7	

fig4 : $a = 5$, $b = -3$, $p = 20$

	A	B	C
1	0	4	"a="
2	1	2	5
3	2	0	"b="
4	3	5	-3
5	4	3	"p="
6	5	1	7
7	6	6	
8	7	4	
9	8	2	
10	9	0	
11	10	5	
12	11	3	
13	12	1	
14	13	6	
15	14	4	

fig5 : $a = 5$, $b = -3$, $p = 7$

	A	B	C
1	0	5	"a="
2	1	17	12
3	2	9	"b="
4	3	1	5
5	4	13	"p="
6	5	5	20
7	6	17	
8	7	9	
9	8	1	
10	9	13	
11	10	5	
12	11	17	
13	12	9	
14	13	1	
15	14	13	

fig6 : $a = 12$, $b = 5$, $p = 20$

On constate que les suites $n \mapsto r_n = \text{mod}(an + b, p)$ sont (du moins dans la limite des choix pris ici pour a, n, p et dans la limite des vingt premiers termes calculés) périodiques.

Plus précisément :

- La suite $n \mapsto \text{mod}(12n + 5, 20)$ semble 5-périodique.
- La suite $n \mapsto \text{mod}(5n - 3, 20)$ semble 4-périodique.
- La suite $n \mapsto \text{mod}(5n - 3, 7)$ semble 7-périodique.

3. (a) On se donne les entiers a, n, p (avec $p \geq 1$), et la suite des $u_n = an + b$.

Les nombres u_0, u_1, \dots, u_p forment une famille de cardinal $p + 1$.

Or il y a p restes différents possibles dans une division par p .

D'après le principe des tiroirs, il existe donc au moins deux nombres parmi u_0, u_1, \dots, u_p qui ont le même reste dans la division euclidienne par p .

(b) Par hypothèse u_{n_0} et u_{n_0+T} ont même reste dans la division euclidienne par p .

Il en découle que $u_{n_0+T} - u_{n_0}$ est un multiple de p .

Or $u_{n_0+T} - u_{n_0} = (a(n_0 + T) + b) - (an_0 + b) = aT$. Donc aT est un multiple de p .

(c) Avec les notations précédentes, posons $aT = qp$, avec q dans \mathbb{N} .

Pour tout entier k de \mathbb{N} , on a : $u_{T+k} = a(T + k) + b = (ak + b) + aT = u_k + qp$.

Ainsi la différence $u_{T+k} - u_k$ est divisible par p .

Ce la signifie que u_{T+k} et u_k ont le même reste dans la division euclidienne par p .

(d) Avec ce qui précède, on a : $\text{mod}(u_{T+k}, p) = \text{mod}(u_k, p)$ (pour tout k de \mathbb{N}).

Cela signifie que la suite $n \mapsto \text{mod}(u_n, p)$ est T -périodique.

4. Complément

Il est légitime de se demander quelle est la période *exacte* (c'est-à-dire la plus petite période strictement positive) de la suite $n \mapsto r_n = \text{mod}(u_n, p)$.

Pour cela, on introduit le pgcd δ de a et p ($\delta \geq 1$ car p est non nul).

On sait qu'il existe deux entiers a', p' premiers entre eux, tels que $a = \delta a'$ et $p = \delta p'$.

On se donne deux entiers naturels m et n et on se demande à quelle condition on a $r_m = r_n$, c'est-à-dire à quelle condition p divise $u_m - u_n$.

Or on a : $u_m - u_n = (am + b) - (an + b) = a(m - n) = \delta a'(m - n)$.

Dans ces conditions : $r_m = r_n \Leftrightarrow p \mid (u_m - u_n) \Leftrightarrow \delta p' \mid \delta a'(m - n) \Leftrightarrow p' \mid a'(m - n)$.

Mais $a' \wedge p' = 1$. Donc $p' \mid a'(m - n) \Leftrightarrow p' \mid (m - n)$, en vertu du théorème de Gauss.

Conclusion : la suite $n \mapsto r_n = \text{mod}(u_n, p)$ est périodique de période $T = p' = \frac{p}{a \wedge p}$.

On retrouve ainsi que :

– La suite $n \mapsto \text{mod}(12n + 5, 20)$ est périodique de période $\frac{20}{12 \wedge 20} = \frac{20}{4} = 5$.

– La suite $n \mapsto \text{mod}(5n - 3, 20)$ est périodique de période $\frac{20}{5 \wedge 20} = \frac{20}{5} = 4$.

– La suite $n \mapsto \text{mod}(5n - 3, 7)$ est périodique de période $\frac{7}{5 \wedge 7} = \frac{7}{1} = 7$.

5. Généralisation

Soit $A(x)$ un polynôme à coefficients entiers, de degré supérieur ou égal à 1.

Pour tout n de \mathbb{N} , $u_n = A(n)$ est un entier relatif et on peut poser $r_n = \text{mod}(A(n), p)$.

La question est : la suite $n \mapsto r_n$ est-elle périodique? (cela généralise considérablement l'exercice du début, dans lequel on a en fait $A(x) = ax + b$).

La réponse est oui, mais la méthode diffère un peu (et on ne connaîtra pas de formule donnant la période minimum). Plus précisément, *une* période de la suite (u_n) est l'entier p (et donc la plus petite période est certainement un diviseur de p , mais lequel?).

En effet, pour tout entier n , le polynôme $B(x) = A(n+x) - A(n)$ s'annule en 0 et est donc divisible par le polynôme x . Plus précisément, il existe un polynôme Q_n (à coefficients entiers dépendant de n) tel que $A(n+x) - A(n) = xQ_n(x)$.

On en déduit $A(n+p) = A(n) + pQ_n(p)$ (avec $Q_n(p)$ dans \mathbb{N}), donc $r_{n+p} = r_n$.

Ainsi la suite $n \mapsto r_n = \text{mod}(A(n), p)$ est périodique (et sa plus petite période est un diviseur de p).