Algèbre et Arithmétique 1

Corrigé de l'interrogation n°5 : mardi 23 novembre 2010

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits. Justifiez toutes vos réponses.

Durée : 30 minutes

NOM :
PRÉNOM :

Exercice 1

1. *Énoncer (sans démonstration) le théorème définissant la division euclidienne des entiers relatifs.*

   Soient a et b des entiers relatifs, b étant supposé non nul. Il existe alors un unique couple $(q, r) \in \mathbb{Z}^2$ vérifiant les deux propriétés suivantes :
   - $a = b\,q + r$
   - $0 \leqslant r \leqslant |b| - 1$

2. *Démontrer que si a, b et c sont des entiers relatifs tels que $a \mid b$ et $b \mid c$, alors $a \mid c$.*

   Comme a divise b, il existe un entier relatif k tel que $b = a.k$. Comme b divise c, il existe un entier relatif k' tel que $c = b.k'$. On a alors $c = b.k' = (a.k).k'$ soit finalement $c = a.(k.k')$. Comme $k.k'$ est un entier relatif, cette dernière relation montre que a divise c.

Exercice 2

Calculer (par un algorithme) le PGCD d de 91 et 399 et des entiers u et v tels que $91u + 399v = d$. (Le détail des calculs devra être indiqué).

Appliquons l'algorithme d'Euclide. Les restes successifs sont indiqués en gras.

$$\begin{aligned}
\mathbf{399} &= 4 \times \mathbf{91} + \mathbf{35}\\
\mathbf{91} &= 2 \times \mathbf{35} + \mathbf{21}\\
\mathbf{35} &= 1 \times \mathbf{21} + \mathbf{14}\\
\mathbf{21} &= 1 \times \mathbf{14} + \mathbf{7}\\
\mathbf{14} &= 2 \times \mathbf{7} + 0
\end{aligned}$$

Le dernier reste non nul est 7, on a donc $\operatorname{pgcd}(91, 399) = 7$.

Pour trouver des entiers u et v convenables on peut « remonter » l'algorithme d'Euclide.

$$\begin{aligned}
\mathbf{7} &= \mathbf{21} - \mathbf{14} \\
&= \mathbf{21} - (\mathbf{35} - \mathbf{21}) \\
&= -\mathbf{35} + 2 \times \mathbf{21} \\
&= -\mathbf{35} + 2 \times (\mathbf{91} - 2 \times \mathbf{35}) \\
&= 2 \times \mathbf{91} - 5 \times \mathbf{35} \\
&= 2 \times \mathbf{91} - 5 \times (\mathbf{399} - 4 \times \mathbf{91}) \\
&= -5 \times \mathbf{399} + 22 \times \mathbf{91}.
\end{aligned}$$

Ainsi $u = 22$ et $v = -5$ conviennent.

Autre possibilité pour déterminer un couple (u, v) *convenable :* on applique l'algorithme d'Euclide étendu : en parallèle de l'algorithme d'Euclide, dont les quotients successifs sont 4, 2, 1, 1, on remplit le tableau suivant (ici ce sont les quotients qui sont écrits en gras)

$$\begin{array}{rrrl}
 & 1 & 0 & \\
 & 0 & 1 & \\
1 - \mathbf{4} \times 0 = & 1 & -4 & = 0 - \mathbf{4} \times 1 \\
0 - \mathbf{2} \times 1 = & -2 & 9 & = 1 - \mathbf{2} \times (-4) \\
1 - \mathbf{1} \times (-2) = & 3 & -13 & = -4 - \mathbf{1} \times 9 \\
-2 - \mathbf{1} \times 3 = & -5 & 22 & = 9 - \mathbf{1} \times (-13)
\end{array}$$

Ainsi $u = 22$ et $v = -5$ conviennent.

Exercice 3

1. *Soit $x \in \mathbb{Z}$ un entier. Montrer que $x^2 \equiv 0 \pmod 4$ ou $x^2 \equiv 1 \pmod 4$.*
   Tout entier x est congru modulo 4 au reste de sa division euclidienne par 4, donc est congru modulo 4 à 0, 1, 2 ou 3.
   – si $x \equiv 0 \pmod 4$, on a $x^2 \equiv 0^2 \pmod 4$, soit $x^2 \equiv 0 \pmod 4$
   – si $x \equiv 1 \pmod 4$, on a $x^2 \equiv 1^2 \pmod 4$, soit $x^2 \equiv 1 \pmod 4$
   – si $x \equiv 2 \pmod 4$, on a $x^2 \equiv 2^2 \equiv 4 \pmod 4$, soit $x^2 \equiv 0 \pmod 4$
   – si $x \equiv 3 \pmod 4$, on a $x^2 \equiv 3^2 \equiv 9 \pmod 4$, soit $x^2 \equiv 1 \pmod 4$
   Autre démonstration possible : Si x est pair, il existe $y \in \mathbb{Z}$ tel que $x = 2\,y$. Alors $x^2 = 4\,y^2$ donc $x^2 \equiv 0 \pmod 4$.
   Si x est impair, il existe $y \in \mathbb{Z}$ tel que $x = 2\,y+1$. Alors $x^2 = 4\,y^2+4\,y+1 = 4\,(y^2+y)+1$ donc $x^2 \equiv 1 \pmod 4$.
2. *Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Quel est le reste de la division euclidienne de $2^n - 1$ par 4 ?*
   On a $2^n = 2^2.2^{n-2} = 4.2^{n-2}$. Comme on a supposé $n \geqslant 2$, 2^{n-2} est un entier. Ainsi 4 divise 2^n. On a alors
   $$2^n - 1 \equiv 0 - 1 \equiv 3 \pmod 4$$
   et comme $0 \leqslant 3 \leqslant 4 - 1$, le reste cherché est 3.

3. *Quels sont les entiers $n \in \mathbb{N}$ tels que 2^n-1 est le carré d'un entier naturel ? (Indication : dans le cas où $n \geqslant 2$, on pourra utiliser les deux questions précédentes).*

   Soit $n \in \mathbb{N}$ tel que $n \geqslant 2$. Supposons que $2^n - 1$ soit le carré d'un entier naturel. D'après la première question, le reste de la division euclidienne de $2^n - 1$ par 4 est 0 ou 1. D'après la deuxième question, c'est 3 : contradiction. Ainsi $2^n - 1$ n'est pas le carré d'un entier naturel si $n \geqslant 2$.

   Si $n = 0$, $2^0 - 1 = 0 = 0^2$ est le carré d'un entier naturel.

   Si $n = 1$, $2^1 - 1 = 1 = 1^2$ est le carré d'un entier naturel.

   Ainsi, les entiers naturels n tels que $2^n - 1$ est le carré d'un entier naturel sont 0 et 1.