www.freemaths.fr

Maths Expertes
Terminale

PGCD, Bézout & Gauss

CORRIGÉ DE L'EXERCICE

PGCD

12

Correction

Rappelons que si $a = bq + r$ désigne la division euclidienne de *a* par *b* : $\text{PGCD}(a\,;b) = \text{PGCD}(b\,;r)$.

1. Montrons l'existence de l'entier *c* :

NB. Notons que dans la formule qui nous est proposée, nous lisons « $\left[(2^b)^c - 1\right] \times 2^r + 2^r$ ». Le nombre 2^r a été « retranché et ajouté ». Nous serons sans nul doute amenés à procéder à cette astuce de calcul pour obtenir le résultat attendu …

Soit $a = b \times q + r$ la division euclidienne de *a* par *b*, conformément à ce que nous avons dit dans notre préambule. Considérons la puissance de 2 dont l'exposant est égal à *a* et écrivons-la de deux façons :

$$2^a = 2^{bq+r}$$

En vertu des règles de calcul sur les puissances : $\begin{cases} 2^{bq+r} = 2^{bq} \times 2^r \\ 2^{bq} = (2^b)^q \end{cases}$ donc $2^{bq+r} = (2^b)^q \times 2^r$.

Retranchons et ajoutons le nombre 2^r :

$$2^{bq+r} = (2^b)^q \times 2^r = (2^b)^q \times 2^r - 2^r + 2^r$$

Factorisons partiellement par 2^r :

$$2^a = 2^{bq+r} = \left[(2^b)^q - 1\right] \times 2^r + 2^r$$

Retranchons 1 à chaque membre de ces égalités :

$$2^a - 1 = 2^{bq+r} - 1 = \left[(2^b)^q - 1\right] \times 2^r + 2^r - 1$$

Comme nous l'avons noté en préambule, vu que $a > b$, ce quotient *q* de la division euclidienne de *a* par *b* est un entier au moins égal à 1. Nous avons obtenu avec $c = q$ le résultat escompté.

Il existe un entier strictement positif *c,* qui n'est autre que le quotient *q* de la division euclidienne de *a* par *b*, tel que : $2^a - 1 = \left[(2^b)^c - 1\right] \times 2^r + 2^r - 1$

2. Vérifions l'identité que l'énoncé nous propose :

Appliquons l'identité rappelée en préambule avec $n = c$ et avec $x = 2^b$:

$$(2^b)^c - 1 = (2^b - 1)\left((2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1\right)$$

3. Déduisons-en une relation entre divers PGCD :

Des relations démontrées aux questions 1 et 2, à savoir :

$$\begin{cases} 2^a - 1 = \left[(2^b)^c - 1\right] \times 2^r + 2^r - 1 \\ (2^b)^c - 1 = (2^b - 1)\left((2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1\right) \end{cases}$$

nous pouvons déduire la relation :

$$2^a - 1 = \left[(2^b - 1)\left((2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1\right)\right] \times 2^r + 2^r - 1$$

Autrement dit :

$$2^a - 1 = \left[2^r\left((2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1\right)\right] \times (2^b - 1) + (2^r - 1)$$

Désignons par *Q* le nombre entier : $Q = 2^r\left((2^b)^{c-1} + (2^b)^{c-2} + \cdots + 2^b + 1\right)$

Les trois nombres $A = 2^a - 1$; $B = 2^b - 1$ et $R = 2^r - 1$ sont liés par la relation : $A = BQ + R$.

Nous avons vu que $0 < r < b$, donc $1 < 2^r < 2^b$ et $0 < 2^r - 1 < 2^b - 1$, autrement dit $0 < R < B$.

Le nombre *R* est un nombre positif strictement plus petit que *B*. La relation $A = BQ + R$ est l'écriture authentique d'une division euclidienne, celle de *A* par *B*, division dans laquelle le nombre *R* est le reste.

D'après le cours, nous savons que : $\text{PGCD}(A\ ; B) = \text{PGCD}(B\ ; R)$

Avec les notations originelles :

$$\text{PGCD}\left(2^a - 1\ ;\ 2^b - 1\right) = \text{PGCD}\left(2^b - 1\ ;\ 2^r - 1\right)$$

4. Justifions que : $\text{PGCD}\left(2^a - 1\ ;\ 2^b - 1\right) = 2^d - 1$:

L'algorithme d'Euclide itère le procédé de la question précédente tant que le reste de la division euclidienne courante est non nul. Nous obtenons des relations de la forme :

$\text{PGCD}\left(2^a - 1\ ;\ 2^b - 1\right) = \cdots = \text{PGCD}(2^{r_{k-1}} - 1\ ;\ 2^{r_k} - 1)$ où r_{k-1} ; r_k sont deux restes successifs de l'algorithme d'Euclide appliqué aux entiers *a* et *b*.

Il reste à voir ce qu'il se passe lorsque le reste de la division euclidienne courante est nul (au niveau du PGCD *d* de *a* et de *b*) c'est-à-dire lorsque cette division se présente sous la forme : $r_{n-1} = q_n d$.

Alors, à ce niveau : $2^{r_{n-1}} - 1 = 2^{q_n d} - 1 = \left(2^d - 1\right)\left(1 + 2^d + \cdots + 2^{(q_n - 1)d}\right)$.

Le nombre $2^{r_{n-1}} - 1$ est un multiple de $2^d - 1$, le PGCD de ces deux nombres est $2^d - 1$.

En fin de compte :

$$\text{PGCD}\left(2^a - 1\ ;\ 2^b - 1\right) = \cdots = \text{PGCD}\left(2^{r_{n-1}} - 1\ ;\ 2^d - 1\right) = 2^d - 1$$

5. Déterminons le PGCD de 2020 et de 1996 :

Une option parmi d'autres est de s'aider d'un modeste algorithme « Python » :

```
>>> def euclide(a,b):
        r=a%b
        q=int((a-b)/r)
        while r>0:
                print(a,"=",q,"x",b,"+",r)
                a=b
                b=r
                r=a%b
                q=int((a-r)/b)
        print("Le PGCD est égal à",b)
```

```
>>> euclide(2020,1996)
2020 = 1 x 1996 + 24
1996 = 83 x 24 + 4
Le PGCD est égal à 4
```

6. Déduisons-en le PGCD de $2^{2020} - 1$ et de $2^{1996} - 1$:

Utilisons le résultat de la **question 4**. Sachant que $\text{PGCD}(2020\ ;\ 1996) = 4$:

$$\text{PGCD}(2^{2020} - 1\ ;\ 2^{1996} - 1) = 2^4 - 1 = 15$$

NB. Une recherche directe à l'aide de l'algorithme Python de la **question 5** déclenche en principe un message d'erreur : « OverflowError: integer division result too large for a float ».

En revanche, TI-Nspire confirme le résultat que nous avons trouvé.

$$\gcd\left(2^{2020}-1, 2^{1996}-1\right) \qquad 15$$