Lycée J.P Vernant
spéTS

Année scolaire 2010-2011
Mathématiques

CORRECTION DU DEVOIR SURVEILLE N° 2

SUJET (a)

Exercice 1 :

1. (a) $1404 = 481 \times 2 + 442$; $481 = 1 \times 442 + 39$; $442 = 39 \times 11 + 13$; $39 = 13 \times 3 + 0$. Le dernier reste non nul dans la suite des divisions successives est 13 donc $PGCD(481\,,\,1404) = 13$.

   (b) D'après les calculs précédents :

   $$\begin{aligned} 13 &= 442 - 39 \times 11 = 442 - (481 - 442) \times 11 = 12 \times 442 - 11 \times 481 \\ &= 12 \times (1404 - 2 \times 481) - 11 \times 481 = 12 \times 1404 - (24 + 11) \times 481 = 12 \times 1404 - 35 \times 481 \end{aligned}$$

   On a obtenu $481u + 1404v = 13$ avec $(u\,;\,,\,v) = (-35\,;\,12)$.

2. (a) Théorème de Bézout : Soit a et b des entiers naturels. a et b sont premiers entre eux si eu seulement s'il existe un couple $(u\,;\,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$.

   Démonstration :
   - On suppose a et b premiers entre eux. Alors $PGCD(a\,;\,b) = 1$. D'après l'identité de Bézout, il exsite un couple d'entiers $(u\,;\,v)$ tels que $au + bv = PGCD(a\,;\,b) = 1$; ce qui démontre le sens direct du théorème de Bézout.
   - On suppose qu'il existe un couple $(u\,;\,v) \in \mathbb{Z}^2$ tel que $au + bv = 1$ et on note $d = PGCD(a\,;\,b)$. Alors d divise a et d divise b donc d divise $au + bv$ puisque a et b sont des entiers. Ainsi, d divise 1 donc $d = 1$. Les nombres a et b sont donc premiers entre eux, ce qui justifie le sens réciproque du théroème de Bézout.

   (b) Soit $n \in \mathbb{N}$ quelconque. Alors : $n^2 - (n+1)(n-1) = n^2 - (n^2 - 1) = 1$ donc on a trouvé un couple $(u\,;\,v) = (1\,;\,-(n-1)) \in \mathbb{Z}^2$ tel que $n^2u + (n+1)v = 1$. D'après le théorème de Bézout (sens réciproque), on peut donc affirmer que $n+1$ et n^2 sont premiers entre eux.

3. (a) $n^2 + n - 9 = (n-2)n + 3n - 9$ donc $PGCD(n^2 + n - 9\,;\,n-2) = PGCD(n-2\,;\,3n-9)$ d'après le lemme d'Euclide puis $3n - 9 = 3(n-2) - 3$ donc toujours avec le lemme d'Euclide, on sait que $PGCD(3n-9\,;\,n-2) = PGCD(n-2\,;\,-3) = PGCD(n-2\,;\,3)$. Or, $PGCD(n-2\,;\,3)$ est un diviseur positif de 3 donc il vaut soit 1 soit 3. $PGCD(n-2\,;\,3) = 3$ si et seulement si 3 divise $n-2$, c'est-à-dire $n \equiv 2\ [3]$. Finalement, $PGCD(n^2 + n - 9\,;\,n-2) = \begin{cases} 3 \text{ si } n \equiv 2\ [3] \\ 1 \text{ sinon} \end{cases}$.

   (b) On pose $P(x) = x^2 + x - 6$ et on remarque que $P(2) = 2^2 + 2 - 6 = 0$ donc $x_1 = 2$ est une racine de $P(x)$. L'autre racine x_2 vérifie $x_1 \times x_2 = \dfrac{c}{a} = -6$ d'où $x_2 = \dfrac{-6}{2} = -3$. Ainsi, $P(x) = (x-2)(x+3)$. En particulier, $n^2 + n - 6 = (n-2)(n+3)$. Essayons alors de multiplier $n^2 + n - 9$ par ce même facteur $n+3$.

   $$(n^2 + n - 9)(n+3) = n^3 + 3n^2 + n^2 + 3n - 9n - 27 = n^3 + 4n^2 - 6n - 27$$

   Finalement,

   $$\begin{aligned} PGCD(n^3 + 4n^2 - 6n - 27\,;\,n^2 + n - 6) &= PGCD((n+3)(n^2 + n - 9)\,;\,(n+3)(n-2)) \\ &= |n+3|\,PGCD(n^2 + n - 9\,;\,n-2) \\ &= \begin{cases} 3|n+3| \text{ si } n \equiv 2\ [3] \\ |n+3| \text{ sinon} \end{cases} \quad \text{(question précédente)} \end{aligned}$$

4. (a) On fait un tableau à double entrée modulo 3 et on met dans les cases le résultat de x^2+y^2 modulo 3.

$y \backslash x$	0	1	2
0	0	1	$4 \equiv 1$ [3]
1	1	2	$5 \equiv 2$ [3]
2	$4 \equiv 1$ [3]	$5 \equiv 2$ [3]	$8 \equiv 2$ [3]

On remarque que la seule case pour laquelle le résultat est nul est celle pour x et y congrus à 0 modulo 3 donc tous les couples $(x\,;\,y)$ vérifiant $x^2+y^2 \equiv 0$ [3] sont des couples de multiples de 3.
La phrase est FAUSSE

(b) **La phrase est FAUSSE**
En effet pour $a=6$ et $b=7$, alors $2\times 6-1\times 7=12-7=5$ en choisissant $(u\,;\,v)=(2\,;\,-1)\in\mathbb{Z}^2$ et pourtant $PGCD(6\,;\,7)\neq 5$ (5 ne divise ni 6 ni 7 !)

(c) On choisit $a=3$ et $b=5$. Ce sont deux nombre premiers donc ils sont premiers entre eux. De plus, $3a+b=3\times 3+5=9+5=14$ et $a-2b=3-10=-7$. Ces deux nombres sont divisibles par 7 donc ils ne sont pas premiers entre eux. On a donc trouvé un contre-exemple pour le sens réciproque.
La phrase est FAUSSE

Exercice 2 :

1. (a)
- $3^1=3$ donc pour $n=1$, le reste de la division euclidienne de 3^n par 7 est 3.
- $3^2=9$ et $9\equiv 2$ [7] donc pour $n=2$, le reste de la division euclidienne de 3^n par 7 est 2.
- $3^3=3^2\times 3\equiv 2\times 3$ [7] donc $3^3\equiv 6$ [7]. Pour $n=3$, le reste de la division euclidienne de 3^n par 7 est 6.
- $3^4=(3^2)^2\equiv 2^2$ [7] soit $3^4\equiv 4$ [7]. Pour $n=4$, le reste de la division euclidienne de 3^n par 7 est 4.
- $3^5=3^4\times 3\equiv 4\times 3$ [7]. Or, $12\equiv 5$ [7] donc $3^5\equiv 5$ [7] par transitivité. Pour $n=5$, le reste de la division euclidienne de 3^n par 7 est 5.
- $3^6=(3^2)^3\equiv 2^3$ [7]. Or, $2^3=8\equiv 1$ [7] donc $3^6\equiv 1$ [7]. Pour $n=6$, le reste de la division euclidienne de 3^n par 7 est 1.

(b) Pour tout $n\in\mathbb{N}^*$, $3^{n+6}=3^n\times 3^6$. Or, on a déjà remarqué que $3^6\equiv 1$ [7] d'où $3^{n+6}\equiv 3^n$ [7], ce qui équivaut à dire que $3^{n+6}-3^n$ est divisible par 7.
Comme $3^n\equiv 3^{n+6}$ [7], par définition de la congruence, les nombres 3^n et 3^{n+6} ont le même reste dans la division par 7.

(c) On fait la division euclidienne de 1000 par 6 : $1000=6\times 166+4$.
Ainsi, $3^{1000}=3^{6\times 166+4}=(3^6)^{166}\times 3^4$. Or, $3^6\equiv 1$ [7] donc $(3^6)^{166}\equiv 1$ [7] puis $3^{1000}\equiv 3^4$ [7]. D'après la question (a), $3^4\equiv 4$ [7] donc $3^{1000}\equiv 4$ [7]. Le reste de la division euclidienne de 3^{1000} par 7 est égal à 4.

(d) Pour n quelconque, on détermine le reste r de la division euclidienne de n par 6 : il existe un couple $(q\,,\,r)$ d'entiers tels que $n=6q+r$ avec $0\leqslant r<6$. Alors $3^n=(3^6)^q\times 3^r$. Or, $3^6\equiv 1$ [7] donc $(3^6)^q\equiv 1$ [7] et $3^n\equiv 3^r$ [7]. Comme r est un entier compris entre 0 et 5, on a déjà calculé les restes de la division euclidienne de 3^r par 7 à la question 1. a). Ainsi, en utilisant les résultats du 1. a) :
- Si $n\equiv 0$ [6], alors $r=0$ et $3^n\equiv 3^0$ [7] soit $3^n\equiv 1$ [7].
- Si $n\equiv 1$ [6] alors $r=1$ et $3^n\equiv 3$ [7].
- Si $n\equiv 2$ [6] alors $r=2$ et $3^n\equiv 3^2$ [7] soit $3^n\equiv 2$ [7].
- Si $n\equiv 3$ [6], alors $r=3$ et $3^n\equiv 3^3$ [7] soit $3^n\equiv 6$ [7].
- Si $n\equiv 4$ [6], alors $r=4$ et $3^n\equiv 3^4$ [7] soit $3^n\equiv 4$ [7].
- Si $n\equiv 5$ [6], alors $r=5$ et $3^n\equiv 3^5$ [7] soit $3^n\equiv 5$ [7].

(e) Comme les seuls diviseurs positifs de 7 sont 1 et 7, alors $PGCD(3^n\,;\,7)$ vaut soit 1 soit 7. Il sera égal à 7 si et seulement si 3^n est multiple de 7, c'est-à-dire $3^n\equiv 0$ [7]. D'après les résultats de la question précédente, on remarque que quelque soit $n\in\mathbb{N}$, le reste de la division euclidienne de

3^n par 7 n'est jamais égal à 0. Par conséquent, 7 ne divise jamais 3^n donc 3^n et 7 sont premiers entre eux.

2. (a) On considère la suite (u_n) définie pour tout $n \in \mathbb{N}$ par $u_n = 3^n$.
Comme $u_{n+1} = 3^{n+1} = 3 \times 3^n = 3u_n$ pour tout $n \in \mathbb{N}$, alors (u_n) est géométrique de raison 3 et A_n est la somme des n premiers termes de la suite (u_n) : $A_n = u_0 + u_1 + \cdots + u_{n-1}$.

$$A_n = \text{premier terme} \times \frac{1 - \text{raison}^{\text{nombre de termes}}}{1 - \text{raison}} = 3^0 \times \frac{1 - 3^n}{1 - 3} = \frac{3^n - 1}{2}$$

Ainsi, $3^n - 1 = 2A_n$. Si A_n est divisible par 7, alors $2A_n$ est aussi divisible par 7 donc $3^n - 1$ est divisible par 7.

(b) On suppose que $3^n - 1$ est divisible par 7, donc 7 divise $2A_n$. Or, $PGCD(2\,;7) = 1$ (en effet 7 n'est pas pair) ; on peut donc utiliser le théorème de Gauss pour affirmer que 7 divise A_n.
On a donc montré une double implication dans les questions 2. a) et 2. b), par conséquent,

$$A_n \text{ est divisible par } 7 \;\Leftrightarrow\; 3^n - 1 \text{ est divisible par } 7 \;\Leftrightarrow\; 3^n \equiv 1\ [7]$$

Avec les résultats du 1. d), on remarque que $3^n \equiv 1\ [7]$ si et seulement si $n \equiv 0\ [6]$ donc finalement, A_n est divisible par 7 si et seulement si n est un mutiple de 6.

Exercice 3 :

PARTIE A

1. Théorème de Gauss : Si a divise bc et que $PGCD(a\,;b) = 1$ alors a divise c.

Démonstration :

Comme $PGCD(a\,;b) = 1$ alors il existe un couple d'entiers $(u\,;v) \in \mathbb{Z}^2$ tels que $au + bv = 1$ d'après le théorème de Bézout. En mutipliant par c, on obtient : $auc + bvc = c$. Comme $(uv) \in \mathbb{Z}$ alors a divise (auc). De plus, a divise bc et $v \in \mathbb{Z}$ d'où a divise bcv. On en déduit que a divise $auc + bvc$ soit a divise c.

2. Si a et b sont premiers entre eux, N est divisible par ab si et seulement si N est divisible par a et N est divisible par b.

Démonstration :

- On suppose que N est divisible par ab. Comme $b \in \mathbb{Z}$, b divise ab et comme ab divise N, alors b divise ab par transitivité. De même, a divise ab et ab divise N d'où a divise N. Finalement, N est divisible par a et par b.
- On suppose que N est divisible par a et par b. Il existe donc $k \in \mathbb{Z}$ tel que $N = ka$ et il existe $k' \in \mathbb{Z}$ tels que $N = k'b$. Ainsi, $ka = k'b$. Comme $k \in \mathbb{Z}$, alors a divise $k'b$. On sait que $PGCD(a\,;b) = 1$ donc, d'après le théorème de Gauss, a divise k'. On en déduit qu'il existe que $p \in \mathbb{Z}$ tel que $k' = ap$. Par conséquent, $N = k'b = apb$, ce qui implique que N est divisible par ab (car $p \in \mathbb{Z}$).

3. $N \equiv 28\ [100] \;\Leftrightarrow$ 100 divise $N - 28$. On sait que $100 = 4 \times 25$ et on utilise l'algorithme d'Euclide pour déterminer $PGCD(25\,;4)$. Or, $25 = 4 \times 6 + 1$, $4 = 4 \times 1 + 0$ donc le dernier reste non nul dans ces successions de division euclidienne est 1 et $PGCD(25\,;4) = 1$. On peut utiliser la question précédente avec $a = 25$ et $b = 4$. Ainsi, 100 divise N si et seulement si 4 divise N et 25 divise N. Finalement,

$$N \equiv 28\ [100] \;\Leftrightarrow\; \begin{cases} N \equiv 28\ [4] \\ N \equiv 28\ [25] \end{cases}$$

Comme $28 = 7 \times 4$, alors $28 \equiv 0\ [4]$. De plus, $28 = 25 + 3$ donc $28 \equiv 3\ [25]$. On peut donc conclure par transitivité que

$$N \equiv 28\ [100] \;\Leftrightarrow\; \begin{cases} N \equiv 0\ [4] \\ N \equiv 3\ [25] \end{cases}$$

PARTIE B

1. $u_1 = 5u_0 - 6 = 5 \times 14 - 6 = 64$; $u_2 = 5 \times u_1 - 6 = 5 \times 64 - 6 = 314$; $u_3 = 5u_2 - 6 = 5 \times 314 - 6 = 1564$; $u_4 = 5 \times u_3 - 6 = 5 \times 1564 - 6 = 7814$.
   On peut conjecturer que les deux derniers chiffres de u_n sont soit 64, soit 14.

2. $u_{n+2} = 5u_{n+1} - 6 = 5(5u_n - 6) - 6 = 25u_n - 30 - 6 = 25u_n - 36$. Comme $25 = 6 \times 4 + 1$ alors $25 \equiv 1$ [4] et que $36 = 9 \times 4$ alors $36 \equiv 0$ [4]. Par conséquent, $25u_n - 36 \equiv u_n$ [4] soit $u_{n+2} \equiv u_n$ [4].
   On raisonne par récurrence en posant P_k : "$u_{2k} \equiv 2$ [4] et $u_{2k+1} \equiv 0$ [4]".
   - *initialisation*

     Pour $k = 0$, $u_{2k} = u_0 = 14 = 4 \times 3 + 2$ donc $u_0 \equiv 2$ [4] puis $u_{2k+1} = u_1 = 64 = 4 \times 16$ donc $u_1 \equiv 0$ [4]. On a ainsi montré que P_1 est vraie.
   - *étape d'hérédité*

     Soit $k \in \mathbb{N}$. On suppose que P_k est vraie c'est-à-dire que $u_{2k} \equiv 2$ [4] et $u_{2k+1} \equiv 0$ [4]. Montrons que P_{k+1} est vraie.
     $u_{2(k+1)} = u_{2k+2} \equiv u_{2k}$ [4] d'après ce qui a été montré au début de la question. Or, d'après P_k, $u_{2k} \equiv 2$ [4] donc $u_{2(k+1)} \equiv 2$ [4]. De même, $u_{2(k+1)+1} = u_{2k+3} \equiv u_{2k+1}$ [4] et $u_{2k+1} \equiv 0$ [4] donc $u_{2k+1} \equiv 0$ [4]. On a donc montré que P_{k+1} est vraie.
   - *conclusion*

     D'après le principe de récurrence, pour tout $k \in \mathbb{N}$, $u_{2k} \equiv 2$ [4] et $u_{2k+1} \equiv 0$ [4].

3. (a) On pose Q_n : "$2u_n = 5^{n+2} + 3$ pour tout $n \in \mathbb{N}$.
   - *initialisation*

     Pour $n = 0$, $5^{0+2} + 3 = 25 + 3 = 28 = 2 \times 14 = 2u_0$. La propriété P_0 est donc vraie.
   - *étape d'hérédite*

     Soit $n \in \mathbb{N}$. On suppose P_n vraie, c'est-à-dire que $2u_n = 5^{n+2} + 3$. Montrons que P_{n+1} est vraie.
     $2u_{n+1} = 2(5u_n - 6) = 2 \times 5u_n - 12 = 5 \times 2u_n - 12 = 5 \times (5^{n+2} + 3) - 12 = 5^{n+3} + 15 - 12 = 5^{n+3} + 3$.
     Finalement, P_{n+1} est vraie.
   - *conclusion*

     D'après le principe de récurrence, pour tout $n \in \mathbb{N}$, $u_n = 5^{n+2} + 3$.

   (b) On a déjà remarqué que $u_n \equiv 2$ [4] ou bien $u_n \equiv 0$ [4] donc $2u_n \equiv 4$ [4] ou bien $2u_n \equiv 0$ [4]. Comme $4 \equiv 4$ [0], alors dans tous les cas : $2u_n \equiv 0$ [4].
   Pour tout $n \in \mathbb{N}$, $2u_n = 5^{n+2} + 3 = 5^2 \times 5^n + 3 = 25 \times 5^n + 3$. Comme $25 \equiv 0$ [25], alors $5^n \times 25 \equiv 0$ [25] donc $5^n \times 25 + 3 \equiv 3$ [25] soit $2u_n \equiv 3$ [25].
   Comme $2u_n \equiv 0$ [4] et $2u_n \equiv 3$ [25] alors $2u_n \equiv 28$ [100] d'après la question 3 de la partie A.

4. (a) $200 = 25 \times 8$ et $25 = 8 \times 3 + 1$ donc d'après le lemme d'Euclide, $PGCD(25\,;\,8) = PGCD(8\,;\,1) = 1$.
   $2u_n \equiv 28$ [200] si et seulement si $2u_n - 28$ est divisible par $200 = 25 \times 8$. D'après une conséquence du théorème de Gauss, $2u_n - 28$ est divisible par 200 si et seulement si $2u_n - 28$ est divisible par 25 et par 8, c'est-à-dire $2u_n \equiv 28$ [25] et $2u_n \equiv 28$ [8].
   On peut donc conclure que $2u_n \equiv 28$ [200] $\Leftrightarrow \begin{cases} 2u_n \equiv 28 \text{ [25]} \\ 2u_n \equiv 28 \text{ [8]} \end{cases}$
   On a déjà montré que $2u_n \equiv 28$ [25] $\Leftrightarrow$ $2u_n \equiv 3$ [25]. En outre $28 = 3 \times 8 + 4$ donc $28 \equiv 4$ [8] et $2u_n \equiv 28$ [8] $\Leftrightarrow$ $2u_n \equiv 4$ [8]. On a déjà justifié que $2u_n \equiv 3$ [25]. De plus, si n est pair, on peut l'écrire sous la forme $n = 2k$ avec $k \in \mathbb{N}$ donc $u_n = u_{2k} \equiv 2$ [4] et $2u_n \equiv 4$ [8]. Finalement, on sait que $2u_n \equiv 28$ [25] et $2u_n \equiv 28$ [8] d'où $2u_n \equiv 28$ [200] (équivalence justifié précédemment).

   On sait que $2u_n \equiv 28$ [200] donc il existe $m \in \mathbb{Z}$ tel que $2u_n = 28 + 200m$ d'où $u_n = 14 + 100m$. Ainsi, $u_n \equiv 14$ [100]. Par définition de (u_n), $u_{n+1} = 5u_n - 6$. Comme $u_n \equiv 14$ [100] alors $5u_n \equiv 5 \times 14$ [100] soit $5u_n \equiv 70$ [100] puis $5u_n - 6 \equiv 64$ [100]. Finalement, $u_{n+1} \equiv 64$ [100].

   (b) Si n est pair, on a justifié que $u_n \equiv 14$ [100], ce qui signifie que les deus derniers chiffres de l'écriture décimale de u_n sont 14.

   Si n est impair, alors $n-1$ est pair et $u_n \equiv 64$ [500] d'après la question précédente. Par conséquent, il existe $p \in \mathbb{Z}$ tel que $u_n = 64 + 500p = 64 + 100 \times (5p)$ donc $u_n - 64$ est divisible par 100, ce qui

signifie que $u_n \equiv 64$ [100] et donc que les deux derniers chiffres de l'écriture décimale de u_n sont 64.

5. (a) – On suppose que u_n est divisible par 3. Alors 3 divise $5u_n$. Comme 3 divise aussi -6 alors 3 divise la somme $5u_n - 6 = u_{n+1}$
   – On suppose que u_{n+1} est divisible par 3. On sait que $5u_n = u_{n+1} + 6$. On sait que 3 divise 6 donc 3 divise $u_{n+1}+6 = 5u_n$. Or, $PGCD(3\,;\,5) = 1$ (en effet, 3 et 5 sont premiers donc premiers entre eux). D'après le théorème de Gauss, 3 divise u_n.

   On a justifié une double implication donc l'équivalence : u_{n+1} est divisible par 3 si et seulement si u_n est divisible par 3.

   (b) On sait que $u_{n+1} = 5u_n - 6$ donc en utilisant le lemme d'Euclide, $PGCD(u_{n+1}\,;\,u_n) = PGCD(u_n\,;\,6)$. Les diviseurs positifs de 6 sont 1, 2, 3 et 6 donc $PGCD(u_n\,;\,6)$ vaut soit 1, soit 2 soit 3, soit 6. On a montré que les deux derniers chiffres de u_n sont soit 14, soit 64 donc u_n est nécessairement un nombre pair. Ainsi, 2 est un diviseur commun de 6 et de u_n d'où $PGCD(6\,;\,u_n)$ est un mutiple de 2 : il ne reste plus que 2 et 6 comme possibilité.

   Montrons que : P_n : "3 ne divise pas u_n" est vraie pour tout $n \in \mathbb{N}$.
   – *initialisation*

     $u_0 = 14$ et 3 ne divise pas 14. P_0 est donc vraie.
   – *étape d'hérédite*

     Soit $n \in \mathbb{N}$. On suppose que P_n est vraie, c'est-à-dire que u_n n'est pas divisible par 3. Si u_{n+1} était divisible par 3, il en serait de même de u_n d'après la question 5.a). Cela contredit P_n d'où u_{n+1} n'est pas divisible par 3. P_{n+1} est donc vraie.
   – *conclusion* D'après le principe de récurrence, u_n n'est pas divisible par 3 quelque soit $n \in \mathbb{N}$.

   Comme 3 ne divise pas u_n, $PGCD(u_n\,;\,6)$ ne peut pas valoir 6. Finalement, pour tout $n \in \mathbb{N}$, $PGCD(u_n\,;\,6) = 2$ soit $PGCD(u_n\,;\,u_{n+1}) = 2$ pour tout $n \in \mathbb{N}$.

SUJET (b)

Seul l'exercice 1 était différent entre les deux sujets

Exercice 1 :

1. (a) $2176 = 561 \times 3 + 493$; $561 = 1 \times 493 + 68$; $493 = 68 \times 7 + 17$; $68 = 17 \times 4 + 0$. Le dernier reste non nul dans la suite des divisions successives est 17 donc $PGCD(561\,,\,2176) = 17$.

   (b) D'après les calculs précédents :

$$\begin{aligned} 17 &= 493 - 68 \times 7 = 493 - (561 - 493) \times 7 = 8 \times 493 - 7 \times 561 \\ &= 8 \times (2176 - 3 \times 561) - 7 \times 561 = 8 \times 2176 - (24 + 7) \times 561 = 8 \times 2176 - 31 \times 561 \end{aligned}$$

   On a obtenu $561u + 2176v = 17$ avec $(u\,;\,,\,v) = (-31\,;\,8)$.

2. (a) voir sujet a)

   (b) Soit $n \in \mathbb{N}$ quelconque. Alors : $n^2 - (n-1)(n+1) = n^2 - (n^2 - 1) = 1$ donc on a trouvé un couple $(u\,;\,v) = (1\,;\,-(n+1)) \in \mathbb{Z}^2$ tel que $n^2u + (n-1)v = 1$. D'après le théorème de Bézout (sens réciproque), on peut donc affirmer que $n-1$ et n^2 sont premiers entre eux.

3. (a) $n^2 - n - 11 = (n-3)n + 2n - 11$ donc $PGCD(n^2 + n - 9\,;\,n-3) = PGCD(n-3\,;\,2n-11)$ d'après le lemme d'Euclide puis $2n - 11 = 2(n-3) - 5$ donc toujours avec le lemme d'Euclide, on sait que $PGCD(2n-11\,;\,n-3) = PGCD(n-3\,;\,-5) = PGCD(n-3\,;\,5)$. Or, $PGCD(n-3\,;\,5)$ est un diviseur positif de 5 donc il vaut soit 1 soit 5. $PGCD(n-3\,;\,5) = 5$ si et seulement si 5 divise $n-3$, c'est-à-dire $n \equiv 3\ [5]$. Finalement, $PGCD(n^2 - n - 11\,;\,n-3) = \begin{cases} 5 \text{ si } n \equiv 3\ [5] \\ 1 \text{ sinon} \end{cases}$.

   (b) On pose $P(x) = x^2 - x - 6$ et on remarque que $P(2) = 3^2 - 3 - 6 = 0$ donc $x_1 = 3$ est une racine de $P(x)$. L'autre racine x_2 vérifie $x_1 \times x_2 = \dfrac{c}{a} = -6$ d'où $x_2 = \dfrac{-6}{3} = -2$. Ainsi, $P(x) = (x-3)(x+2)$. En particulier, $n^2 - n - 6 = (n-3)(n+2)$. Essayons alors de multiplier $n^2 - n - 11$ par ce même facteur $n+2$.

$$(n^2 - n - 11)(n+2) = n^3 + 2n^2 - n^2 - 2n - 11n - 22 = n^3 + n^2 - 13n - 22$$

   Finalement,

$$\begin{aligned} PGCD(n^3 + n^2 - 13n - 22\,;\,n^2 - n - 6) &= PGCD((n+2)(n^2 - n - 11)\,;\,(n+2)(n-3)) \\ &= |n+2|\,PGCD(n^2 - n - 11\,;\,n-3) \\ &= \begin{cases} 5|n+2| \text{ si } n \equiv 3\ [5] \\ |n+2| \text{ sinon} \end{cases} \quad \text{(question précédente)} \end{aligned}$$

4. (a) **La phrase est FAUSSE**
   En effet pour $a = 5$ et $b = 2$, alors $3 \times 5 - 4 \times 2 = 15 - 8 = 7$ en choisissant $(u\,;\,v) = (3\,;\,-4) \in \mathbb{Z}^2$ et pourtant $PGCD(5\,;\,2) \neq 7$ (7 ne divise ni 5 ni 2 !)

   (b) On choisit $a = 5$ et $b = 4$. Ce sont deux nombre premiers donc ils sont premiers entre eux. De plus, $2a + b = 2 \times 5 + 4 = 10 + 4 = 14$ et $a - 3b = 5 - 12 = -7$. Ces deux nombres sont divisibles par 7 donc ils ne sont pas premiers entre eux. On a donc trouvé un contre-exemple pour le sens réciproque.
   La phrase est FAUSSE

   (c) voir question 4. a) du sujet a)