Maths Expertes
Terminale

PGCD, Bézout & Gauss

CORRIGÉ DE L'EXERCICE

PGCD

II

Correction

Rappelons la formule explicite donnant la somme des *n* premiers entiers :

Pour tout entier *n* strictement positif,

$$1+2+\cdots+n=\sum_{i=1}^{n} i=\frac{n(n+1)}{2}$$

La somme des $(n-1)$ premiers entiers, utile pour la **question 2.b**, s'exprime donc ainsi :

$$1+2+\cdots+n-1=\sum_{i=1}^{n-1} i=\frac{n(n-1)}{2}$$

1. Exprimons a_n en fonction de n :

Du fait de sa définition, la suite $(a_n)_{n\in\mathbb{N}^*}$ apparaît comme étant la suite arithmétique de premier terme $a_1=3$ et de raison $r=2$.

Nous savons que la formule explicite donnant le terme général u_n d'une suite arithmétique (u_n) de premier terme u_1 et de raison *r* est la formule : $u_n=u_1+(n-1)r$.

Dans notre contexte : $a_n=3+2(n-1)=2n+1$

2.a. Justifions la formule de sommation que l'énoncé nous propose :

Pour l'entier *k* allant de 2 à *n*, écrivons les $(n-1)$ formules de récurrence définissant les termes b_k :

$$\begin{cases} b_2=b_1+a_1 \\ b_3=b_2+a_2 \\ \quad\cdots \\ b_{n-1}=b_{n-2}+a_{n-2} \\ b_n=b_{n-1}+a_{n-1} \end{cases}.$$

Ajoutons membre à membre ces $(n-1)$ égalités :

Nous obtenons : $b_2+\cdots+b_n=(b_1+\cdots+b_{n-1})+(a_1+\cdots+a_{n-1})$.

Il se crée un « effet domino » car des mêmes termes se trouvent de part et d'autre du symbole d'égalité : $(b_2 + \cdots + b_{n-1}) + b_n = b_1 + (b_2 + \cdots + b_{n-1}) + (a_1 + \cdots + a_{n-1})$.

L'élimination en domino de ces termes communs aux deux membres de l'égalité ne laisse parmi les termes de la suite (b_n) que le terme de rang n et celui de rang 1 :

$$b_n = b_1 + (a_1 + \cdots + a_{n-1})$$

Soit, sous forme de « notation sigma » :

$$b_n = b_1 + \sum_{i=1}^{n-1} a_i$$

2.b. Déduisons-en une expression de b_n en fonction de n :

Compte tenu de la formule explicite exprimant les termes a_i obtenue à la **question 1** et de celle donnant la somme des premiers entiers rappelée en préambule :

$$b_n = 2 + \sum_{i=1}^{n-1} (2i+1) = 2 + \sum_{i=1}^{n-1} 1 + 2\sum_{i=1}^{n-1} i = 2 + (n-1) + 2 \times \frac{n(n-1)}{2}$$

En fin de compte : $b_n = n^2 + 1$.

3.a. Montrons qu'un diviseur commun à a_n et à b_n est un diviseur de 5 :

Pour cela, tentons de trouver une relation indépendante de n entre a_n et b_n.

Une idée est d'exprimer de deux façons différentes le nombre n^2 ou mieux, le nombre $4n^2$.

- D'une part, $2n = a_n - 1$ donc $4n^2 = (a_n - 1)^2 = a_n{}^2 - 2a_n + 1$
- D'autre part, $n^2 = b_n - 1$ donc $4n^2 = 4b_n - 4$

Nous en déduisons : $a_n{}^2 - 2a_n + 1 = 4b_n - 4$, autrement dit : $4b_n + 2a_n - a_n{}^2 = 5$.

Tout diviseur commun à a_n et à b_n divise $a_n{}^2$ et donc divise la combinaison entière $4b_n + 2a_n - a_n{}^2$ des trois nombres a_n, b_n et $a_n{}^2$, combinaison qui est égale à 5, indépendamment de n.

Tout diviseur commun à a_n et à b_n divise 5.

NB. En particulier, il en est ainsi du PGCD. Le PGCD de a_n et de b_n est égal ou bien à 1 ou bien à 5, puisque 5, en tant que nombre premier, admet deux diviseurs positifs.

3.b. Montrons que si $\mathrm{PGCD}(a_n\ ;\ b_n) = 5$, alors $n \equiv 2\ \ [5]$:

NB. L'abréviation « ssi… » figurant dans l'énoncé est censée signifier « seulement si ». La locution abrégée « (proposition *A*) ssi (proposition *B*) », certes quelque peu ambigüe, est censée signifier « $A \Longrightarrow B$ » ou « si *A* alors *B* ». Elle se différencie de l'abréviation « si et ssi » qui est censée signifier « si et seulement si » c'est-à-dire « est équivalent à ». Il n'est pas conseillé d'utiliser ce genre d'abréviation dans la rédaction d'une solution.

Supposons que $\mathrm{PGCD}(a_n\ ;\ b_n) = 5$.

Alors, $a_n = 2n + 1$ est un multiple de 5, ce qui s'exprime, en langage de congruence modulo 5 par :

$$2n + 1 \equiv 0\ \ [5]$$

Multiplions par 3 (qui est un « inverse modulo 5 » de 2) les deux membres de cette congruence :

$$6n + 3 \equiv 0\ \ [5]$$

Or, $6n + 3 = (n - 2) + 5n + 5$, donc $6n + 3 \equiv n - 2\ \ [5]$

Par transitivité, nous obtenons : $n - 2 \equiv 0\ \ [5]$.

$$\mathrm{PGCD}(a_n\ ;\ b_n) = 5 \quad \Rightarrow \quad n \equiv 2\ \ [5]$$

NB. Réciproquement (car c'est bien de la réciproque dont nous avons besoin pour finaliser la valeur du PGCD), $n - 2 \equiv 0\ \ [5]\ \ \Rightarrow\ \ 2n - 4 \equiv 0\ \ [5]\ \ \Rightarrow a_n = 2n + 1 = (2n - 4) + 5 \equiv 0\ \ [5]$.

L'entier a_n est un multiple de 5 et, s'il en est ainsi, $4b_n = -2a_n + {a_n}^2 - 5$, donc b_n lui-même, aussi ;

Si $n - 2 \equiv 0\ \ [5]$, alors $\mathrm{PGCD}(a_n\ ;\ b_n) = 5$.

3.c. Déterminons $\mathrm{PGCD}(a_n\ ;\ b_n) = 5$ pour les autres valeurs de *n* :

La **question 3.b** a montré que, si $\mathrm{PGCD}(a_n\ ;\ b_n) = 5$, alors *n* vérifie la congruence $n \equiv 2\ \ [5]$.

Cette implication établit en même temps, par sa contraposition, que si *n* ne vérifie pas la congruence $n \equiv 2\ \ [5]$, alors $\mathrm{PGCD}(a_n\ ;\ b_n)$ n'est pas égal à 5.

Or, nous avons vu que ce PGCD était égal ou bien à 1 ou bien à 5. L'implication contraposée peut donc aussi bien s'énoncer ainsi :

Si $n \not\equiv 2\ \ [5]$,alors $\mathrm{PGCD}(a_n\ ;\ b_n) = 1$.

Pour les valeurs de *n* non congrues à 2 modulo 5, a_n et b_n sont premiers entre eux.

Cet algorithme Python illustre l'exercice. Il affiche, selon les valeurs de l'entier *n* de 2 à 13, les premiers termes des deux suites et leur PGCD. Nous observons un PGCD égal à 5 lorsque *n* est égal à 2, 7 et 12 et égal à 1 pour « les autres valeurs ».	`>>> from math import gcd`
	`>>> def pgcd11():`
	`        a=3`
	`        b=2`
	`        n=1`
	`        for i in range(1,13):`
	`                n=n+1`
	`                b=a+b`
	`                a=a+2`
	`                print(n,a,b,gcd(a,b))`
		`>>> pgcd11()`
		`2 5 5 5`
		`3 7 10 1`
		`4 9 17 1`
		`5 11 26 1`
		`6 13 37 1`
		`7 15 50 5`
		`8 17 65 1`
		`9 19 82 1`
		`10 21 101 1`
		`11 23 122 1`
		`12 25 145 5`
		`13 27 170 1`