

∞ DEVOIR MAISON 18 ∞ CALCUL DE PGCD

Exercice 1. Dans cet exercice, on pourra utiliser le résultat suivant ;

« Etant donné deux entiers naturels a et b non nuls, si $\text{PGCD}(a; b) = 1$ alors $\text{PGCD}(a^2; b^2) = 1$ ».

Une suite $(S_n)_{n \in \mathbb{N}}$ est définie pour $n > 0$ par :

$$S_n = \sum_{i=1}^n p^3$$

On se propose de calculer, pour tout entier naturel n le plus grand diviseur commun entre S_n et S_{n+1} .

1. Démontrer, par récurrence, que pour tout $n > 0$, on a :

$$S_n = \left(\frac{n(n+1)}{2} \right)^2$$

Notons cette propriété $\mathcal{P}(n)$ et montrons la par récurrence.

– **Initialisation** : Si $n = 1$ alors $S_n = 1$ et $n(n+1)/2 = 1$ donc $\left(\frac{n(n+1)}{2} \right)^2 = 1$ ce qui montre bien que $\mathcal{P}(1)$ est vraie.

– **Initialisation** Montrons que si $S_n = \left(\frac{n(n+1)}{2} \right)^2$ alors $S_{n+1} = \left(\frac{(n+1)(n+2)}{2} \right)^2$.

$S_{n+1} = S_n + (n+1)^3$ donc si $S_n = \left(\frac{n(n+1)}{2} \right)^2$ alors :

$$S_{n+1} = \left(\frac{n(n+1)}{2} \right)^2 + (n+1)^3 = \frac{n^2(n+1)^2 + 4(n+1)^3}{4} = \frac{(n+1)^2 [n^2 + 4(n+1)]}{4} = \frac{(n+1)^2 (n+2)^2}{4}$$

Par conséquent

$$S_{n+1} = \left(\frac{(n+1)(n+2)}{2} \right)^2$$

$\mathcal{P}$ est héréditaire.

– **Conclusion** : $\mathcal{P}$ est initialisée à partir de $n = 1$ et est héréditaire par conséquent on a démontré par récurrence que pour tout $n > 0$:

$$S_n = \left(\frac{n(n+1)}{2} \right)^2$$

2. Etude du cas où n est pair. Soit k l'entier naturel non nul tel que $n = 2k$.

(a) Démontrer que $\text{PGCD}(S_{2k}; S_{2k+1}) = (2k+1)^2 \text{PGCD}(k^2; (k+1)^2)$.

$$S_{2k} = \left(\frac{2k(2k+1)}{2} \right)^2 = (k(2k+1))^2 = k^2(2k+1)^2$$

$$S_{2k+1} = \left(\frac{(2k+1)(2k+2)}{2} \right)^2 = ((2k+1)(k+1))^2 = (k+1)^2(2k+1)^2$$

On rappelle que si $k \neq 0$ on a :

$$\text{PGCD}(ka; kb) = k \text{PGCD}(a; b)$$

donc ici :

$$\text{PGCD}(S_{2k}; S_{2k+1}) = \text{PGCD}(k^2(2k+1)^2; (k+1)^2(2k+1)^2) = (2k+1)^2 \text{PGCD}(k^2; (k+1)^2)$$

(b) Calculer $\text{PGCD}(k; k+1)$. $n > 0$ on a alors $k \geq 1$, si $k = 1$ alors $k+1 = 2$ et $\text{PGCD}(1; 2) = 1$ sinon on effectue la suite de division euclidienne :

$$k+1 = 1 \times k + 1$$

$$k = 1 \times k + 0$$

donc dans tous les cas $\text{PGCD}(k; k+1) = 1$.

- (c) Calculer
- $\text{PGCD}(S_{2k}; S_{2k+1})$
- .

Puisque $\text{PGCD}(k; k+1) = 1$ on a $\text{PGCD}(k^2; (k+1)^2) = 1$ donc :

$$\text{PGCD}(S_{2k}; S_{2k+1}) = (2k+1)^2 \times 1 = (2k+1)^2$$

3. Etude du cas où
- n
- est impair. Soit
- k
- l'entier naturel non nul tel que
- $n = 2k+1$
- .

4. (a) Démontrer que les entiers
- $2k+1$
- et
- $2k+3$
- sont premiers entre eux.

$2k+1$ et $2k+3$ sont deux nombres impairs. De plus toute combinaison linéaire de $2k+3$ et $2k+1$ divise leur PGCD en particulier $2k+3 - 2k - 1 = 2$ divise leur PGCD donc $\text{PGCD}(2k+1; 2k+3) = 1$ ou 2 .

Etant deux nombres impairs on conclut que :

$$\text{PGCD}(2k+1; 2k+3) = 1$$

- (b) Calculer
- $\text{PGCD}(S_{2k+1}; S_{2k+2})$

$$S_{2k+1} = \left(\frac{(2k+1)(2k+2)}{2} \right)^2 = (2k+1)^2 (k+1)^2$$

$$S_{2k+2} = \left(\frac{(2k+2)(2k+3)}{2} \right)^2 = (2k+3)^2 (k+1)^2$$

Donc :

$$\text{PGCD}(S_{2k+1}; S_{2k+2}) = \text{PGCD}((2k+1)^2 (k+1)^2; (2k+3)^2 (k+1)^2) = (k+1)^2 \text{PGCD}((2k+1)^2; (2k+3)^2)$$

Puisque $\text{PGCD}(2k+1; 2k+3) = 1$ il suit que $\text{PGCD}((2k+1)^2; (2k+3)^2) = 1$ par conséquent :

$$\text{PGCD}(S_{2k+1}; S_{2k+2}) = (k+1)^2$$

5. Dédurre des questions précédentes qu'il existe une unique valeur de
- n
- , que l'on déterminera, pour laquelle
- S_n
- et
- S_{n+1}
- sont premiers entre eux.

Si n est pair, alors S_n et S_{n+1} sont premiers entre eux si et seulement si :

$$(2k+1)^2 = 1 \iff 2k+1 = 1 \quad \text{ou} \quad 2k+1 = -1 \iff k = 0 \quad \text{ou} \quad k = -1$$

Si $k = 0$ alors $n = 0$ ce qui est impossible puisque $n > 0$ et si $k = -1$ alors $n = -2$ ce qui est impossible pour la même raison.

Si n est pair, alors S_n et S_{n+1} ne sont jamais premiers entre eux.

Si n est impair alors S_n et S_{n+1} sont premiers entre eux si et seulement si

$$(k+1)^2 = 1 \iff k+1 = 1 \quad \text{ou} \quad k+1 = -1 \iff k = 0 \quad \text{ou} \quad k = -2$$

Si $k = 0$ alors $n = 1$ auquel cas S_n et S_{n+1} sont premiers entre eux.

Si $k = -2$ alors $n = -3$ ce qui est impossible puisque $n > 0$.

Au final S_n et S_{n+1} sont premiers entre eux si et seulement si $n = 1$ auquel cas $S_1 = 1$ et $S_2 = 1 + 8 = 9$.

Exercice 2.

1. Montrer que, pour tout entier naturel non nul
- k
- et pour tout entier naturel
- x
- :

$$(x-1) \left(1 + x + x^2 + \dots + x^{k-1} \right) = x^k - 1.$$

Dans toute la suite de l'exercice, on considère un nombre entier a supérieur ou égal à 2.

2. (a) Soit
- n
- un entier naturel non nul et
- d
- un diviseur positif de
- n
- :
- $n = dk$
- .

Montrer que $a^d - 1$ est un diviseur de $a^n - 1$.

- (b) Dédurre de la question précédente que
- $2^{2004} - 1$
- est divisible par 7, par 63 puis par 9.

3. Soient
- m
- et
- n
- deux entiers naturels non nuls et
- d
- leur pgcd.

- (a) On définit m' et n' par $m = dm'$ et $n = dn'$. En appliquant le théorème de Bezout à m' et n' , montrer qu'il existe des entiers relatifs u et v tels que : $mu - nv = d$.
- (b) On suppose u et v strictement positifs.
Montrer que : $(a^{mu} - 1) - (a^{nv} - 1)a^d = a^d - 1$.
Montrer ensuite que $a^d - 1$ est le pgcd de $a^{mu} - 1$ et de $a^{nv} - 1$.
- (c) Calculer, en utilisant le résultat précédent, le pgcd de $2^{63} - 1$ et de $2^{60} - 1$.

Solution :

1. $1 + x + x^2 + \dots + x^{k-1}$ est la somme des k premiers termes de la suite géométrique de premier terme 1 et de raison x : elle est donc égale à : $\frac{x^k - 1}{x - 1}$ (pour $x \neq 1$).

$$\text{Donc } (x - 1) \left(1 + x + x^2 + \dots + x^{k-1} \right) = (x - 1) \times \frac{x^k - 1}{x - 1} = x^k - 1.$$

Pour $x = 1$: l'égalité est évidente.

2. (a) $n \in \mathbb{N}$, $n = dk$.

D'après la question 1. $a^n - 1 = (a - 1)(1 + a + a^2 + \dots + a^{n-1}) = a^{dk} - 1 = (a^d)^k - 1 = (a^d - 1)(\dots + \dots)$, la parenthèse étant une somme d'entiers donc un entier.

Conclusion : $a^n - 1 = (a^d - 1)(\dots + \dots)$, ce qui signifie que $(a^d - 1)$ est un diviseur de $a^n - 1$.

- (b) On a donc

- 2004 est multiple de 3, donc d'après le a. $2^{2004} - 1$ est divisible par $2^3 - 1 = 7$;
- 2004 est multiple de 3 et de 2, donc de 6 ; d'où $2^{2004} - 1$ est divisible par $2^6 - 1 = 63$;
- On vient de voir que $2^{2004} - 1 = 63k = 9 \times (7k)$, donc $2^{2004} - 1$ est divisible par 9.

3. (a) $m = dm'$ et $n = dn'$. Puisque d est le plus grand diviseur commun à m et n , on sait que m' et n' sont premiers entre eux. D'après Bezout il existe $(u, v) \in \mathbb{Z}^2$ tel que

$$m'u - n'v = 1 \iff m'ud - n'vd = d \iff mu - nv = d$$

- (b) Avec u et v positifs, l'égalité précédente peut s'écrire $mu = nv + d$.

$$\text{D'où : } (a^{mu} - 1) - (a^{nv} - 1)a^d = (a^{nv+d} - 1) - (a^{nv} - 1)a^d = (a^{nv} \times a^d - 1) - (a^{nv} - 1)a^d = (a^{nv} \times a^d) - 1 - (a^{nv} \times a^d) + a^d = a^d - 1.$$

Le PGCD de $a^{mu} - 1$ et $a^{nv} - 1$ divise aussi $a^{mu} - 1$ et $(a^{nv} - 1)a^d$ (et c'est le plus grand diviseur) donc leur différence qui est $a^d - 1$.

Donc le PGCD de $(a^{mu} - 1) - (a^{nv} - 1)a^d$ et de $a^{nv} - 1$ est égal au PGCD de $a^d - 1$ et de $a^{nv} - 1$. Nous avons vu à la question précédente que comme d divise n , $a^d - 1$ divise $a^{nv} - 1$.

Conclusion : le PGCD de $a^{mu} - 1$ et $a^{nv} - 1$ est égal à $a^d - 1$.

- (c) Application : $m = 63$, $n = 60$.

$$63 = 3^2 \times 7 \text{ et } 60 = 2 \times 3 \times 5. \text{ Donc PGCD}(63 ; 60) = 3.$$

$$\text{On a } m = 63 = 3 \times 21 = 3m' \text{ et } n = 60 = 3 \times 20 = 3n'.$$

D'autre part 21 et 20 sont premiers et on trouve facilement

$$u = 1, v = 1 \text{ tels que } 21 \times 1 - 20 \times 1 = 1.$$

Donc $mu - nv = 63 - 60 = 3 = \text{PGCD}(63 ; 60)$. En appliquant le résultat de la question précédente :

$$\text{PGCD}(2^{63} - 1 ; 2^{60} - 1) = 2^3 - 1 = 7.$$