CORRECTION DES EXERCICES POUR LE VENDREDI 26 NOVEMBRE

Exercice F :

1. **VRAI**
   Si $3a - 7b = -1$ alors $(-3)a + 7b = 1$. Si on pose $u = -3$ et $v = 7$, alors $au + bv = 1$ avec $(u\,;\,v) \in \mathbb{Z}^2$. D'après le théorème de Bézout (sens réciprique), alors a et b sont premiers entre eux.

2. **FAUX**
   Il est possible que $5a + 4b = 2$ soit vérifiée et que a et b soient premiers entre eux.
   Par exemple : $5 \times (-2) + 4 \times 3 = -10 + 12 = 2$ et les nombres -2 et 3 sont premiers entre eux (ils n'ont pas d'autres diviseurs communs que 1).

3. **VRAI**
   – Si a et b sont pairs : $a \equiv 0\ [2]$ et $b \equiv 0\ [2]$ donc $a + b \equiv 0\ [2]$ et $a - b \equiv 0\ [2]$. Les nombres $(a + b)$ et $(a - b)$ sont donc pairs, c'est-à-dire tous les deux divisibles par 2. Ainsi, $PGCD(a + b\,;\,a - b)$ est un multiple de 2 (en effet les diviseurs communs à $a + b$ et à $a - b$ sont les diviseurs de leur $PGCD$).
   – Si a et b sont tous les deux impairs, alors $a \equiv 1\ [2]$ et $b \equiv 1\ [2]$ d'où $a + b \equiv 2\ [2]$. Or, $\equiv 0\ [2]$ car 2 divise 2 donc $a + b \equiv 0\ [2]$. De plus, $a - b \equiv 0\ [2]$. Ainsi, $a + b$ et $a - b$ sont pairs donc, comme précédemment, $PGCD(a\,;\,b) \neq 1$.

4. **FAUX**
   Par exemple, $a = 10$ et $b = 5$ n'ont pas la même parité. De plus, $a + b = 15$ et $a - b = 5$ et ces deux nombres ne sont pas premiers entre eux. En effet, 3 est un diviseur commun à $a + b$ et à $a - b$.

Exercice H :

1. Pour tout $n \in \mathbb{Z}$, $n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1)$.
   Ce nombre est divisible par 2 car parmi les trois nombres consécutifs $n - 1$, n et $n + 1$, au moins un des trois est pairs.
   Ce nombre est également divisible par 3 car parmi trois nombres consécutifs, au moins un est divisible par 3.
   Comme $PGCD(2\,;\,3) = 1$ (le seul diviseur commun à 2 et 3 est 1), alors tout nombre divisible par 2 et par 3 est également divisible par 6 (conséquence du théorème de Gauss). Ainsi, $n^3 - n$ est divisible par 6.

2. On suppose n impair : il existe $k \in \mathbb{Z}$ tel que $n = 2k + 1$. Ainsi,
   $$n^3 - n = n(n-1)(n+1) = (2k+1)(2k+1-1)(2k+1+1) = 2k(2k+1) \times 2(k+1) = 4k(k+1)(2k+1)$$
   Le nombre $n^3 - n$ est alors divisible par 24 si et seulement si $k(k + 1)(2k + 1)$ est divisible par 6.
   Or, $k(k + 1)$ est divisible par 2 car parmi les deux entiers consécutifs k et $k + 1$, l'un des deux est pair. Par conséquent $k(k + 1)(2k + 1)$ est divisible par 2.
   De plus, si on raisonne modulo 3 :
   – si $k \equiv 0\ [3]$, alors $k(k + 1)(2k + 1) \equiv 0\ [3]$
   – si $k \equiv 1\ [3]$, alors $2k \equiv 2\ [3]$ d'où $2k+1 \equiv 3\ [3]$. Or, $3 \equiv 0\ [3]$ donc $2k+1 \equiv 0\ [3]$ puis $k(k+1)(2k+1) \equiv 0\ [3]$
   – si $k \equiv 2\ [3]$, alors $k + 1 \equiv 3\ [3]$ donc $k + 1 \equiv 0\ [3]$ puis $k(k + 1)(2k + 1) \equiv 0\ [3]$
   Dans tous les cas, $k(k+1)(2k+1) \equiv 0\ [3]$ donc ce nombre est divisible par 3. On a justifié qu'il est également divisible par 2 donc il est divisible par 6. Finalement, $n^3 - n$ est bien divisible par 24.

Exercice I :

1. (a) Soit d un diviseur positif de $4n+1$ et de $5n+1$. Alors d divise $5(4n+1)-4(5n+1) = 20n+5-20n-4 = 1$. Par conséquent, $d = 1$. On en déduit que $PGCD(4n+1\,;\,5n+1) = 1$, c'est-à-dire que les nombres $4n+1$ et $5n + 1$ sont premiers entre eux.

(b) $7n+2 = 2(4n+1) - n$ donc $PGCD(7n+1\,;\,4n+1) = PGCD(4n+1\,,;\,-n)$ d'après le lemme d'Euclide. En outre, $4n+1 = (-4)\times(-n)+1$ donc $PGCD(4n+1\,;\,-n) = PGCD(-n\,;\,1)$ d'après le lemme d'Euclide. Finalement, $PGCD(7n+1\,;\,4n+1) = PGCD(-n\,;\,1)$ car le seul diviseur positif de 1 est 1. On en déduit que les nombres $4n+1$ et $7n+1$ sont premiers entre eux.

2. On pose $P(x) = 35x^2 + 17x + 2$. Le discriminant est $\Delta = 17^2 - 4\times 35\times 2 = 9$.
Ses racines sont $x_1 = \dfrac{-17-3}{70} = -\dfrac{2}{7}$ et $x_2 = \dfrac{-17+3}{70} = \dfrac{-14}{70} = -\dfrac{1}{5}$ donc

$$P(x) = a(x-x_1)(x-x_2) = 35(x+\frac{2}{7})(x+\frac{1}{5}) = 7(x+\frac{2}{7})\times 5(x+\frac{1}{5}) = (7x+2)(5x+1)$$

On pose $d = PGCD(4n+1\,;\,35n^2+17n+2) = PGCD\,(4n+1\,;\,(5n+1)(7n+2))$. d est un diviseur de $4n+1$ donc il existe $k\in\mathbb{N}$ tel que $(4n+1) = kd$. De même d est un diviseur de $(5n+1)(7n+2)$ donc il existe $k'\in\mathbb{N}$ tel que $k'd = (5n+1)(7n+2)$. Alors $kk'd = k'(4n+1) = k(5n+1)(7n+2)$. Comme $k'\in\mathbb{Z}$, alors $4n+1$ est un diviseur de $k(5n+1)(7n+1)$. Or, $4n+1$ et $5n+1$ sont premiers entre eux (d'après la question 1) donc, d'après le théorème de Gauss, $4n+1$ est un diviseur de $k(7n+1)$. De plus, $4n+1$ et $7n+1$ sont premiers entre eux (question 1) donc, en utilisant une nouvelle fois le théorème de Gauss, $4n+1$ est un diviseur de k. Ainsi, il existe $k''\in\mathbb{N}$ tel que $k = k''(4n+1)$. Or, on sait que $4n+1 = kd$ donc $4n+1 = k''d(4n+1)$ d'où $kk'' = 1$. Comme k'' et d sont des entiers naturels alors $d = k'' = 1$. On a bien prouvé que $PGCD(4n+1\,;\,35n^2+17n+2) = 1$, c'est-à-dire que $4n+1$ et $35n^2+17n+2$ sont premiers entre eux.

`Remarque` : On pouvait utiliser directement le deuxième corollaire du théorème de Gauss : $PGCD(x\,;\,a) = 1$ et $PGCD(x\,;\,b) = 1$ si et seulement si $PGCD(x\,;\,ab) = 1$ avec $a = 5n+1$, $b = 7n+1$ et $x = 4n+1$.

Exercice 39 p.31 :

1. *Montrons que $a+b$ et ab sont premiers entre eux.*
Soit d un diviseur positif commun à $a+b$ et à ab. On sait que a et b sont premiers entre eux donc, d'après le théorème de Bézout, il existe u et v deux entiers relatifs tels que $au+bv = 1$. Ainsi, $(a+b)u - bu + bv = 1$ soit $(a+b)u + b(v-u) = 1$. On mutiliplie par a : $a(a+b)u + ab(v-u) = b$. Comme d divise $a+b$ et ab et que au et $(v-u)$ sont des entiers relatifs, alors d est un diviseur de $(a+b)au + ab(v-u) = b$. De plus, d divise $(a+b)$ donc d divise $(a+b) - b = a$. Comme a et b sont premiers entre eux, le seul diviseur positif commun à a et à b est égal à 1. Ainsi, $d = 1$, ce qui implique que $a+b$ et ab sont premiers entre eux.

Montrons que $a+b$ et a^2-ab+b^2 sont premiers entre eux ou divisibles par 3
On sait que $(a+b)^2 = a^2+2ab+b^2$ donc $a^2-ab+b^2 = (a+b)^2-3ab$. D'après le lemme d'Euclide, $d = PGCD(a^2-ab+b^2\,;\,a+b) = PGCD(a+b\,;\,-3ab)$. D'après le théorème de Bézout, comme $a+b$ et ab sont premiers entre eux (montré avant), alors il existe $(u\,;\,v)\in\mathbb{Z}^2$ tel que $(a+b)u + abv = 1$. Ainsi, $-3(a+b)u - 3abv = -3$.Comme d divise $(a+b)$ et $-3ab$ alors il divise $(-3u)(a+b) + v(-3ab) = -3$ (car $-3u$ et v sont des entiers relatifs). Les seuls diviseurs positifs de -3 sont 1 et 3 donc $d = 1$ ou $d = 3$.
Si $d = 1$, cela signifie que $a+b$ et a^2-ab+b^2 sont premiers entre eux.
Sinon, alors $d = 3$ donc 3 est un diviseur commun à $a+b$ et a^2-ab+b^2

2. On distingue deux cas :
   – si $PGCD(a+b\,;\,a^2-ab+b^2) = 3$, alors 3 est un diviseur de $a+b$ donc $PGCD(a+b\,;\,3) = 3$ (en effet ce $PGCD$ est nécéssairement un diviseur de 3 et comme chacun des deux nombres est divisible par 3, il vaut 3). En particulier, $PGCD(a+b\,;\,a^2-ab+b^2) = PGCD(a+b\,;\,3)$.
   – si $PGCD(a+b\,;\,a^2-ab+b^2) = 1$, on sait que $PGCD(a+b\,;\,3)$ est un diviseur positif de 3, donc il vaut 1 ou 3. On raisonne par l'absurde en supposant que $PGCD(a+b\,;\,3) = 3$. Cela signifie que 3 est un diviseur de $a+b$. On sait aussi que 3 est un diviseur de $3ab$ (car $ab\in\mathbb{Z}$). On en déduit que 3 est un diviseur de $(a+b)^2-3ab = a^2-ab+b^2$. Si 3 divise à la fois $a+b$ et a^2-ab+b^2, cela contredit l'hypothèse $PGCD(a+b\,;\,a^2-ab+b^2) = 1$. On en déduit que $PGCD(a+b\,;\,1)$ d'où $PGCD(a+b\,;\,a^2-ab+b^2) = PGCD(a+b\,;\,3)$.

   Dans tous les cas, on a démontré que $PGCD(a+b\,;\,a^2-ab+b^2) = PGCD(a+b\,;\,3)$.