Maths Expertes
Terminale

Arithmétique

CORRIGÉ DE L'EXERCICE

Arithmétique, Synthèse

24

Correction

1. Démontrons l'identité $(x-1)(1+x+\cdots+x^{k-1}) = x^k - 1$:

Appliquons une première fois la distributivité de la multiplication sur l'addition :

$$(x-1)(1+x+\cdots+x^{k-1}) = (x-1) + x(x-1) + \cdots + x^{k-1}(x-1)$$

Appliquons cette propriété de distributivité à chacun des termes $x(x-1), \ldots,\ x^{k-1}(x-1)$:

$$(x-1)(1+x+\cdots+x^{k-1}) = x - 1 + x^2 - x + \cdots + x^k - x^{k-1}$$

Tous les termes intermédiaires s'éliminent deux à deux (on parle d'« effet domino »), il ne reste que les termes d'exposants extrêmes, soit :

$$(x-1)(1+x+\cdots+x^{k-1}) = x^k - 1$$

NB. Désormais, on pose $x = a$, a étant un entier supérieur ou égal à 2.

2.a. Montrons que, si *d* est un diviseur de *n*, $a^d - 1$ est un diviseur de $a^n - 1$:

n est un entier strictement positif et *d* est un diviseur positif de *d*, c'est-à-dire qu'il existe un entier strictement positif *k* vérifiant $n = kd$.

Appliquons l'identité de la **question 1** avec l'entier *k* ainsi défini et avec $x = a^d$:
Cette identité permet d'écrire : $(a^d - 1)\left(1 + a^d + \cdots + (a^d)^{k-1}\right) = (a^d)^k - 1$.

Or, $(a^d)^k = a^{dk} = a^n$. Nous obtenons : $(a^d - 1)\left(1 + a^d + \cdots + (a^d)^{k-1}\right) = a^n - 1$

Les nombres $a^d, \ldots, (a^d)^{k-1}$ sont tous des entiers strictement positifs.
Leur somme $K = 1 + a^d + \cdots + (a^d)^{k-1}$ est donc un nombre entier strictement positif.

Il existe un entier *K* strictement positif vérifiant la relation $a^n - 1 = K(a^d - 1)$. Ce qui prouve :

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

2.b. Prouvons que $2^{2004} - 1$ est divisible par 63 :

NB. L'énoncé nous demande de prouver que « $2^{2004} - 1$ est divisible par 7, par 63 puis par 9 », curieusement dans cet ordre. Or, il y a une hiérarchie entre ces trois nombres. En effet, 63 est un multiple de 7 et de 9 puisque 63 est le produit de ces deux nombres. Tout multiple de 63 est un multiple de 7 et de 9.
C'est pourquoi la démonstration clef consiste à montrer que $2^{2004} - 1$ est divisible par 63. La divisibilité par 63 impliquera à la fois la divisibilité par 7 et celle par 9.
Notons à cet effet que $63 = 64 - 1 = 2^6 - 1$, relation que nous allons exploiter.

L'entier 2004 est un multiple de 6. En effet, cet entier est un entier pair dont les chiffres vérifient le critère de divisibilité par 3. Précisément, nous avons : $2004 = 6 \times 334$.

Nous pouvons appliquer le résultat de la **question 2.a** avec $a = 2$; $n = 2004$; $d = 6$; $k = 334$:

Il existe un entier *K* vérifiant la relation $2^{2004} - 1 = K(2^6 - 1)$, soit la relation : $2^{2004} - 1 = 63K$.
Il s'agit de l'entier $K = 1 + 2^6 + \cdots + (2^6)^{333}$.

Donc, le nombre $2^6 - 1 = 63$ est un diviseur de $2^{2004} - 1$.

Le nombre $2^{2004} - 1$ est divisible par 63. Par voie de conséquence, il est divisible par 7 et il est divisible par 9.

3. Dans cette question, les entiers *m* et *n* sont deux entiers naturels non nuls et *d* est leur PGCD. L'entier *a* est un entier au moins égal à 2.

3.a. Montrons qu'il existe deux entiers relatifs *u* et *v* tels que $mu - nv = d$:

Définissons, comme indiqué dans l'énoncé, *m'* et *n'* par les relations : $m = dm'$ et $n = dn'$.

Ces deux entiers *m'* et *n'* sont premiers entre eux car, s'ils ne l'étaient pas, ils auraient un diviseur commun *k* strictement plus grand que 1 et l'entier *kd* serait un diviseur commun à *m* et à *n* strictement plus grand que *d*, ce qui serait contraire au statut de PGCD du diviseur *d*.

Le fait que *m'* et *n'* soient premiers entre eux étant justifié, nous sommes en droit d'appliquer à ces deux entiers le théorème de Bézout. Il existe deux entiers relatifs *u'* et *v'* tels que : $m'u' + n'v' = 1$.

Multiplions par *d* les deux membres de cette égalité :

$$d(m'u' + n'v') = (dm')u' + (dn')v' = d$$

.

Or $m'd = m$; $n'd = n$. Si en outre nous choisissons : $u = u'$; $v = -v'$, nous obtenons l'égalité :

$$mu - nv = d$$

Soit *d* le PGCD des entiers *m* et *n*. Il existe deux entiers relatifs *u* et *v* vérifiant $mu - nv = d$

NB. Cette relation s'écrit aussi bien : $mu = nv + d$

3.b. Montrons que $(a^{mu}-1)-(a^{nv}-1)\times a^d = a^d - 1$:

NB. Les entiers *u* et *v* étant supposés strictement positifs, les exposants *mu* et *nv* que nous affectons à *a* sont strictement positifs, les nombres a^{mu} et a^{nv} sont des nombres entiers au moins égaux à 2. Il en est de même du nombre a^d. Les nombres $a^{mu}-1$; $a^{nv}-1$; a^d-1 sont tous trois des entiers strictement positifs.

Les entiers *u* et *v*, introduits dans la question précédente, vérifient : $mu = nv + d$. En conséquence :

$$(a^{mu}-1)-(a^{nv}-1)\times a^d = (a^{mu}-1)-\left(a^{nv+d}-a^d\right) = a^{mu}-1-a^{mu}+a^d.$$

Nous obtenons comme prévu :

$$(a^{mu}-1)-(a^{nv}-1)\times a^d = a^d-1$$

.

3.c. Montrons que a^d-1 est le PGCD de $a^{mu}-1$ et de $a^{nv}-1$:

NB. Pour montrer qu'un entier strictement positif Δ est le PGCD de deux entiers non nuls *a* et *b*, on peut vérifier les deux propriétés suivantes :

- Δ est un diviseur commun à *a* et à *b*.
- Tout diviseur commun à *a* et à *b* divise Δ.

En effet, s'il en est ainsi, pour tout diviseur commun à *a* et à *b* positif *D*, il existe un entier non nul *k* tel que $\Delta = kD$, donc $\Delta \geq D$ et de ce fait parmi les diviseurs communs positifs, Δ est le plus grand. Ces deux propriétés vérifiées simultanément caractérisent le PGCD.

- L'entier strictement positif *d* étant le PGCD de *m* et de *n*, il divise *mu* et il divise *nv*. D'après le résultat de la question 2.a, le nombre $\Delta = a^d-1$ divise $a^{mu}-1$ et divise $a^{nv}-1$, il est un diviseur commun à $a^{mu}-1$ et à $a^{nv}-1$.
- Soit *D* un diviseur positif commun à $a^{mu}-1$ et à $a^{nv}-1$. Alors, il divise leur combinaison entière $(a^{mu}-1)-(a^{nv}-1)\times a^d$ vue à la question précédente. Il en résulte que *D* divise a^d-1. Tout diviseur *D* positif commun à $a^{mu}-1$ et de $a^{nv}-1$ divise a^d-1.

Les deux propriétés que nous venons d'évoquer sont simultanément vérifiées.

Le nombre $\Delta = a^d-1$ est le PGCD de $a^{mu}-1$ et de $a^{nv}-1$

3.d. Déterminons le PGCD de $2^{63}-1$ et de $2^{60}-1$:

Le PGCD de 63 et de 60 est 3. En effet, 3 est diviseur commun à 60 et à 63 et tout diviseur commun à 60 et à 63 divise leur différence $63-60=3$.

Nous pouvons appliquer les résultats de l'exercice avec $a=2$, $m=63, n=60, d=3$, $u=v=1$.

En vertu de ces résultats, le PGCD de $2^{63}-1$ et de $2^{60}-1$ est le nombre 2^3-1.

Le PGCD de $2^{63}-1$ et de $2^{60}-1$ est égal à 7.