ARITHMETIQUE

Exercice 1 :

Étant donnés cinq nombres entiers consécutifs, on trouve toujours parmi eux (vrai ou faux et pourquoi) :

1. au moins deux multiples de 2.
2. au plus trois nombres pairs.
3. au moins deux multiples de 3.
4. exactement un multiple de 5.
5. au moins un multiple de 6.
6. au moins un nombre premier.

Allez à : Correction exercice 1 :

Exercice 2 :

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. 60 a plus de diviseurs (positifs) que 100.
2. 60 a moins de diviseurs (positifs) que 90.
3. 60 a moins de diviseurs (positifs) que 120.
4. si un entier divise 60, alors il divise 120.
5. si un entier strictement inférieur à 60 divise 60, alors il divise 90.
6. si un nombre premier divise 120, alors il divise 60.

Allez à : Correction exercice 2 :

Exercice 3 :

On veut constituer la somme exacte de 59 euros seulement à l'aide de pièces
de 2 euros et de billets de 5 euros. Parmi les affirmations suivantes, lesquelles sont vraies,
lesquelles sont fausses et pourquoi ?

1. Il y a au plus 22 pièces de 2 euros.
2. Il peut y avoir exactement 10 pièces de 2 euros.
3. Il peut y avoir exactement 12 pièces de 2 euros.
4. Il peut y avoir un nombre pair de billets de 5 euros.
5. Il y a au moins un billet de 5 euros.

Allez à : Correction exercice 3 :

Exercice 4 :

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. Si un nombre est divisible par 9, alors il est divisible par 6.
2. Si un nombre est divisible par 100, alors il est divisible par 25.
3. Si un nombre est divisible par 2 et par 3, alors il est divisible par 12.
4. Si un nombre est divisible par 10 et par 12, alors il est divisible par 15.
5. Si un nombre est divisible par 6 et par 8, alors il est divisible par 48.
6. Le produit des entiers de 3 à 10 est divisible par 1000.
7. Le produit des entiers de 3 à 10 est divisible par 1600.
8. Si la somme des chiffres d'un entier en écriture décimale vaut 39, alors il est divisible par 3 mais pas par 9.
9. Si la somme des chiffres d'un entier en écriture décimale vaut 18, alors il est divisible par 6 et par 9.

Allez à : Correction exercice 4 :

Exercice 5 :

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. Si un entier est divisible par deux entiers, alors il est divisible par leur produit.
2. Si un entier est divisible par deux entiers premiers entre eux, alors il est divisible par leur produit.
3. Si un entier est divisible par deux entiers, alors il est divisible par leur PPCM.
4. Si un nombre divise le produit de deux entiers, alors il divise au moins un de ces deux entiers.
5. Si un nombre premier divise le produit de deux entiers, alors il divise au moins un de ces deux entiers.
6. Si un entier est divisible par deux entiers, alors il est divisible par leur somme.

7. Si un entier divise deux entiers, alors il divise leur somme.
8. Si deux entiers sont premiers entre eux, alors chacun d'eux est premier avec leur somme.
9. Si deux entiers sont premiers entre eux, alors chacun d'eux est premier avec leur produit.
10. Si deux entiers sont premiers entre eux, alors leur somme et leur produit sont premiers entre eux.

Allez à : Correction exercice 5 :

Exercice 6 :

Soient a, b et d trois entiers. Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. Si d divise a et b, alors d divise leur $PGCD$.
2. S'il existe deux entiers u et v tels que $au + bv = d$, alors $d = PGCD(a, b)$.
3. S'il existe deux entiers u et v tels que $au + bv = d$, alors d divise $PGCD(a, b)$.
4. S'il existe deux entiers u et v tels que $au + bv = d$, alors $PGCD(a, b)$ divise d.
5. Si $PGCD(a, b)$ divise d, alors il existe un couple d'entiers (u, v) unique, tel que $au + bv = d$.
6. L'entier d est un multiple de $PGCD(a, b)$ si et seulement si il existe un couple d'entiers (u, v), tel que $au + bv = d$.

Allez à : Correction exercice 6 :

Exercice 7 :

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. Si un entier est congru à 0 modulo 6, alors il est divisible par 6.
2. Si le produit de deux entiers est congru à 0 modulo 6 alors l'un des deux est multiple de 6.
3. Si un entier est congru à 5 modulo 6 alors toutes ses puissances paires sont congrues à 1 modulo 6.
4. Si deux entiers sont congrus à 4 modulo 6, alors leur somme est congrue à 2 modulo 6.
5. Si deux entiers sont congrus à 4 modulo 6, alors leur produit est congru à 2 modulo 6.
6. Si un entier est congru à 4 modulo 6 alors toutes ses puissances sont aussi congrues à 4 modulo 6.

Allez à : Correction exercice 7 :

Exercice 8 :

Parmi les affirmations suivantes, lesquelles sont vraies, lesquelles sont fausses et pourquoi ?

1. Si le produit de deux entiers est congru à 0 modulo 5 alors l'un des deux est multiple de 5.
2. Si un entier est congru à 2 modulo 5 alors sa puissance quatrième est congrue à 1 modulo 5.
3. Si deux entiers sont congrus à 2 modulo 5, alors leur somme est congrue à 1 modulo 5.
4. Pour tout entier, non multiple de 5, il existe un entier tel que le produit des deux soit congru à 1 modulo 5.
5. Aucun entier n'est tel que son carré soit congru à -1 modulo 5.
6. Aucun entier n'est tel que son carré soit congru à 2 modulo 5.
7. La puissance quatrième d'un entier quelconque est toujours congrue à 1 modulo 5.
8. La puissance quatrième d'un entier non multiple de 5 est toujours congrue à 1 modulo 5.

Allez à : Correction exercice 8 :

Exercice 9 :

Soit $n \in \mathbb{N}$ un entier.

1. Démontrer que si n n'est divisible par aucun entier inférieur ou égal à $\sqrt{n}$, alors n est premier.
2. Démontrer que les nombres $n! + 2, n! + 3, \dots, n! + n$ ne sont pas premiers.
3. En déduire que pour tout n, il existe n entiers consécutifs non premiers.

Allez à : Correction exercice 9 :

Exercice 10 :

Le premier janvier 2007 était un lundi. Calculer quel jour de la semaine sera le

1. 2 juillet 2007
2. 15 janvier 2008
3. 19 mars 2008 (attention, 2008 est une année bissextile)
4. 14 juillet 2010
5. 26 août 2011

Allez à : Correction exercice 10 :

Exercice 11 :

On choisit un nombre entier, on le divise par 7 et on trouve un reste égal à 5. On divise à nouveau le quotient obtenu par 7, on trouve un reste égal à 3 et un quotient égal à 12. Quel était le nombre de départ ?

Allez à : Correction exercice 11 :

Exercice 12 :

On donne l'égalité suivante.

$$96842 = 256 \times 375 + 842$$

Déterminer, sans effectuer la division, le quotient et le reste de la division euclidienne de 96842 par 256 et par 375.

Allez à : Correction exercice 12 :

Exercice 13 :

On donne les deux égalités suivantes.

$$3379026 = 198765 \times 17 + 21, \qquad 609806770 = 35870986 \times 17 + 8$$

On s'intéresse au nombre entier $N = 3379026 \times 609806770$. Quel est le reste de la division euclidienne de N par 17 ?

Allez à : Correction exercice 13 :

Exercice 14 :

Donner la décomposition en facteurs premiers des entiers suivants.

60 ; 360 ; 2400 ; 4675 ; 9828 ; 15200 ; 45864 ; 792792.

Allez à : Correction exercice 14 :

Exercice 15 :

Déterminer le $PGCD(2244,1089)$ et déterminer l'identité de Bézout correspondante.

Allez à : Correction exercice 15 :

Exercice 16 :

On considère les couples d'entiers (a, b) suivants.

a) $a = 60$, $b = 84$ Allez à correction a)
b) $a = 360$, $b = 240$ Allez à la correction b)
c) $a = 160$, $b = 171$ Allez à la correction 0
d) $a = 360$, $b = 345$ Allez à la correction d)
e) $a = 325$, $b = 520$ Allez à la correction e)
f) $a = 720$, $b = 252$ Allez à la correction f)
g) $a = 955$, $b = 183$ Allez à la correction 0
h) $a = 1665$, $b = 1035$ Allez à la correction h)
i) $a = 18480$, $b = 9828$ Allez à la correction i)

Pour chacun de ces couples :

1. Calculer $PGCD(a, b)$ par l'algorithme d'Euclide.
2. En déduire une identité de Bézout.
3. Calculer $PPCM(a, b)$.
4. Déterminer l'ensemble des couples (u, v) d'entiers relatifs tels que : $au + bv = PGCD(a, b)$
5. Donner la décomposition en facteurs premiers de a et b.
6. En déduire la décomposition en facteurs premiers de $PGCD(a, b)$ et $PPCM(a, b)$, et retrouver les résultats des questions 1 et 3.

Allez à : Correction exercice 16 :

Exercice 17 :

1. Calculer le PGCD de 8303 et 2717 et donner l'identité de Bézout correspondante.

2. En déduire le PPCM de 8303 et 2717.
3. Calculer le PGCD de 1001 et 315 et donner l'identité de Bézout correspondante.
4. Déterminer le $PGCD(2244,1089)$ et déterminer l'identité de Bézout correspondante.

Allez à : Correction exercice 17 :

Exercice 18 :
Résoudre dans $\mathbb{Z} \times \mathbb{Z}$ les équations suivantes :

1. $3x - 5y = 13$
2. $212x + 45y = 3$
3. $42x + 45y = 4$
4. $7x + 5y = 3$

Allez à : Correction exercice 18 :

Exercice 19 :

1. Donner, en le justifiant, le nombre de diviseurs positifs de 100^{100}.
2. Déterminer le reste de la division de 101^{101} par 3, et par 5, en déduire le reste de la division euclidienne de 101^{101} par 15.
3. Soit $n \in \mathbb{N}$ un entier naturel et p un nombre premier supérieur ou égal à 3. En utilisant un résultat du cours, montrer que si $0 < n < p$ alors p divise l'un des entiers $n^{\frac{p-1}{2}} - 1$ et $n^{\frac{p-1}{2}} + 1$

Allez à : Correction exercice 19 :

Exercice 20 :
Déterminer le nombre de diviseurs positifs de
$$N = 72^{10} \times 162^{50}$$
On pourra présenter le résultat sous forme d'un produit de nombre entier.

Allez à : Correction exercice 20 :

Exercice 21 :
Quel est le plus petit entier naturel, qui divisé par 8, 15, 18 et 24 donne pour restes respectifs 7, 14, 17 et 23 ?

Allez à : Correction exercice 21 :

Exercice 22 :
Dans une UE de maths à l'université Claude Bernard, il y a entre 500 et 1000 inscrits. L'administration de l'université a remarqué qu'en les répartissant en groupes de 18, ou bien en groupes de 20, ou bien aussi en groupes de 24, il restait toujours 9 étudiants. Quel est le nombre d'inscrits ?

Allez à : Correction exercice 22 :

Exercice 23 :
Soient a et b deux entiers tels que $1 \leq a < b$.

1. Soient q_1 et r_1 (respectivement : q_2 et r_2) le quotient et le reste de la division euclidienne de a (respectivement : b) par $b - a$. Démontrer que $r_1 = r_2$ et $q_2 = q_1 + 1$.
2. On note q le quotient de la division euclidienne de $b - 1$ par a. Soit $n > 0$ un entier. Exprimer en fonction de q, r et n le quotient et le reste de la division euclidienne de $ba^n - 1$ par a^{n+1}.
3. Soit d le $PGCD$ de a et b. Déterminer le $PGCD$ de $A = 15a + 4b$ et $B = 11a + 3b$
4. Soit d le $PGCD$ de a et b. Montrer que $d = PGCD\big(a + b, PPCM(a, b)\big)$.
5. Démontrer que si $d = 1$ (a et b sont premiers entre eux), alors pour tous $m \in \mathbb{N}$ et $n \in \mathbb{N}$, a^m et b^n sont premiers entre eux.
6. En déduire que pour tout $n \in \mathbb{N}$, le $PGCD$ de a^n et b^n est d^n.

Allez à : Correction exercice 23 :

Exercice 24 :
Soient a, b et c trois entiers relatifs non nuls.

1. Montrer que $PGCD(ca, cb) = |c| \times PGCD(a, b)$.
2. Montrer que si $PGCD(a, b) = 1$ et si c divise a, alors $PGCD(c, b) = 1$.
3. Montrer que $PGCD(a, bc) = 1$ si et seulement si $PGCD(a, b) = PGCD(a, c) = 1$.
4. Montrer que si $PGCD(b, c) = 1$ alors $PGCD(a, bc) = PGCD(a, b) \times PGCD(a, c)$.

Allez à : Correction exercice 24 :

Exercice 25 :

Soient $a \in \mathbb{N}$, $b \in \mathbb{N}$ deux entiers tels que $0 < a < b$.

1. Démontrer que si a divise b, alors pour tout $n \in \mathbb{N}$, $n^a - 1$ divise $n^b - 1$.
2. Pour $n \in \mathbb{N}^*$, démontrer que le reste de la division euclidienne de $n^b - 1$ par $n^a - 1$ est $n^r - 1$, où r est le reste de la division euclidienne de b par a.
3. Pour $n \in \mathbb{N}^*$, démontrer que le $PGCD$ de $n^b - 1$ et $n^a - 1$ est $n^d - 1$, où d est le $PGCD$ de a et b.

Allez à : Correction exercice 25 :

Exercice 26 :

Soit n un entier relatif. On pose $a = 2n + 3$ et $b = 5n - 2$.

1. Calculer $5a - 2b$. En déduire le $PGCD$ de a et b en fonction de n.
2. Procéder de même pour exprimer en fonction de n le $PGCD$ de $2n - 1$ et $9n + 4$.

Allez à : Correction exercice 26 :

Exercice 27 :

Soient $a = 2n + 1$ et $b = 5n + 1$ deux entiers.

1. Déterminer deux entiers u et v tels que $au + bv = 3$
2. En déduire les valeurs possibles de $d = PGCD(a, b)$?
3. Montrer que si $n \equiv 1 \ \ [3]$ alors $d = 3$, que vaut d sinon ?

Allez à : Correction exercice 27 :

Exercice 28 :

Soit $\in \mathbb{N}^*$, pour quelles valeurs les nombres $2n$ et $3n + 1$ sont premiers entre eux ?

Allez à : Correction exercice 28 :

Exercice 29 :

1. Montrer que pour tout $n \in \mathbb{Z}$, les entiers $14n + 3$ et $5n + 1$ sont premiers entre eux
2. On considère l'équation (E) : $87x + 31y = 2$ où x et y sont des entiers relatifs
   2.1. Montrer que 87 et 31 sont premiers entre eux.
   2.2. En déduire un couple $(u, v) \in \mathbb{Z}^2$ tels que $87u + 31v = 1$, puis une solution (x_0, y_0) de (E)
   2.3. Déterminer l'ensemble des solutions de (E).

Allez à : Correction exercice 29 :

Exercice 30 :

1. Déterminer les restes possibles de la division euclidienne du carré d'un nombre impair par 8.
2. Soit $n \in \mathbb{N}^*$ un entier pair. En déduire que l'équation

$$x^n + y^n = z^n$$

N'a pas de solution pour x, y et z impairs.

Allez à : Correction exercice 30 :

Exercice 31 :

Déterminer le reste de la division euclidienne de 5^{1000} par 7.

Allez à : Correction exercice 31 :

Exercice 32 :

Montrer que pour tout $n \in \mathbb{N}$, l'entier $3^{n+3} - 4^{4n+2}$ est un multiple de 11.
Allez à : Correction exercice 32 :

Exercice 33 :
Montrer que : 4^n est congru à $1 + 3n$ modulo 9. En déduire que $2^{2n} + 15n - 1$ est toujours divisible par 9.
Allez à : Correction exercice 33 :

Exercice 34 :
1. Montrer par récurrence que pour $n \geq 0$, $a_n = 4^{2n+2} - 1$ est un multiple de 15.
2. Soit $n \geq 0$, $b_n = 4^{2n+2} - 15n - 16$, calculer $b_{n+1} - b_n$ et montrer que $b_{n+1} - b_n$ est un multiple de $225 = 15 \times 15$.
3. Montrer que pour tout entier $n \geq 0$, b_n est un multiple de 225.

Allez à : Correction exercice 34 :

Exercice 35 :
Montrer que pour tout $n \in \mathbb{N}$, $5^{n+2} + 3^{n+1}5^{2n}$ est divisible par 7.
Allez à : Correction exercice 35 :

Exercice 36 :
On se propose de déterminer tous les couples $(m, n) \in \mathbb{N} \times \mathbb{N}$ solutions de l'équation : $2^m - 3^n = 1$.
1. Soit $k \in \mathbb{N}^*$.
   a) Quel est le reste de la division euclidienne de 9^k par 8 ?
   b) Déterminer les restes de la division euclidienne de $3^{2k} + 1$ par 8, puis de $3^{2k+1} + 1$ par 8
2. Soit $(m, n) \in \mathbb{N} \times \mathbb{N}$ un couple de solution, montrer à l'aide de 1°) que $m \leq 2$.
3. En déduire tous les couples $(m, n) \in \mathbb{N} \times \mathbb{N}$ d'entier naturels solutions de l'équation.

Allez à : Correction exercice 36 :

Exercice 37 :
Montrer que 3 divise $a^3 - b^3$ si et seulement si 3 divise $a - b$.
Allez à : Correction exercice 37 :

Exercice 38 :
Montrer que 7 divise $a^2 + b^2$ si et seulement si 7 divise a et b.
Allez à : Correction exercice 38 :

Exercice 39 :
Déterminer toutes les solutions dans $\mathbb{Z} \times \mathbb{Z}$ de l'équation :
$$7x + 5y = 3$$
Allez à : Correction exercice 39 :

Exercice 40 :
Résoudre dans $\mathbb{Z}$, $12x \equiv 5\ \ [35]$
Allez à : Correction exercice 40 :

Exercice 41 :
1. Trouver une solution particulière de $13u + 5v = 3$
2. Déterminer tous les couples d'entiers $(u, v) \in \mathbb{Z}^2$ tels que $13u + 5v = 3$.
3. Déterminer les restes de la division euclidienne de 2^{2013} par 5 et par 13.
4. Déduire des deux questions qui précèdent le reste de la division euclidienne de 2^{2013} par 65.

Allez à : Correction exercice 41 :

Exercice 42 :

(1) a. Déterminer le reste de la division de $N = 222^{333}$ par 7 et par 11.

b. Déterminer deux entiers u et v tels que $7u + 11v = 1$.

c. En déduire le reste de la division de N par 77.

(2) Toto veut faire don des livres de sa bibliothèque. Il en a plus de 10. S'il les répartit dans les cartons contenant 20 livres ou des cartons qui en contiennent 25, il lui reste toujours 7 livres. Quel est le nombre minimal de livres dans la bibliothèque de Toto ?

Allez à : Correction exercice 42 :

Exercice 43 :

1. Ecrire une identité de Bézout entre 99 et 56.
2. Résoudre le système

$$\begin{cases} x \equiv 2 \quad [56] \\ x \equiv 3 \quad [99] \end{cases}$$

Allez à : Correction exercice 43 :

Exercice 44 :

Déterminer la plus petite solution positive du système :

$$\begin{cases} x \equiv 6 \quad [11] \\ x \equiv 3 \quad [13] \end{cases}$$

Allez à : Correction exercice 44 :

Exercice 45 :

1. Déterminer toutes les solutions de $2u + 5v = 59$
2. Donner tous les couples (u, v) tels que la somme de u pièces de 2 euros et de v billets de 5 euros égale à 59 euros.

Allez à : Correction exercice 45 :

Exercice 46 :

1. Résoudre : $\begin{cases} 7x + 5y \equiv 2 \quad [8] \\ 5x + 4y \equiv 16 \quad [8] \end{cases}$
2. Résoudre : $\begin{cases} 7x + 5y \equiv 2 \quad [9] \\ 5x + 4y \equiv 16 \quad [9] \end{cases}$

Allez à : Correction exercice 46 :

Exercice 47 :

Résoudre dans $\mathbb{Z}$ les systèmes suivants :

1.
$$\begin{cases} n \equiv 1 \quad [6] \\ n \equiv 5 \quad [9] \end{cases}$$

2.
$$\begin{cases} n \equiv 3 \quad [6] \\ n \equiv 6 \quad [9] \end{cases}$$

Allez à : Correction exercice 47 :

Exercice 48 :

Soit $p \geq 3$ un nombre premier

1. Quels sont les éléments $x \in \mathbb{Z}$ tels que : $x^2 \equiv 1 \quad [p]$?

2. En déduire le théorème de Wilson : si p est premier alors $(p-1)!+1$ est divisible par p.

Allez à : Correction exercice 48 :

Exercice 49 :

On considère un entier $n \geq 3$.

1. Montrer que, quel que soit l'entier x, les carrés des nombres x et $n-x$ sont congrus modulos n.
2. On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $\{0,1,\dots,n-1\}$ des restes modulo n, et c l'application de $\mathbb{Z}/n\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ qui a un reste associe son carré modulo n. Cette application est-elle injective ? surjective ?
3. Dresser la table des carrés modulo 7.
4. Montrer que l'équation $x^2-6xy+2y^2=7003$ n'a pas de solutions (x,y) entière. (Exprimer le premier membre comme un carré modulo 7).

Allez à : Correction exercice 49 :

CORRECTIONS

Correction exercice 1 :

1. Si n est pair, $n+2$ et $n+4$ sont pairs alors que $n+1$ et $n+3$ sont impairs.
   Si n est impair, $n+2$ et $n+4$ sont impairs alors que $n+1$ et $n+3$ sont pairs.
   Il y a deux ou trois nombres pairs parmi ces cinq entiers, donc au moins deux nombres pairs.
2. D'après 1°) il y a deux ou trois nombres impairs donc au plus trois.
3. D'après 1°) et 2°) il y a au moins deux multiples de trois.
4. Parmi cinq nombres consécutifs il y a au moins un multiple de cinq, notons le $n+k, k\in\{0,1,2,3,4\}$, le multiple de cinq suivant est $n+k+5$ qui n'appartient pas à $\{n,n+1,n+2,n+3,n+4\}$, donc il y a exactement un multiple de cinq.
5. C'est faux, par exemple dans $\{1,2,3,4,5\}$ il ni a pas de multiple de six.
6. C'est faux, par exemple dans $\{24,25,26,27,28\}$ il n'y a pas de nombre premier.

Allez à : Exercice 1 :

Correction exercice 2 :

1. $60=2^2\times 3^1\times 5^1$ donc les diviseurs positifs de 60 sont de la forme $2^i\times 3^j\times 5^k$ avec
   $$(i,j,k)\in\{0,1,2\}\times\{0,1\}\times\{0,1\}$$
   60 a donc $3\times 2\times 2=12$ diviseurs
   $100=2^2\times 5^2$ donc les diviseurs positifs de 100 sont de la forme $2^i\times 5^j$ avec
   $$(i,j)\in\{0,1,2\}\times\{0,1,2\}$$
   100 a donc $3\times 3=9$ diviseurs.
   60 a plus de diviseurs positifs que 100.
2. $90=2^1\times 3^2\times 5^1$ donc les diviseurs positifs de 90 sont de la forme $2^i\times 3^j\times 5^k$ avec
   $$(i,j,k)\in\{0,1\}\times\{0,1,2\}\times\{0,1\}$$
   90 a donc $2\times 3\times 2=12$ diviseurs
   60 a le même nombre de diviseurs positifs que 90, la réponse est donc vraie.
3. $120=2^3\times 3^1\times 5^1$ donc les diviseurs positifs de 120 sont de la forme $2^i\times 3^j\times 5^k$ avec
   $$(i,j,k)\in\{0,1,2,3\}\times\{0,1\}\times\{0,1\}$$
   120 a donc $4\times 2\times 2=16$ diviseurs
   Donc 60 a moins de diviseurs positifs que 120.
   Deuxième méthode : $120=2\times 60$ donc les diviseurs de 60 sont aussi des diviseurs de 120, comme 120 est un diviseur de 120 mais pas de 60, 120 a plus de diviseurs que 60.
4. Soit n un diviseur de 60, il existe $k\in\mathbb{Z}$ tel que $60=k\times n$ donc $120=2k\times n$ par conséquent n est un diviseur de 120.
5. C'est faux, 20 divise 60 et 20 ne divise pas 90.
6. Les diviseurs premiers de 120 sont 2, 3 et 5, ils divisent tous les trois 60.

Autre méthode :

$120 = 2 \times 60$. 2 divise 60, et soit $p > 2$ un diviseur premier de 120, il existe $k \in \mathbb{Z}$ tel que $120 = p \times k$, alors $p \times k = 2 \times 60$, d'après le théorème de Gauss, $p|2 \times 60$ et p est premier avec 2 donc p divise 60.

Remarque : cette deuxième méthode est plus longue que la première mais dans d'autres circonstances cela peut s'avérer utile.

Allez à : Exercice 2 :

Correction exercice 3 :

Première méthode théorique (indispensable à connaitre)

On cherche les solutions de $2u + 5v = 59 \quad (1)$ avec $u \in \mathbb{N}$ (c'est le nombre de pièces de 2 euros) et $v \in \mathbb{N}$ (c'est le nombre de billets de 5 euros), comme 2 et 5 sont premier entre eux, il existe u_0 et v_0 tels que $2u_0 + 5v_0 = 1$, il existe une solution évidente $2 \times (-2) + 5 \times 1 = 1$, si ce n'est pas le cas on utilise l'algorithme d'Euclide. En multiplie par 59 : $2 \times (-118) + 5 \times 59 = 59 \quad (2)$,

En soustrayant (1) et (2) on trouve :

$$2(u + 118) + 5(v - 59) = 0 \Leftrightarrow 2(u + 2) = -5(v - 1)$$

2 est premier avec 5 et 2 divise $-5(v - 59)$, d'après le théorème de Gauss 2 divise $-(v - 59)$, donc il existe $k \in \mathbb{Z}$ tel que $-(v - 59) = 2k \Leftrightarrow v = -2k + 59$, on remplace $-(v - 59) = 2k$ dans $2(u + 118) = -5(v - 59)$, on trouve $2(u + 118) = 5 \times 2k \Leftrightarrow u + 118 = 5k \Leftrightarrow u = 5k - 118$, la réciproque est évidente.

Les solutions de (1) sont $\begin{cases} u = 5k - 118 \\ v = -2k + 59 \end{cases}$ avec $k \in \mathbb{Z}$.

Or $u \geq 0$ et $v \geq 0$,

$$\begin{cases} 5k - 118 \geq 0 \\ -2k + 59 \geq 0 \end{cases} \Leftrightarrow \begin{cases} k \geq \dfrac{118}{5} = 23 + \dfrac{3}{5} \\ k \leq \dfrac{59}{2} = 29 + \dfrac{1}{2} \end{cases} \Leftrightarrow \begin{cases} k \geq 24 \\ k \leq 29 \end{cases}$$

Chaque valeur de $k \in \{24,25,26,27,28,29\}$ donne une solution de l'équation (1) avec $u \geq 0$ et $v \geq 0$.

1. D'après les considérations ci-dessus
   Prenons $k = 29$, $u = 5 \times 29 - 118 = 145 - 118 = 27$ et $v = -2 \times 29 + 59 = 1$
   (Pour se rassurer $27 \times 2 + 5 = 59$) donc $(27,1)$ est une solution avec 27 pièces de 2 euros.
   C'est faux.
2. Est-il possible que $u = 10$? Or $u = 5k - 118$, cela entrainerait que $5k - 118 = 10 \Leftrightarrow 5k = 128$, ce qui n'est pas possible.
3. Est-il possible que $u = 12$? Or $u = 5k - 118$, cela qui est équivalent à $5k - 118 = 12 \Leftrightarrow 5k = 130 \Leftrightarrow k = 26 \in \{24,25,26,27,28,29\}$, la réponse est oui.
4. Est-il possible que $v = 2 \times l,\ \ l \in \mathbb{N}$? Or $v = -2k + 59$, cela entrainerait que $-2k + 59 = 2l \Leftrightarrow 59 = 2(l + k)$, ce qui est impossible. La réponse est non.
5. Est-il possible que $v = 0$? Or $v = -2k + 59$, cela entrainerait que $2k = 59$, ce qui est impossible, donc il y a au moins un billet de 5 euros.

Deuxième solution sans théorie

1. On cherche les solutions de $2u + 5v = 59$, avec $u \in \mathbb{N}$ (c'est le nombre de pièces de 2 euros) et $v \in \mathbb{N}$ (c'est le nombre de billets de 5 euros).
   $5 + 2 \times 27 = 59$, donc un billet de 5 euros et 27 pièces de deux euros convient, « il y a au plus 22 pièces de deux euros » est faux.
2. $2 \times 10 + 5v = 59 \Leftrightarrow 5v = 39$, c'est impossible, il ne peut pas y avoir exactement 10 pièces de 2 euros.
3. $2 \times 12 + 5v = 59 \Leftrightarrow 5v = 35 \Leftrightarrow v = 7$, la réponse est oui.
4. $v = 2l$, $2u + 5v = 59 \Leftrightarrow 2u + 10l = 59$, ce qui est impossible car 59 est impair.
5. $v = 0 \Leftrightarrow 2u = 59$, c'est impossible.

Remarque : c'est plus simple ainsi, mais ne négligez pas la première méthode.

Allez à : Exercice 3 :

Correction exercice 4 :

1. 9 est divisible par 9 mais pas par 6.
2. Soit n un nombre divisible par 100, donc il existe $k \in \mathbb{Z}$ tel que : $n = 100k = 25 \times 4k$ donc n est divisible par 25.
3. 6 est divisible par 2 et 3 mais pas par 12.
4. Soit n un nombre divisible par 10 et par 12, ilexiste $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$ tels que :
$$\begin{cases} n = 10k \\ n = 12k' \end{cases} \Rightarrow 10k = 12k' \Rightarrow 5k = 6k'$$
5 divise $6k'$ et 5 est premier avec 6, d'après le théorème de Gauss, 5 divise k', il existe $l \in \mathbb{Z}$ tel que $k' = 5l$, ce que l'on remplace dans $n = 12k'$, $n = 12k' = 12 \times 5l = 4 \times 3 \times 5l = 15 \times 4l$, donc n est divisible par 15.

Autre méthode :

n est divisible par $PPCM(10,12) = 60$, par conséquent il existe $l' \in \mathbb{Z}$ tel que $n = 60l' = 15 \times 4l'$, donc n est divisible par 15.

5. 24 est divisible par 6 et 8 mais 24 n'est pas divisible par 48.
6. On pose $n = 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10$.
$$1000 = 10^3 = (2 \times 5)^3 = 2^3 \times 5^3$$
$$n = 3 \times 2^2 \times 5 \times (2 \times 3) \times 7 \times 2^3 \times 3^2 \times (2 \times 5) = 2^6 \times 3^4 \times 5^2 \times 7 = 2^3 \times 5^2 \times 3^4 \times 7$$
$3^4 \times 7$ n'est pas divisible par 5 donc n n'est pas divisible par 1000.
7. $1600 = 16 \times 100 = 2^4 \times 4 \times 25 = 2^6 \times 5^2$
Donc $n = 1600 \times 3^4 \times 7$, n est un multiplie de 1600.
8. Soit N un entier dont l'écriture décimale est $a_n a_{n-1} \dots a_2 a_1 a_0$ alors
$$N = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = \sum_{i=0}^{n} a_i 10^i$$

Exemple :

Si $N = 2534$ alors $N = 2000 + 500 + 30 + 4 = 2 \times 10^3 + 5 \times 10^2 + 3 \times 10 + 4$

L'énoncé ce traduit par :
$$a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 = 39$$
On rappelle qu'un nombre est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3, et qu'un nombre est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.
39 est divisible par 3 et pas par 9, d'où le résultat.

9. 18 est divisible par 6 et par 9 d'où le résultat.

Allez à : Exercice 4 :

Correction exercice 5 :

1. Faux, 12 est divisible par 4 et par 6 mais 12 n'est pas divisible par $4 \times 6 = 24$.
2. Soit n un entier divisible par p et q, (avec p et q premier entre eux) alors il existe $k \in \mathbb{Z}$ et $l \in \mathbb{Z}$ tels que :
$$\begin{cases} n = kp \\ n = lq \end{cases} \Rightarrow kp = lq$$
p divise lq et p est premier avec q, d'après le théorème de Gauss, p divise l, il existe $k' \in \mathbb{Z}$ tel que $l = k'p$, ce que l'on remplace dans $n = lq$, $n = k'qp$ donc pq divise n.
3. Soit n divisible par a et par b, il existe $k \in \mathbb{Z}$ et $l \in \mathbb{Z}$ tels que $n = ka$ et $n = lb$, soit $d = PGCD(a, b)$, il existe $k' \in \mathbb{Z}$ et $l' \in \mathbb{Z}$ tels que $a = k'd$ et $b = l'd$ avec k' et l' premier entre eux.
$$\begin{cases} n = ka \\ n = lb \end{cases} \Rightarrow ka = lb \Rightarrow kk'd = ll'd \Rightarrow kk' = ll'$$
k' divise ll' et k' est premier avec l', d'après le théorème de Gauss k' divise l, il existe $k'' \in \mathbb{Z}$ tel que $l = k'k''$, ce que l'on remplace dans $n = lb$, alors $n = k'k''b$
Comme $ab = dm$ où $m = PPCM(a, b)$, $m = \frac{ab}{d} = \frac{(k'd)b}{d} = k'b$, donc
$$n = k''(k'b) = k''m$$
Ce qui montre bien que n est divisible par $PPCM(a, b)$.
4. $12 = 2 \times 6$, 4 divise 12 mais 4 ne divise pas 2 et ne divise pas 6. C'est faux
5. Soit p un nombre premier qui divise $n = ab$, en décomposant a et b en produit de facteurs premiers on sent bien que la réponse est vraie, on va faire un peu mieux.

Supposons que p ne divise pas b, donc p et b sont premiers entre eux, or p divise ab, d'après le théorème de Gauss p divise a. Cela suffit pour prouver que p divise a ou que p divise b.

6. 12 est divisible par 2 et par 6 mais 12 n'est pas divise par $2+6=8$.
7. Soient a, b et n trois entiers tels que n divise a et n divise b, il existe $k\in\mathbb{Z}$ et $l\in\mathbb{Z}$ tels que $a=kn$ et $b=ln$, alors $a+b=(k+l)n$ donc n divise $a+b$. La réponse est vraie.
8. Soient a et b deux entiers premiers entre eux, d'après l'identité de Bézout ils existent $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tels que : $au+bv=1$, alors $au+bu-bu+bv=1\Leftrightarrow(a+b)u+(-u+v)b=1$ ce qui montre que $a+b$ et b sont premiers entre eux, en inversant les rôle de a et b on montre de même que $a+b$ et a sont premier entre eux.
9. C'est faux, 2 et 3 sont premiers entre eux mais aucun des deux n'est premier avec $2\times 3=6$.
10. Soient a et b deux entiers premiers entre eux, d'après 8. a est premier avec $a+b$ et b est premier avec $a+b$, autrement dit les diviseurs premiers de a ne sont pas des diviseurs premiers de $a+b$, de même les diviseurs premiers de b ne sont pas des diviseurs premiers de $a+b$, donc les diviseurs premiers de ab (ce sont ceux de a et ceux de b) ne sont pas des diviseurs premiers de $a+b$, ce qui montre que ab et $a+b$ sont premiers entre eux.

Autre méthode : On reprend 8°) et on pose $c=a+b$, il existe des entiers u, u', v et v' tels que :

$$\begin{cases} au+cv=1 \\ bu'+cv'=1 \end{cases} \Rightarrow (au+cv)(bu'+cv')=1\times 1=1 \Rightarrow abuu'+acuv'+bcvu'+c^2vv'=1$$

$$\Rightarrow ab(uu')+c(auv'+bvu'+cvv')=1$$

$uu'\in\mathbb{Z}, auv'+bvu'+cvv'\in\mathbb{Z}$ d'après Bézout ab et $c=a+b$ sont premiers entre eux.

Allez à : Exercice 5 :

Correction exercice 6 :

1. Soit $D=PGCD(a,b)$, d'après l'identité de Bézout il existe $u\in\mathbb{Z}$ et $v\in\mathbb{Z}$ tel que :
$$au+bv=D$$
Si d divise a et b alors il existe $k\in\mathbb{Z}$ et $l\in\mathbb{Z}$ tels que $a=kd$ et $b=ld$, ce que l'on remplace dans l'identité ci-dessus
$$kdu+ldv=D\Leftrightarrow d(ku+lv)=D$$
Donc d divise D.
2. $8\times 3+(-4)\times 5=4$, mais 4 n'est pas le $PGCD(3,5)=1$, c'est faux.
3. En reprenant l'exemple ci-dessus 4 ne divise pas $1=PGCD(3,5)$, c'est faux.
4. On pose $D=PGCD(a,b)$ il existe $a'\in\mathbb{Z}$ et $b'\in\mathbb{Z}$ tels que $a=a'D$ et $b=b'D$ avec a' et b' premier entre eux. Ce que l'on remplace dans $au+bv=d$
$$a'Du+b'Dv=d\Leftrightarrow D(a'u+b'v)=d$$
Donc D divise d. C'est vrai.
5. On pose $D=PGCD(a,b)$ il existe $a'\in\mathbb{Z}$ et $b'\in\mathbb{Z}$ tels que $a=a'D$ et $b=b'D$ avec a' et b' premier entre eux. Si D divise d il existe $k_d\in\mathbb{Z}$ tel que $d=k_dD$
$$au+bv=d\Leftrightarrow a'Du+b'Dv=k_dD\Leftrightarrow a'u+b'v=k_d \quad (1)$$
Comme a' et b' sont premiers entre eux, il existe $u_0\in\mathbb{Z}$ et $v_0\in\mathbb{Z}$ tel que ;
$$a'u_0+b'v_0=1$$
En multipliant par k_d
$$a'k_du_0+b'k_dv_0=k_d \quad (2)$$
En soustrayant (1) et (2) :
$$a'(u-k_du_0)+b'(v-k_dv_0)=0\Leftrightarrow a'(u-k_du_0)=-b'(v-k_dv_0)$$
a' divise $-b'(v-k_dv_0)$ et a' et b' sont premiers entre eux, d'après le théorème de Gauss, a' divise $v-k_dv_0$ donc il existe $k\in\mathbb{Z}$ tel que $v-k_dv_0=ka'\Leftrightarrow v=k_dv_0+ka'$, ce que l'on remplace dans $a'(u-k_du_0)=-b'(v-k_dv_0)\Leftrightarrow a'(u-k_du_0)=-b'ka'\Leftrightarrow u-k_du_0=-b'k\Leftrightarrow u=k_du_0-b'k$

La réciproque est évidente.

Tous les couples $(u,v)=(k_du_0-b'k,k_dv_0+ka')\quad k\in\mathbb{Z}$ sont solutions de
$$au+bv=d$$
Il y a une infinité de solutions.

Prenons un exemple pour « visualiser » les choses.
$$10\times 30+14\times(-21)=6$$
$$10\times 9+14\times(-6)=6$$

C'est-à-dire $a = 10$, $b = 14$, $d = 6$, on a deux couples (u, v) $((30, -21)$ et $(9, -6))$ tels que :

$$10u + 14v = 6$$

6. On pose $D = PGCD(a, b)$.
   Si d est un multiple de $PGCD(a, b)$, il existe $k \in \mathbb{Z}$ tel que $d = kD$, or d'après l'identité de Bézout il existe $u' \in \mathbb{Z}$ et $v' \in \mathbb{Z}$ tels que $au' + bv' = D$, en multipliant cette égalité par k on trouve $a(ku') + b(kv') = kD$, on pose alors $u = ku'$ et $v = kv'$ ce qui donne $au + bv = d$, on a montré l'une des deux implications

Réciproque : s'il existe un couple d'entiers (u, v), tel que $au + bv = d$.

On utilise 4°) et alors D divise d, autrement dit d est un multiple de $D = PGCD(a, b)$.

Allez à : Exercice 6 :

Correction exercice 7 :

1. Soit n un entier congru à 0 modulo 6, il existe $k \in \mathbb{Z}$ tel que $n = 0 + 6k = 6k$, ce qui montre que 6 divise n (c'était vraiment évident).
2. $2 \times 3 = 6 \equiv 0 \ \ [6]$ et pourtant ni 2, ni 3 ne sont congrus à 0 modulo 6.
3. Soit n un entier congru à 5 modulo 6, il existe $k \in \mathbb{Z}$ tel que $n = 5 + 6k$, alors
$$n = -1 + 6 + 6k = -1 + 6(k + 1)$$
   Ce qui montre que n est congru à -1 modulo 6. (On peut affirmer ceci sans faire la démonstration ci-dessus).
   Maintenant on va utiliser les propriétés des congruences
$$n \equiv -1 \ \ [6] \Rightarrow n^{2p} \equiv (-1)^{2p} \ \ [6] \equiv 1 \ \ [6]$$
   C'est bien cela, les puissances paires de n sont congrus à -1 modulo 6.
4. Si $a \equiv 4 \ \ [6]$ et $b \equiv 4 \ \ [6]$ alors $a + b \equiv 4 + 4 \ \ [6] \equiv 8 \ \ [6] \equiv 2 \ \ [6]$
5. Si $a \equiv 4 \ \ [6]$ et $b \equiv 4 \ \ [6]$ alors $ab \equiv 4 \times 4 \ \ [6] \equiv 16 \ \ [6] \equiv 4 \ \ [6]$
   L'affirmation est fausse.
6. D'après le 5. $a^2 \equiv 4 \ \ [6]$, puis par une récurrence très simple, $a^n \equiv 4 \ \ [6]$.
   L'affirmation est vraie.

Allez à : Exercice 7 :

Correction exercice 8 :

1. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $ab \equiv 0 \ \ [5]$, il existe $k \in \mathbb{Z}$ tel que : $ab = 5k$
   Supposons que a ne soit pas un multiple de 5, 5 étant premier, a et 5 sont premiers entre eux, de plus 5 divise $5a$, d'après le théorème de Gauss 5 divise b, autrement dit b est un multiple de 5. Cela suffit à montrer que a ou b est un multiple de 5.
2. Soit $a \in \mathbb{Z}$ tels que $a \equiv 2 \ \ [5]$, $a^2 \equiv 2^2 \ \ [5] \equiv 4 \ \ [5] \equiv -1 \ \ [5]$, $a^4 \equiv (-1)^2 \ \ [5] \equiv 1 \ \ [5]$.
3. Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}$ tels que $a \equiv 2 \ \ [5]$ et $b \equiv 2 \ \ [5]$ alors $a + b \equiv 2 + 2 \ \ [5] \equiv 4 \ \ [5]$, l'affirmation est fausse.
4. Soit $a \in \mathbb{Z}$ non multiple de 5, a et 5 sont premier entre eux, d'après l'identité de Bézout, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que $au + 5v = 1$, on en déduit que $au = 1 + 5(-v)$, autrement dit $au \equiv 1 \ \ [5]$.
   L'affirmation est vraie, pour tout $a \in \mathbb{Z}$ il existe $u \in \mathbb{Z}$ tel que : $au \equiv 1 \ \ [5]$
5. $3 \times 3 = 9 \equiv -1 \ \ [5]$, l'affirmation est fausse.
6. $0^2 = 0 \equiv 0 \ \ [5]$, $1^2 = 1 \equiv 1 \ \ [5]$, $2^2 = 4 \equiv -1 \ \ [5]$, $3^3 = 9 \equiv -1 \ \ [5]$, $4^2 = 16 \equiv 1 \ \ [5]$.
   Pour les autres entiers, ils sont congrus soit à $0 \ \ [5]$, soit à $1 \ \ [5]$, soit à $2 \ \ [5]$, soit à $3 \ \ [5]$, soit à $4 \ \ [5]$, donc leur carré est congru à $0^2 \ \ [5]$, soit à $1^2 \ \ [5]$, soit $2^2 \ \ [5]$, soit à $3^2 \ \ [5]$, soit à $4^2 \ \ [5]$, par conséquent il n'y a pas d'entier dont le carré soit congru à 2 modulo 5.
7. C'est faux $0^4 = 0 \ \ [5]$.
8. Au 6. on a vu que tous les entiers non multiples de 5 avait un carré congru à -1 ou 1. Dont le carré du carré (la puissance 4ième) est congru à 1 modulo 5.

Allez à : Exercice 8 :

Correction exercice 9 :

1. La contraposée de cette proposition est :
   Si n n'est pas premier alors n est divisible par au moins un nombre inférieur ou égal à $\sqrt{n}$.

Démontrons cela.

n n'est pas premier, il existe $a \in \mathbb{N}$ et $b \in \mathbb{N}$ tels que $n = ab$ et $a \geq b$ (Si cela ne vous plait pas, on peut prendre $a \leq b$), donc $n \geq b^2$, par conséquent $\sqrt{n} \geq b$.

2. $n! + 2$ est divisible par 2, $n! + 3$ est divisible par 3,…, $n! + n$ est divisible par n, ces nombres ne sont pas premiers.
3. $n! + 2, n! + 3, \ldots, n! + n$ sont $n - 1$ entiers consécutifs non premiers, ceci étant vrai pour tout $n \in \mathbb{N}$, il existe n entiers consécutifs non premiers. $((n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1))$.

Allez à : Exercice 9 :

Correction exercice 10 :

Réfléchissons un peu avant de nous lancer dans les calculs. Il y a 7 jours par semaines, la congruence modulo 7 va nous rendre service.

Ensuite on va compter le nombre de jours entre le premier Janvier 2007 (ce jour là compris) et un jour quelconque.

Il y a $n_1 = 31$ jours en Janvier, $n_2 = 28$ (ou $n_2' = 29$ en Février 2008), $n_3 = 31$ jours en Mars,…

$$a = n_1 = n_3 = n_5 = n_7 = n_8 = n_{10} = n_{12} = 31 \equiv 3 \ [7]$$

$$n_2 = 28 \equiv 0 \ [7] \ ou \ n_2' = 29 \equiv 1 \ [7]$$

$$b = n_4 = n_6 = n_9 = n_{11} = 30 \equiv 2 \ [7]$$

Si on s'y prend de cette façon (ce n'est pas la seule façon de faire), si on tombe sur un nombre congru à 1 c'est un Lundi, si le nombre est congru à 2 c'est un Mardi, si le nombre est congru à 3 c'est un Mercredi, si le nombre est congru à 4 c'est un Jeudi, si le nombre est congru à 5 c'est un Vendredi, si le nombre est congru à 6 c'est un Samedi et enfin si le nombre est congru à 6 c'est un Dimanche.

1. Le nombre de jour entre le premier Janvier 2007 (ce jour là compris) et le 2 Juillet 2007 est :
$$N = n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + 2 = 3a + n_2 + 2b + 2 \equiv 9 + 0 + 4 + 2 \ [7] \equiv 13 \ [7] \equiv 1 \ [7]$$
Le 2 Juillet 2007 était un Lundi.
2. Le nombre de jour entre le premier Janvier 2007 (ce jour là compris) et le 15 Janvier 2008 est :
$$N = n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 + n_9 + n_{10} + n_{11} + n_{12} + 15 = 7a + n_2 + 4b + 15$$
$$\equiv 0 \times 3 + 0 + 4 \times 2 + 1 \ [7] \equiv 2 \ [7]$$
Le 15 Janvier 2008 était un Mardi.
3. Le nombre de jour entre le premier Janvier 2007 (ce jour là compris) et le 19 Mars 2008 est :
$$N = n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 + n_9 + n_{10} + n_{11} + n_{12} + n_1 + n_2' + 19$$
$$= 8a + n_2 + n_2' + 4b + 19 \equiv 1 \times 3 + +0 + 1 + 4 \times 2 + 5 \ [7] \equiv 3 \ [7]$$
Le 19 Mars 2008 était un Mercredi.
4. Le nombre de jour entre le premier Janvier 2007 (ce jour là compris) et le 14 Juillet 2010 est :
On va un peu raccourcir, du 1 Janvier 2007 au 31 Décembre 2009, cela fait 3 ans, dont une année bissextile.
$$N = 3(n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 + n_9 + n_{10} + n_{11} + n_{12}) + 1 + n_1 + n_2 + n_3 + n_4$$
$$+ n_5 + n_6 + 14 = 3(7a + n_2 + 4b) + 1 + 3a + n_2 + 2b + 14$$
$$= 24a + 4n_2 + 14b + 15 \equiv 3 \times 3 + 4 \times 0 + 0 \times 2 + 1 \ [7] \equiv 3 \ [7]$$
Le 14 Juillet 2010 était un Mercredi.
5. Le nombre de jour entre le premier Janvier 2007 (ce jour là compris) et le 26 Août 2011 est :
On va un peu raccourcir, du 1 Janvier 2007 au 31 Décembre 2010, cela fait 4 ans, dont une année bissextile.
$$N = 4(n_1 + n_2 + n_3 + n_4 + n_5 + n_6 + n_7 + n_8 + n_9 + n_{10} + n_{11} + n_{12}) + 1 + n_1 + n_2 + n_3 + n_4$$
$$+ n_5 + n_6 + n_7 + 26 = 4(7a + n_2 + 4b) + 1 + 4a + n_2 + 2b + 26$$
$$= 32a + 5n_2 + 18b + 27 \equiv 4 \times 3 + 5 \times 0 + 4 \times 2 + 6 \ [7] \equiv 5 \ [7]$$
Le 26 Août 2011 sera un Vendredi.

Allez à : Exercice 10 :

Correction exercice 11 :

Soit n ce nombre, il existe $q \in \mathbb{N}$ tel que $n = 7q + 5$ et $q = 7 \times 12 + 3 = 87$ donc
$$n = 7 \times 87 + 5 = 611$$

Allez à : Exercice 11 :

Correction exercice 12 :

$$842 = 256 \times 3 + 74$$

Donc

$$96842 = 256 \times 375 + 3 \times 256 + 74 = 256 \times 378 + 74$$

Le reste de la division euclidienne de 96842 par 256 est 74.

$$842 = 375 \times 2 + 92$$

Donc

$$96842 = 256 \times 375 + 375 \times 2 + 92 = 375 \times 258 + 92$$

Le reste de la division euclidienne de 96842 par 375 est 92.

Allez à : Exercice 12 :

Correction exercice 13 :

$$\begin{aligned}N = 3379026 \times 609806770 &= (198765 \times 17 + 21) \times (35870986 \times 17 + 8)\\ &= 198765 \times 17 \times 35870986 \times 17 + 198765 \times 17 \times 8 + 21 \times 35870986 \times 17 + 21\\ &\times 8 = 17 \times (198765 \times 17 \times 35870986 + 198765 \times 8 + 21 \times 35870986) + 21 \times 8\\ &= 17 \times (198765 \times 17 \times 35870986 + 198765 \times 8 + 21 \times 35870986) + (17 + 4)\\ &\times 8\\ &= 17 \times (198765 \times 17 \times 35870986 + 198765 \times 8 + 21 \times 35870986 + 8) + 4 \times 8\\ &= 17 \times (198765 \times 17 \times 35870986 + 198765 \times 8 + 21 \times 35870986 + 8) + 32\\ &= 17 \times (198765 \times 17 \times 35870986 + 198765 \times 8 + 21 \times 35870986 + 8) + 17 + 15\\ &= 17 \times (198765 \times 17 \times 35870986 + 198765 \times 8 + 21 \times 35870986 + 8 + 1) + 15\end{aligned}$$

Comme $0 \le 15 < 17$.

Le reste de la division euclidienne de N par 17 est 15.

Autre méthode

En utilisant les congruences modulo 17.

$$3379026 = 198765 \times 17 + 21 \equiv 21 \quad [17] \equiv 4 \quad [17]$$

$$609806770 = 35870986 \times 17 + 8 \equiv 8 \quad [17]$$

Donc $N \equiv 4 \times 8 \quad [17] \equiv 32 \quad [17] \equiv 15 \quad [17]$

Comme $0 \le 15 < 17$.

Le reste de la division euclidienne de N par 17 est 15.

Allez à : Exercice 13 :

Correction exercice 14 :

La méthode classique veut que l'on regarde si 2 divise ce nombre, si la réponse est oui, on divise par 2 sinon on regarde si 3 divise ce nombre, si la réponse est oui on divise par 3, sinon on regarde si 5 divise ce nombre, etc…pour tous les nombres premiers jusqu'à la partie entière de la racine carrée de ce nombre.

$$60 = 2 \times 30 = 2^2 \times 15 = 2^2 \times 3 \times 5$$

$$360 = 2 \times 180 = 2^2 \times 90 = 2^3 \times 45 = 2^3 \times 3 \times 15 = 2^3 \times 3^2 \times 5$$

$$2400 = 2 \times 1200 = 2^2 \times 600 = 2^3 \times 300 = 2^4 \times 150 = 2^5 \times 75 = 2^5 \times 3 \times 25 = 2^5 \times 3 \times 5^2$$

$$4675 = 5 \times 935 = 5^2 \times 187 = 5^2 \times 11 \times 17$$

$$\begin{aligned}9828 &= 2 \times 4914 = 2^2 \times 2457 = 2^2 \times 3 \times 819 = 2^2 \times 3^2 \times 273 = 2^2 \times 3^3 \times 91\\ &= 2^2 \times 3^3 \times 7 \times 13\end{aligned}$$

$$\begin{aligned}15200 &= 2 \times 7600 = 2^2 \times 3800 = 2^3 \times 1900 = 2^4 \times 950 = 2^5 \times 475 = 2^5 \times 5 \times 95\\ &= 2^5 \times 5^2 \times 19\end{aligned}$$

$$\begin{aligned}45864 &= 2 \times 22932 = 2^2 \times 11466 = 2^3 \times 5733 = 2^3 \times 3 \times 1911 = 2^3 \times 3^2 \times 637\\ &= 2^3 \times 3^2 \times 7 \times 91 = 2^3 \times 3^2 \times 7^2 \times 13\end{aligned}$$

$$792792$$

Cela risque d'être pénible si on utilise la méthode classique, on remarque que :

$$792792 = 792 \times 1001$$

$$1001 = 7 \times 143 = 7 \times 11 \times 13$$

$$792 = 2 \times 396 = 2^2 \times 198 = 2^3 \times 99 = 2^3 \times 3 \times 33 = 2^3 \times 3^2 \times 11$$

Donc

$$792792 = 7 \times 11 \times 13 \times 2^3 \times 3^2 \times 11 = 2^3 \times 3^2 \times 7 \times 11^2 \times 13$$

Allez à : Exercice 14 :

Correction exercice 15 :

$2244 = 2 \times 1089 + 66$, $1089 = 16 \times 66 + 33$ et $66 = 2 \times 33 + 0$

Donc $PGCD(2244,1089) = 33$ et

$$33 = 1089 - 16 \times 66 = 1089 - 16 \times (2244 - 2 \times 1089) = -16 \times 2244 + 33 \times 1089$$

Allez à : Exercice 15 :

Correction exercice 16 :

a)

$$84 = 1 \times 60 + 24$$
$$60 = 2 \times 24 + 12$$
$$24 = 2 \times 12$$
$$PGCD(84,60) = 12$$

C'est le dernier reste non nul.

$$PPCM(84,60) = \frac{84 \times 60}{PGCD(84,60)} = \frac{84 \times 60}{12} = 420$$
$$12 = 60 - 2 \times 24 = 60 - 2 \times (84 - 1 \times 60) = -2 \times 84 + 3 \times 60$$

Une solution particulière de $60u + 84v = 12$ est :

$$3 \times 60 + (-2) \times 84 = 12$$

On fait la soustraction de $60u + 84v = 12$ avec $3 \times 60 + (-2) \times 84 = 12$

$$60(u-3) + 84(v+2) = 0 \Leftrightarrow 60(u-3) = -84(v+2) \Leftrightarrow 5(u-3) = -7(v+2)$$

5 divise $-7(v+2)$ et 5 est premier avec 7, d'après le théorème de Gauss 5 divise $-(v+2)$, par conséquent il existe $k \in \mathbb{Z}$ tel que $-(v+2) = 5k \Leftrightarrow v = -2 - 5k$, ce que l'on remplace dans $5(u-3) = -7(v+2)$, ce qui donne $5(u-3) = 7 \times 5k \Leftrightarrow u - 3 = 7k \Leftrightarrow u = 3 + 7k$.

Réciproque

$$60(u-3) + 84(v+2) = 60(3 + 7k - 3) + 84(-2 - 5k + 2) = 60 \times 7k - 84 \times 5k = 0$$

L'ensemble des couples (u, v) recherchés sont :

$$(3 + 7k, -2 - 5k), \quad k \in \mathbb{Z}$$
$$60 = 2^2 \times 3 \times 5 \quad et \quad 84 = 2^2 \times 3 \times 7$$
$$PGCD(60,84) = 2^2 \times 3 = 12$$
$$PPCM(60,84) = 2^2 \times 3 \times 5 \times 7 = 420$$

Allez à : Exercice 16 :

b)

$$360 = 1 \times 240 + 120$$
$$240 = 2 \times 120$$
$$PGCD(360,240) = 120$$

C'est le dernier reste non nul

$$PPCM(360,240) = \frac{360 \times 240}{120} = 720$$
$$120 = 1 \times 360 - 1 \times 240$$

Une solution particulière de $360u + 240v = 120$ est $120 = 1 \times 360 - 1 \times 240$

On fait la soustraction $360u + 240v = 120$ avec $1 \times 360 - 1 \times 240 = 120$

$$360(u-1) + 240(v+1) = 0 \Leftrightarrow 360(u-1) = -240(v+1) \Leftrightarrow 3(u-1) = -2(v+1)$$

3 divise $-2(v+1)$ et 3 est premier avec 2, d'après le théorème de Gauss 3 divise $-(v+1)$, par conséquent il existe $k \in \mathbb{Z}$ tel que $-(v+1) = 3k \Leftrightarrow v = -1 - 3k$, ce que l'on remplace dans $3(u-1) = -2(v+1)$, ce qui donne $3(u-1) = 2 \times 3k \Leftrightarrow u - 1 = 2k \Leftrightarrow u = 1 + 2k$.

La réciproque est évidente (voir a)), l'ensemble des couples (u,v) recherchés sont :

$$(1+2k,-1-3k),\quad k\in\mathbb{Z}$$
$$360=2^3\times 3^2\times 5$$
$$240=2^4\times 3\times 5$$
$$PGCD(360,240)=2^3\times 3\times 5=120$$
$$PPCM(360,240)=2^4\times 3^2\times 5=720$$

Allez à : Exercice 16 :

c)

$$171=1\times 160+11$$
$$160=14\times 11+6$$
$$11=1\times 6+5$$
$$6=1\times 5+1$$
$$5=5\times 1$$
$$PGCD(171,160)=1$$

C'est le dernier reste non nul.

$$PPCM(171,160)=171\times 160=27360$$
$$1=6-1\times 5=6-1\times(11-1\times 6)=-1\times 11+2\times 6=-1\times 11+2\times(160-14\times 11)$$
$$=2\times 160-29\times 11=2\times 160-29\times(171-1\times 160)=-29\times 171+31\times 160$$
$$-29\times 171+31\times 160=1$$

Une solution particulière de $160u+171v=1$ est $31\times 160-29\times 171=1$.

On fait la soustraction de $160u+171v=1$ par $31\times 160-29\times 171=1$

$$160(u-31)+171(v+29)+0\Leftrightarrow 160(u-31)=-171(v+29)$$

160 divise $-171(v+29)$ et 160 est premier avec 171, d'après le théorème de Gauss 160 divise $-(v+29)$, il existe $k\in\mathbb{Z}$ tel que $-(v+29)=160k\Leftrightarrow v=-29-160k$, ce que l'on remplace dans

$$160(u-31)=-171(v+29)\Leftrightarrow 160(u-31)=171\times 160k\Leftrightarrow u-31=171k\Leftrightarrow u=31+171k$$

La réciproque étant toujours aussi évidente, les couples (u,v) recherchés sont :

$$(31+171k,-29-160k),\quad k\in\mathbb{Z}$$
$$171=3^2\times 19$$
$$160=2^5\times 5$$
$$PGCD(171,160)=1$$
$$PPCM(171,160)=2^5\times 3^2\times 5\times 19=27360$$

Allez à : Exercice 16 :

d)

$$360=1\times 345+15$$
$$345=23\times 15$$
$$PGCD(360,345)=15$$
$$PPCM(360,345)=\frac{360\times 345}{15}=8280$$
$$15=1\times 360-1\times 345$$

Une solution particulière de $360u+345v=15$ est $1\times 360-1\times 345=15$

On fait la soustraction de $360u+345v=15$ par $1\times 360-1\times 345=15$

$$360(u-1)+345(v+1)=0\Leftrightarrow 360(u-1)=-345(v+1)\Leftrightarrow 24(u-1)=-23(v+1)$$

24 divise $-23(v+1)$ et 24 est premier avec 23, d'après le théorème de Gauss 24 divise $-(v+1)$, il existe $k\in\mathbb{Z}$ tel que $-(v+1)=24k\Leftrightarrow v=-1-24k$, ce que l'on remplace dans

$$24(u-1)=-23(v+1)\Leftrightarrow 24(u-1)=23\times 24k\Leftrightarrow u-1=23k\Leftrightarrow u=1+23k$$

Comme d'habitude la réciproque est évidente, les couples (u,v) recherchés sont

$$(1+23k,-1-24k),\quad k\in\mathbb{Z}$$
$$360=2^3\times 3^2\times 5$$
$$345=3\times 5\times 23$$
$$PGCD(360,345)=3\times 5=15$$
$$PPCM(360,345)=2^3\times 3^2\times 5\times 23=8280$$

Allez à : Exercice 16 :

e)

$$520=1\times 325+195$$
$$325=1\times 195+130$$
$$195=1\times 130+65$$
$$130=2\times 65$$
$$PGCD(520,325)=65$$
$$PPCM(520,325)=\frac{520\times 325}{65}=2600$$
$$65=195-1\times 130=195-1\times(325-1\times 195)=-1\times 325+2\times 195$$
$$=-1\times 325+2\times(520-1\times 325)=2\times 520-3\times 325$$

Une solution particulière de $325u+520v=65$ est $-3\times 325+2\times 520=65$

On fait la soustraction de $325u+520v=65$ par $-3\times 325+2\times 520=65$

$$325(u+3)+520(v-2)=0\Leftrightarrow 325(u+3)=-520(v-2)\Leftrightarrow 5(u+3)=-8(v-2)$$

5 divise $-8(v-2)$ et 5 est premier avec 8, d'après le théorème de Gauss 5 divise $-(v-2)$, il existe $k\in\mathbb{Z}$ tel que $-(v-2)=5k\Leftrightarrow v=2-5k$, ce que l'on remplace dans

$$5(u+3)=-8(v-2)\Leftrightarrow 5(u+3)=8\times 5k\Leftrightarrow u+3=8k\Leftrightarrow u=-3+8k$$

Les couples recherchés sont

$$(-3+8k,2-5k),\quad k\in\mathbb{Z}$$
$$520=2^3\times 5\times 13$$
$$325=5^2\times 13$$
$$PGCD(325,520)=5\times 13=65$$
$$PPCM(325,520)=2^3\times 5^2\times 13=2600$$

Remarque : pour faire ce genre de calculs la calculatrice est totalement inutile, il suffit de bien s'y prendre et le calcul est on ne peut plus simple :

$$2^3\times 5^2\times 13=(2\times 5)\times(2\times 5)\times 2\times 13=10\times 10\times 26=2600$$

Cela se fait de tête !

Allez à : Exercice 16 :

f)

$$720=2\times 252+216$$
$$252=1\times 216+36$$
$$216=6\times 36$$
$$PGCD(720,252)=36$$
$$PPCM(720,252)=\frac{720\times 252}{36}=5040$$
$$36=252-1\times 216=252-1\times(720-2\times 252)=-1\times 720+3\times 252$$

Une solution particulière de $720u+252v=36$ est $-1\times 720+3\times 252=36$

On fait la soustraction de $720u+252v=36$ par $-1\times 720+3\times 252=36$

$$720(u+1)+252(v-3)=0\Leftrightarrow 720(u+1)=-252(v-3)\Leftrightarrow 20(u+1)=-7(v-3)$$

20 divise $-7(v-3)$ et 20 est premier avec $-7(v-3)$, d'après le théorème de Gauss 20 divise $-(v-3)$, il existe $k\in\mathbb{Z}$ tel que $-(v-3)=20k\Leftrightarrow v=3-20k$, ce que l'on remplace dans

$$20(u+1)=-7(v-3)\Leftrightarrow 20(u+1)=7\times 20k\Leftrightarrow u+1=7k\Leftrightarrow u=-1+7k$$

Les couples (u,v) recherchés sont

$$(-1+7k,3-20k),\quad k\in\mathbb{Z}$$
$$720=2^4\times 3^2\times 5$$
$$252=2^2\times 3^2\times 7$$
$$PGCD(720,252)=2^2\times 3^2=36$$
$$PPCM(720,252)=2^4\times 3^2\times 5\times 7=5040$$

Allez à : Exercice 16 :

g)

$$955=5\times 183+40$$
$$183=4\times 40+23$$
$$40=1\times 23+17$$
$$23=1\times 17+6$$
$$17=2\times 6+5$$
$$6=1\times 5+1$$
$$5=5\times 1$$
$$PGCD(955,183)=1$$
$$PPCM(955,183)=955\times 183=174765$$
$$\begin{aligned}1&=6-1\times 5=6-1\times(17-2\times 6)=-1\times 17+3\times 6=-1\times 17+3\times(23-1\times 17)\\&=3\times 23-4\times 17=3\times 23-4\times(40-1\times 23)=-4\times 40+7\times 23\\&=-4\times 40+7\times(183-4\times 40)=7\times 183-32\times 40\\&=7\times 183-32\times(955-5\times 183)=-32\times 955+167\times 183\end{aligned}$$

Une solution particulière de $955u+183v=1$ est $-32\times 955+167\times 183=1$

On fait la soustraction de $955u+183v=1$ par $-32\times 955+167\times 183=1$

$$955(u+32)+183(v-167)=0\Leftrightarrow 955(u+32)=-183(v-167)$$

955 divise $-183(v-167)$ et 955 est premier avec 183, d'après le théorème de Gauss 955 divise $-(v-167)$, il existe $k\in\mathbb{Z}$ tel que $-(v-167)=955k\Leftrightarrow v=167-955k$, ce que l'on remplace dans

$$955(u+32)=-183(v-167)\Leftrightarrow 955(u+32)=183\times 955k\Leftrightarrow u+32=183k\Leftrightarrow u=-32+183k$$

Les couples (u,v) recherchés sont

$$(-32+183k,167-955k),\quad k\in\mathbb{Z}$$
$$955=5\times 191$$

191 est premier mais ce n'est pas si évident, ce nombre n'est pas divise par 2, ni par 3, ni par 5, $\frac{191}{7}=27,28\ldots$ donc ni par 7, $\frac{191}{11}=17,36\ldots$ donc ni par 11, $\frac{191}{13}=14,69\ldots$ donc ni par 13, $\frac{191}{17}=11,23\ldots$ donc ni par 17 et là on s'arrête parce que $11,23\ldots<17$ on a vu ce résultat, mais c'est assez intuitif, en effet si ce nombre était divisible par un nombre premier supérieur ou égal à 17 le résultat serait inférieur à $11,23\ldots$ et du coup on s'en serait déjà rendu compte.

$$183=3\times 61$$

61 est premier, c'est l'occasion de rappeler que tous les nombres inférieurs à 100 qui « ont l'air premier » (c'est-à-dire qui ne sont divisibles ni par 2, ni par 3, ni par 5, ni par 7 en étant inférieur à 77) sont premiers sauf 91 car $91=7\times 13$.

$$PGCD(955,183)=1$$
$$PGCD(955,183)=3\times 5\times 61\times 191=174765$$

Là, il faut une machine.

Allez à : Exercice 16 :

h)

$$1665=1\times 1035+630$$
$$1035=1\times 630+405$$
$$630=1\times 405+225$$

$$405 = 1 \times 225 + 180$$
$$225 = 1 \times 180 + 45$$
$$180 = 4 \times 45$$
$$PGCD(1665{,}1065) = 45$$
$$PPCM(1665{,}1035) = \frac{1665 \times 1035}{45} = 38295$$
$$\begin{aligned}45 = 225 - 1 \times 180 = 225 - 1 \times (405 - 1 \times 225) &= -1 \times 405 + 2 \times 225\\ &= -1 \times 405 + 2 \times (630 - 1 \times 405) = 2 \times 630 - 3 \times 405\\ &= 2 \times 630 - 3 \times (1035 - 1 \times 630) = -3 \times 1035 + 5 \times 630\\ &= -3 \times 1035 + 5 \times (1665 - 1 \times 1035) = 5 \times 1665 - 8 \times 1035\end{aligned}$$

Une solution particulière de $1665u + 1035v = 45$ est $5 \times 1665 - 8 \times 1035 = 45$

On fait la soustraction de $1665u + 1035v = 45$ par $5 \times 1665 - 8 \times 1035 = 45$

$$1665(u-5) + 1035(v+8) = 0 \Leftrightarrow 1665(u-5) = -1035(v+8) \Leftrightarrow 37(u-5) = -23(v+8)$$

37 divise $-23(v+8)$ et 37 est premier avec 23, d'après le théorème de Gauss 37 divise $-(v+8)$ il existe $k \in \mathbb{Z}$ tel que $-(v+8) = 37k \Leftrightarrow v = -8 - 37k$, ce que l'on remplace dans

$$37(u-5) = -23(v+8) \Leftrightarrow 37(u-5) = 23 \times 37k \Leftrightarrow u - 5 = 23k \Leftrightarrow u = 5 + 23k$$

Les couples (u, v) recherchés sont

$$(5 + 23k, -8 - 37k), \quad k \in \mathbb{Z}$$
$$1665 = 3^2 \times 5 \times 37$$
$$1035 = 3^2 \times 5 \times 23$$
$$PGCD(1665{,}1035) = 3^2 \times 5 = 45$$
$$PPCM(1665{,}1035) = 3^2 \times 5 \times 23 \times 37 = 38295$$

Allez à : Exercice 16 :

i)

$a = 18480$, $b = 9828$

$$18480 = 1 \times 9828 + 8652$$
$$9828 = 1 \times 8652 + 1176$$
$$8652 = 7 \times 1176 + 420$$
$$1176 = 2 \times 420 + 336$$
$$420 = 1 \times 336 + 84$$
$$336 = 4 \times 84$$
$$PGCD(18480{,}9828) = 84$$
$$PPCM(18480{,}9828) = \frac{18480 \times 9828}{84} = 2162160$$
$$\begin{aligned}84 = 420 - 1 \times 336 = 420 - 1 \times (1176 - 2 \times 420) &= -1 \times 1176 + 3 \times 420\\ &= -1 \times 1176 + 3 \times (8652 - 7 \times 1176) = 3 \times 8652 - 22 \times 1176\\ &= 3 \times 8652 - 22 \times (9828 - 1 \times 8652) = -22 \times 9828 + 25 \times 8652\\ &= -22 \times 9828 + 25 \times (18480 - 1 \times 9828) = 25 \times 18480 - 47 \times 9828\end{aligned}$$

Une solution particulière de $18480u + 9828v = 84$ est $25 \times 18480 - 47 \times 9828 = 84$

On fait la division de $18480u + 9828v = 84$ par $25 \times 18480 - 47 \times 9828 = 84$

$$18480(u-25) + 9828(v+47) = 0 \Leftrightarrow 18480(u-25) = -9828(v+47)$$
$$\Leftrightarrow 220(u-25) = -117(v+47)$$

220 divise $-117(v+47)$ et 220 est premier avec 117, d'après le théorème de Gauss 220 divise $-(v+47)$, il existe $k \in \mathbb{Z}$ tel que $-(v+47) = 220k \Leftrightarrow v = -47 - 220k$, ce que l'on remplace dans

$$220(u-25) = -117(v+47) \Leftrightarrow 220(u-25) = 117 \times 220k \Leftrightarrow u - 25 = 117k \Leftrightarrow u = 25 + 117k$$

Les couples (u, v) recherchés sont

$$(25 + 117k, -47 - 220k), \quad k \in \mathbb{Z}$$
$$18480 = 2^4 \times 3 \times 5 \times 7 \times 11$$
$$9828 = 2^2 \times 3^3 \times 7 \times 13$$
$$PGCD(18480{,}9828) = 2^2 \times 3 \times 7 = 84$$
$$PPCM(18480{,}9828) = 2^4 \times 3^3 \times 5 \times 7 \times 11 \times 13 = 2162160$$

Allez à : Exercice 16 :

Correction exercice 17 :

1. $8303 = 3 \times 2717 + 152$; $2717 = 17 \times 152 + 133$; $152 = 1 \times 133 + 19$; $133 = 7 \times 19 + 0$.
$$19 = 152 - 1 \times 133 = 152 - 1 \times (2717 - 17 \times 152) = -1 \times 2717 + 18 \times 152$$
$$= -1 \times 2717 + 18 \times (8303 - 3 \times 2717) = 18 \times 8303 - 55 \times 2717$$
Et $D = PGCD(8303,2717) = 19$
2. $M = \frac{8303 \times 2717}{19} = 1187329$
3. $1001 = 3 \times 315 + 56$; $315 = 5 \times 56 + 35$; $56 = 1 \times 35 + 21$; $35 = 1 \times 21 + 14$; $21 = 1 \times 14 + 7$; $14 = 2 \times 7 + 0$.
$$7 = 21 - 1 \times 14 = 21 - 1 \times (35 - 1 \times 21) = -1 \times 35 + 2 \times 21 = -1 \times 35 + 2 \times (56 - 1 \times 35)$$
$$= 2 \times 56 - 3 \times 35 = 2 \times 56 - 3 \times (315 - 5 \times 56) = -3 \times 315 + 17 \times 56$$
$$= -3 \times 315 + 17 \times (1001 - 3 \times 315) = 17 \times 1001 - 54 \times 315$$
4. $2244 = 2 \times 1089 + 66$, $1089 = 16 \times 66 + 33$ et $66 = 2 \times 33 + 0$
Donc $PGCD(2244,1089) = 33$ et
$$33 = 1089 - 16 \times 66 = 1089 - 16 \times (2244 - 2 \times 1089) = -16 \times 2244 + 33 \times 1089$$

Allez à : Exercice 17 :

Correction exercice 18 :

1. Une identité de Bézout entre 3 et 5 est $2 \times 3 - 5 = 1$, on multiplie cette égalité par 13 :
$$26 \times 3 - 13 \times 5 = 13$$
On soustrait $3x - 5y = 13$ et $26 \times 3 - 13 \times 5 = 13$:
$$3(x - 26) - 5(y - 13) = 0 \Leftrightarrow 3(x - 26) = 5(y - 13)$$
D'après le théorème de Gauss, comme 3 divise $5(y - 13)$ et que 3 et 5 sont premiers entre eux, 3 divise $y - 13$, il existe donc $k \in \mathbb{Z}$ tel que : $y - 13 = 3k$, d'où $y = 13 + 3k$, on remplace cela dans $3(x - 26) = 5(y - 13)$, cela donne $3(x - 26) = 5 \times 3k \Leftrightarrow x - 26 = 5k \Leftrightarrow x = 26 + 5k$. Les solutions sont :
$$S = \{(26 + 5k, 13 + 3k), k \in \mathbb{Z}\}$$
2. Il faut d'abord trouver une solution particulière de $212x + 45y = 3$, pour cela on va écrire une équation de Bézout entre 212 et 45, ici c'est moins évident que dans le 1.
$212 = 4 \times 45 + 32$; $45 = 1 \times 32 + 13$; $32 = 2 \times 13 + 6$; $13 = 2 \times 6 + 1$; $6 = 6 \times 1 + 0$
$$1 = 13 - 2 \times 6 = 13 - 2 \times (32 - 2 \times 13) = -2 \times 32 + 5 \times 13 = -2 \times 32 + 5 \times (45 - 1 \times 32)$$
$$= 5 \times 45 - 7 \times 32 = 5 \times 45 - 7 \times (212 - 4 \times 45) = -7 \times 212 + 33 \times 45$$
On a $1 = -7 \times 212 + 33 \times 45$, on multiplie cette égalité par 3 : $3 = -21 \times 212 + 99 \times 45$
On soustrait cette égalité à $212x + 45y = 3$, on trouve
$$(-21 - x) \times 212 + (99 - y) \times 45 = 0 \Leftrightarrow 45(99 - y) = 212(21 + x)$$
D'après le théorème de Gauss, comme 45 et 212 sont premiers entre eux et que 45 divise $212(21 + x)$, 45 divise $21 + x$, il existe $k \in \mathbb{Z}$ tel que $21 + x = 45k \Leftrightarrow x = -21 + 45k$, on remplace cette égalité dans $45(99 - y) = 212(21 + x)$, on trouve alors que :
$$45(99 - y) = 212 \times 45k \Leftrightarrow 99 - y = 212k \Leftrightarrow y = -212k + 99$$
L'ensemble des solutions est $S = \{(-21 + 45k, 99 - 212k)\}$
3. $42 = 3 \times 14$ et $45 = 3 \times 15$ donc le $(42,45) = 3$ or 4 n'est pas un multiple de 3, donc il n'y a pas de solution.
4.
$$7 = 1 \times 5 + 2$$
$$5 = 2 \times 2 + 1$$
$$2 = 2 \times 1 + 0$$

Donc $1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 1 \times 5) = -2 \times 7 + 3 \times 5$

On multiplie cette égalité par 3 : $-6 \times 7 + 9 \times 5 = 3$. On soustrayant $7x + 5y = 3$ et $-6 \times 7 + 9 \times 5 = 3$ on trouve que : $7(x + 6) + 5(y - 9) = 0$, ce qui équivaut à $7(x + 6) = -5(y - 9)$, d'après le théorème de Gauss, 7 divise $5(y - 9)$ et $7 \wedge 5 = 1$ donc 7 divise $y - 9$, il existe donc $k \in \mathbb{Z}$ tel que : $y - 9 = 7k$, ce que je remplace dans $7(x + 6) = -5(y - 9)$ ce qui donne $7(x + 6) = -5 \times 7k$, puis en simplifiant par 7 : $x + 6 = -5k$.

L'ensemble des solutions est $\mathcal{S} = \{(-6 - 5k, 9 + 7k), k \in \mathbb{Z}\}$

Allez à : Exercice 18 :

Correction exercice 19 :

1.
$$100^{100} = (2^2 \times 5^2)^{100} = 2^{200} \times 5^{200}$$
Les diviseurs positifs de 1000000 sont de la forme $2^k 5^l$ avec $k \in \{0,1, \dots ,200\}$ et $l \in \{0,1, \dots ,200\}$, il y a donc $201 \times 201 = (200 + 1)^2 = 4000 + 400 + 1 = 40401$ diviseurs positifs.

2. $101 = 3 \times 33 + 2$ donc $101 \equiv 2\ [3]$
$$101^{101} \equiv 2^{101}\ [3] \equiv (-1)^{101}\ [3] \equiv -1\ [3] \equiv 2\ [3]$$
$0 \leq 2 < 3$, donc le reste de la division euclidienne de 101^{101} par 3 est 2.

$101 = 4 \times 25 + 1$ donc $101 \equiv 1\ [5]$
$$101^{101} \equiv 1^{101}\ [5] \equiv 1\ [5]$$
$0 \leq 1 < 5$, donc le reste de la division euclidienne de 101^{101} par 5 est 1.

Première méthode

On pose $N = 101^{101}$, $N \equiv 2\ [3]$ et $N \equiv 1\ [5]$ donc il existe $k, l \in \mathbb{Z}$ tels que $N = 2 + 3k$ et $N = 1 + 5l$

On trouve alors que
$$2 + 3k = 1 + 5l \Leftrightarrow 1 = 5l - 3k$$
Dont une solution particulière est $1 = 5(-1) - 3(-2)$

En faisant la différence on trouve que
$$0 = 5(l + 1) - 3(k + 2) \Leftrightarrow 5(l + 1) = 3(k + 2)$$
Comme 5 divise $3(k + 2)$ et que 5 est premier avec 3, le théorème de Gauss permet d'affirmer que 5 divise $k + 2$, il existe donc $u \in \mathbb{Z}$ tels que $k + 2 = 5u \Leftrightarrow k = -2 + 5u$ (on peut chercher les valeurs que prends l mais cela ne sert à rien ici), ce que l'on remplace dans $N = 2 + 3k = 2 + 3(-2 + 5u) = -4 + 15u$

Attention -4 n'est pas le reste recherché, comme $N \equiv -4\ [15] \equiv 11\ [15]$ le reste de la division de N par 15 est 11 car $0 \leq 11 < 15$.

Deuxième méthode en utilisant le théorème des restes chinois
$$\begin{cases} N = 101^{101} \equiv 2\ [3] \\ N = 101^{101} \equiv 1\ [5] \end{cases}$$
$$M = 3 \times 5 = 15$$
$a_1 = 2, m_1 = 3$ $M_1 = \frac{15}{3} = 5$, $5y_1 \equiv 1\ [3]$ admet une solution évidente $y_1 = 2$

$a_2 = 1, m_1 = 5$ $M_2 = \frac{15}{5} = 3$, $3y_2 \equiv 1\ [5]$ admet une solution évidente $y_2 = 2$

D'après le théorème il existe une unique solution
$$N \equiv a_1 M_1 y_1 + a_2 M_2 y_2\ \ [M] \equiv 2 \times 5 \times 2 + 1 \times 3 \times 2\ \ [15] \equiv 26\ \ [15] \equiv 11\ \ [15]$$
$0 \leq 11 < 15$ donc 11 est le reste de la division de 101^{101} par 15.

3. $\left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right) = \left(n^{\frac{p-1}{2}}\right)^2 - 1 = n^{p-1} - 1 \equiv 0\ [p]$

D'après le petit théorème de Fermat car p est premier et que n n'est pas un multiple de p. Donc p divise $\left(n^{\frac{p-1}{2}} - 1\right)\left(n^{\frac{p-1}{2}} + 1\right)$.

Si $n^{\frac{p-1}{2}} - 1$ est un multiple de p c'est fini, p divise $n^{\frac{p-1}{2}} - 1$.

Sinon $n^{\frac{p-1}{2}}-1$ et p sont premiers entre eux et comme p divise $\left(n^{\frac{p-1}{2}}-1\right)\left(n^{\frac{p-1}{2}}+1\right)$, le théorème de Gauss permet d'affirmer que p divise $n^{\frac{p-1}{2}}+1$.

Cela montre que p divise l'un des entiers $n^{\frac{p-1}{2}}-1$ et $n^{\frac{p-1}{2}}+1$

Allez à : Exercice 19 :

Correction exercice 20 :

$$N=(2^3\times 3^2)^{10}\times(2\times 3^4)^{50}=2^{3\times 10+50}\times 3^{2\times 10+4\times 50}=2^{80}\times 3^{220}$$

Les diviseurs de N sont de la forme

$$2^k\times 3^l$$

Avec $k\in\{0,1,\dots,80\}$ et $l\in\{0,1,\dots,220\}$

Il y a donc $81\times 211=17901$ diviseurs

Allez à : Exercice 20 :

Correction exercice 21 :

Soit n un entier qui vérifie ces conditions :

$$n\equiv 7\quad[8]\equiv -1\quad[8]$$
$$n\equiv 14\quad[15]\equiv -1\quad[15]$$
$$n\equiv 17\quad[18]\equiv -1\quad[18]$$
$$n\equiv 23\quad[24]\equiv -1\quad[24]$$

Il existe $k_1\in\mathbb{N}$, $k_2\in\mathbb{N}$, $k_3\in\mathbb{N}$ et $k_4\in\mathbb{N}$ tels que :

$$n=-1+8k_1$$
$$n=-1+15k_2$$
$$n=-1+18k_3$$
$$n=-1+24k_4$$

On en déduit que : $8k_1=15k_2=18k_3=24k_4\quad(1)$

$$8k_1=15k_2$$

8 est premier avec 15 et 8 divise $15k_2$, d'après le théorème de Gauss, 8 divise k_2, il existe $u\in\mathbb{N}$ tel que $k_2=8u$, ce que l'on remplace dans $8k_1=15k_2$ et obtient que $k_1=15u$, la réciproque étant trivial.

On remplace dans (1) : $15\times 8u=18k_3=24k_4\quad(1')$

Ce que l'on divise par 6 : $20u=3k_3=4k_4\quad(2)$

$$20u=3k_3$$

J'abrège un peu, 3 et 20 sont premiers entre eux et d'après le théorème de Gauss il existe $v\in\mathbb{N}$ tel que : $u=3v$ et $k_3=20v$, cela entraine en particulier que $k_1=15\times 3v=45v$ et $k_2=8\times 3v=24v$.

On remplace dans (2) : $20\times 3v=4k_4\quad(2')$

Ce que l'on divise par 4 : $15v=k_4$

On remplace k_1, k_2, k_3 et k_4 dans les expressions de n :

$$n=-1+8k_1=-1+8\times 45v=-1+360v$$
$$n=-1+15k_2=-1+15\times 24v=-1+360v$$
$$n=-1+18k_3=-1+18\times 20v=-1+360v$$
$$n=-1+24k_4=-1+24\times 15v=-1+360v$$

Le plus petit entier naturel qui vérifie les conditions ci-dessus est 359.

Allez à : Exercice 21 :

Correction exercice 22 :

Soit n le nombre d'étudiants recherché.

Il existe $k_1\in\mathbb{N}$, $k_2\in\mathbb{N}$ et $k_3\in\mathbb{N}$ tels que :

$$n=9+18k_1$$
$$n=9+20k_2$$
$$n=9+24k_3$$

On en déduit que :

$$18k_1=20k_2=24k_3$$

Ce que l'on divise par 2 :

$$9k_1 = 10k_2 = 12k_3 \quad (1)$$

$9k_1 = 10k_2$, comme 9 et 10 sont premiers entre eux et que 9 divise $10k_2$, le théorème de Gauss permet d'affirmer que 9 divise k_2, il existe donc $u \in \mathbb{N}$ tel que $k_2 = 9u$, ce que l'on remplace dans $9k_1 = 10k_2$ pour trouver $k_1 = 10u$, la réciproque étant évidente.

On remplace dans (1) : $90u = 12k_3$, ce que l'on divise par 6 : $15u = 2k_3$. 15 est premier avec 2 et 15 divise $2k_3$, le théorème de Gauss permet d'affirmer que 15 divise k_3, il existe $v \in \mathbb{N}$ tel que $k_3 = 15v$, ce que l'on remplace dans $90u = 12k_3$, d'où l'on déduit que $90u = 12 \times 15v$ entraine que $u = 2v$, la réciproque est toujours aussi évidente. Puis on remplace $u = 2v$ dans $k_1 = 10u = 20v$, $k_2 = 9u = 18v$, on remple k_1, k_2 et k_3 dans

$$n = 9 + 18k_1$$
$$n = 9 + 20k_2$$
$$n = 9 + 24k_3$$

Et on trouve à chaque fois $n = 9 + 360v$, la réciproque est évidente, il reste à trouver v tel que

$$500 < 9 + 360v < 1000$$

Ce qui équivaut à :

$$491 < 360v < 991$$

Il est à peu près clair que $v = 2$ (on rappelle que v est un entier)

Le nombre d'étudiants inscrits est $n = 9 + 2 \times 360 = 729$.

Dans cet exercice on ne s'intéresse pas au nombre d'étudiants présents sous peine de faire fonctionner son système lacrymal.

Allez à : Exercice 22 :

Correction exercice 23 :

1. D'après l'énoncé

$$a = (b-a)q_1 + r_1, \quad 0 \le r_1 < b - a$$
$$b = (b-a)q_2 + r_2 \quad 0 \le r_2 < b - a \Rightarrow -(b-a) < -r_2 \le 0$$

En faisant la différence entre ces deux équations :

$$b - a = \big((b-a)q_2 + r_2\big) - \big((b-a)q_1 + r_1\big) = (b-a)(q_2 - q_1) + r_2 - r_1$$
$$\Leftrightarrow (b-a)\big(1 - (q_2 - q_1)\big) = r_2 - r_1$$

Donc $b - a$ divise $r_2 - r_1$, comme : $-(b-a) < r_2 - r_1 < b - a$ en additionnant les inégalités

$$0 \le r_1 < b - a \quad \text{et} \quad -(b-a) < -r_2 \le 0$$

Le seul multiple de $b - a$ strictement compris entre $-(b-a)$ et $b - a$ est 0, par conséquent $r_2 - r_1 = 0$, ce que l'on remplace dans

$$(b-a)\big(1 - (q_2 - q_1)\big) = r_2 - r_1$$

Pour en déduire que $1 - (q_2 - q_1) = 0$, finalement

$$r_1 = r_2 \quad et \quad q_2 = q_1 + 1$$

2. On pose

$$ba^n - 1 = q_n a^{n+1} + r_n \quad avec \quad 0 \le r_n < a^{n+1}$$

D'après l'énoncé $b - 1 = qa + r \;\; avec \;\; 0 \le r < a$ donc pour $n = 0$, $q_0 = q$ et $r_0 = r$

Pour $n = 1$:

$$ba - 1 = q_1 a^2 + r_1$$

On va chercher q_1 et r_1.

$$b - 1 = qa + r \Leftrightarrow b = qa + r + 1$$
$$ba - 1 = (qa + r + 1)a - 1 = qa^2 + (r+1)a - 1 = qa^2 + ra + a - 1$$
$$r < a \Leftrightarrow r \le a - 1 \Leftrightarrow ra + a - 1 \le (a-1)a + a - 1 = a^2 - 1 \Rightarrow ra + a - 1 < a^2$$

Et $ra + a - 1 \ge a - 1 \ge 0$, cela montre que $r_1 = ra + a - 1$ est le reste de la division euclidienne de $ba - 1$ par a^2 car $0 \le ra + a - 1 < a^2$, en même temps on a montré que $q_1 = q$.

Pour un n quelconque :

En fait ce que l'on a fait ci-dessus ne va servir à rien, c'était juste pour voir ce qu'il se passait.

$$ba^n - 1 = (qa + r + 1)a^n - 1 = qa^{n+1} + (r+1)a^n - 1 = qa^{n+1} + ra^n + a^n - 1$$
$$r < a \Leftrightarrow r \le a - 1 \Leftrightarrow ra^n + a^n - 1 \le (a-1)a^n + a^n - 1 = a^{n+1} - 1 \Rightarrow ra^n + a^n - 1 < a^{n+1}$$

Et

$$ra^n + a^n - 1 \geq a^n - 1 \geq 0$$

Donc $r_n = ra^n + a^n - 1$ est le bon reste, et $q_n = q$.

3. d divise a et b donc d divise $A = 15a + 4b$, de même d divise $B = 11a + 3b$, par conséquent d divise $PGCD(A, B)$.

$$\begin{matrix} L_1 \\ L_2 \end{matrix} \begin{cases} A = 15a + 4b \\ B = 11a + 3b \end{cases} \Leftrightarrow \begin{matrix} L_1 \\ 3L_1 - 4L_2 \end{matrix} \begin{cases} A = 15a + 4b \\ 3A - 4B = a \end{cases} \Leftrightarrow \begin{cases} A = 15(3A - 4B) + 4b \\ a = 3A - 4B \end{cases}$$

$$\Leftrightarrow \begin{cases} -44A + 60B = 4b \\ a = 3A - 4B \end{cases} \Leftrightarrow \begin{cases} b = -11A + 15B \\ a = 3A - 4B \end{cases}$$

$D = PGCD(A, B)$ divise A et B donc D divise $a = 3A - 4B$ et $b = -11A + 15B$.

Ce qui implique $PGCD(A, B)$ divise d.

$PGCD(A, B)$ divise d et d divise $PGCD(A, B)$, puisque que ces entiers sont positifs, entraine que :

$$d = PGCD(A, B)$$

4. Soient $d = PGCD(a, b)$ et $D = PGCD\big(a + b, PPCM(a, b)\big)$.

d divise a et d divse b donc d divise $a + b$, $PPCM(a, b)$ est un multiple de a et de b donc d divise $PPCM(a, b)$, par conséquent d divise $PGCD\big(a + b, PPCM(a, b)\big)$.

d est le pgcd de a et b alors il existe a' et b' deux entiers premiers entre eux tels que $a = da'$ et $b = kb'$, d'autre part $PPCM(a, b) = \frac{ab}{d}$.

Rappel :

Soient a' et b' deux entiers premiers entre eux, la somme $a' + b'$ et le produit $a'b'$ sont premiers entre eux. Il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que :

$$u(a' + b') + va'b' = 1$$

En multipliant cette égalité par d, on trouve que :

$$ud(a' + b') + vda'b' = d \Rightarrow u(da' + db') + v\frac{da'db'}{d} = d \Rightarrow u(a + b) + v\frac{ab}{d} = d$$

$$\Rightarrow u(a + b) + vPPCM(a, b) = d$$

Donc D divise d, or on a vu plus haut que d divise D, ces deux nombres étant positifs ils sont égaux.

5. D'après Bézout Il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que :

$$ua + vb = 1$$

Ce que l'on élève au carré

$$u^2a^2 + 2uavb + v^2b^2 = 1 \Leftrightarrow a(ua + 2uvb) + v^2b^2 = 1$$

Cette dernière identité montre que a et b^2 sont premiers entre eux.

Supposons que a et b^m sont premiers entre eux. D'après Bézout Il existe $u' \in \mathbb{Z}$ et $v' \in \mathbb{Z}$ tel que :

$$u'a + v'b^n = 1$$

Ce que l'on multiplie par $ua + vb = 1$

$$(ua + vb)(u'a + v'b^n) = 1 \times 1 \Leftrightarrow uu'a^2 + uav'b^n + vbu'a + vv'b^{n+1} = 1$$

$$\Leftrightarrow a(uu'a + uv'b^n + u'vb) + vv'b^{n+1} = 1$$

Ce qui montre que a et b^{n+1} sont premiers entre eux.

Il reste à dire que l'on a fait une démonstration par récurrence pour en déduire que :

$\forall n \in \mathbb{N}$, a et b^n sont premiers entre eux.

On réutilise la démonstration ci-dessus en changeant a en b^n, b en a et n en m pour en déduire que :

$\forall m \in \mathbb{N}$, b^m et a^n sont premiers entre eux.

6. Il existe $a' \in \mathbb{N}$ et $b' \in \mathbb{N}$ tels que $a = da'$ et $b = db'$ où a' et b' sont premiers entre eux.

Donc $a^n = d^n a'^n$ et $b^n = d^n b'^n$, comme a'^n et b'^n sont premiers entre eux d'après la question précédente, d^n est le $PGCD$ de a^n et b^n.

Allez à : Exercice 23 :

Correction exercice 24 :

1. On pose $d = PGCD(a, b)$. Il existe $a' \in \mathbb{Z}$ et $b' \in \mathbb{Z}$ tels que $a = da'$ et $b = db'$ où a' et b' sont premiers entre eux.

Si $c > 0$, $ac = (dc)a'$ et $bc = (dc)b'$, comme a' et b' sont premiers entre eux,

$$PGCD(ac, bc) = dc = |c|d$$

Si $c < 0$, $ac = \big(d(-c)\big)(-a')$ et $bc = \big(d(-c)\big)(-b')$, comme a' et b' sont premiers entre eux,

$$PGCD(ac, bc) = d(-c) = |c|d$$

Remarque : le $PGCD$ de deux entiers relatifs est un entier positif.

2. D'après Bézout Il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tel que :
$$ua + vb = 1$$
Comme c divise a, il existe $k \in \mathbb{Z}$ tel que : $a = kc$, ce que l'on remplace dans l'égalité ci-dessus.
$$ukc + vb = 1$$
Cela montre que c et b sont premiers entre eux.
3. Si $PGCD(a, bc) = 1$ alors d'après Bézout il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que :
$$ua + vbc = 1$$
Donc
$$ua + (vb)c = 1$$
C'est une identité de Bézout.
Ce qui montre que a et c sont premier entre eux, autrement dit $PGCD(a, c) = 1$.
De même
$$ua + (vc)b = 1$$
Ce qui montre que a et b sont premier entre eux, autrement dit $PGCD(a, b) = 1$.
On a montré l'implication de gauche à droite.

Réciproquement
Si $PGCD(a, b) = PGCD(a, c) = 1$.
il existe $u \in \mathbb{Z}$, $v \in \mathbb{Z}$, $u' \in \mathbb{Z}$ et $v' \in \mathbb{Z}$ tels que :
$$ua + vb = 1 \quad et \quad u'a + v'c = 1$$
On multiplie ces deux égalités
$$(ua + vb)(u'a + v'c) = 1 \times 1 \Leftrightarrow uu'a^2 + uv'ac + vu'ba + vv'bc = 1$$
$$\Leftrightarrow a(uu'a + uv'c + vu'b) + (vv')bc = 1$$
C'est une identité de Bézout.
Ce qui montre que a et bc sont premiers entre eux, autrement dit $PGCD(a, bc) = 1$.
4. Montrer que si $PGCD(b, c) = 1$ alors $PGCD(a, bc) = PGCD(a, b) \times PGCD(a, c)$.
On pose $d = PGCD(a, bc)$, $d_1 = PGCD(a, b)$ et $d_2 = PGCD(a, c)$
Ecrivons les identités de Bézout suivantes :
Il existe des entiers u, v, u' et v' tels que :
$$ua + vb = d_1 \quad et \quad u'a + v'c = d_2$$
En faisant le produit de deux identités
$$(ua + vb)(u'a + v'c) = d_1 d_2 \Leftrightarrow uu'a^2 + uv'ac + vu'ba + vv'bc = d_1 d_2$$
$$\Leftrightarrow a(uu'a + uv'c + vu'b) + (vv')bc = d_1 d_2$$
C'est une identité de Bézout entre a et bc cela montre que d divise $d_1 d_2$.
Comme a et bc sont premiers entre eux il existe u et v deux entiers tels que :
$$ua + vbc = d$$
Donc
$$ua + (vb)c = d$$
C'est une identité de Bézout donc d_2 divise d.
De même d_1 divise d.
Attention on ne peut pas en déduire que $d_1 d_2$ divise d, et puis il y a une hypothèse que nous n'avons pas utilisé, c'est le fait que b et c sont premiers entre eux.
Evidemment d_1 divise b et d_2 divise c donc il existe k et k', des entiers, tels que :
$$b = kd_1 \quad et \quad c = k'd_2$$
Ecrivons une identité de Bézout entre b et c, il existe $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$ tels que :
$$ub + vc = 1 \Rightarrow ukd_1 + vk'd_2 = 1 \Rightarrow (uk)d_1 + (vk')d_2 = 1$$
D'où l'on déduit que d_1 et d_2 sont premiers entre eux.
On a déjà montré le résultat suivant :
Si d_1 divise d et d_2 divise d avec d_1 et d_2 premiers entre eux alors $d_1 d_2$ divise d mais nous allons recommencer.
Il existe $\alpha \in \mathbb{Z}$ et $\beta \in \mathbb{Z}$ tels que $d = \alpha d_1 = \beta d_2$, comme d_1 et d_2 sont premier entre eux, le théorème de Gauss entraine que d_1 divise β, il existe donc $\gamma \in \mathbb{Z}$ tel que $\beta = \gamma d_1$, ce que l'on remplace dans $d = \beta d_2 = \gamma d_1 d_2$, ce qui montre bien que $d_1 d_2$ divise d.
d divise $d_1 d_2$ et $d_1 d_2$ divise d, ces deux nombres étant positifs, on en déduit que :
$$d = d_1 d_2 \Leftrightarrow PGCD(a, bc) = PGCD(a, b) \times PGCD(a, c)$$

Allez à : Exercice 24 :

Correction exercice 25 :

1. Nous allons utiliser les congruences modulo $n^a - 1$.
   Il existe $k \in \mathbb{N}^*$ tel que $b = ka$, alors
   $$n^b - 1 = n^{ka} - 1 = (n^a)^k - 1 \equiv 1^k - 1 \quad [n^a - 1] \equiv 0 \quad [n^a - 1]$$
   Ce qui montre que $n^b - 1$ est divise par $n^a - 1$.
   (En effet il existe $K \in \mathbb{Z}$ tel que $n^b - 1 = 0 + K(n^a - 1)$).
2. D'après la division euclidienne de b par a, il existe un unique couple $(q, r) \in \mathbb{N} \times \{0,1,2, \dots, a - 1\}$ tel que : $b = aq + r$.
   Comme ci-dessus nous allons utiliser les congruences modulo $n^a - 1$.
   $$n^b - 1 = n^{aq+r} - 1 = (n^a)^q n^r - 1 \equiv 1^q n^r - 1 \quad [n^a - 1] \equiv n^r - 1 \quad [n^a - 1]$$
   il existe $k \in \mathbb{Z}$ tel que $n^b - 1 = n^r - 1 + k(n^a - 1)$.

Attention :

On ne peut pas encore conclure que $n^r - 1$ est le « bon » reste, il faut vérifier que celui-ci est compris entre 0 et $(n^a - 1) - 1$.
$$n^r > 0 \Rightarrow n^r \geq 1 \Rightarrow n^r - 1 \geq 0$$
$$r < a \Rightarrow n^r < n^a \Rightarrow n^r - 1 < n^a - 1$$
C'est bon le reste de la division euclidienne de $n^b - 1$ par $n^a - 1$ est $n^r - 1$.

3. On va utiliser l'algorithme d'Euclide
   $$b = aq_1 + r_1 \quad 0 \leq r_1 < a$$
   $$a = r_1 q_2 + r_2 \quad 0 \leq r_2 < r_1$$
   $$r_1 = r_2 q_3 + r_3 \quad 0 \leq r_3 < r_2$$
   Jusqu'à
   $$r_{n-2} = r_{n-1} q_n + r_n \quad 0 \leq r_n < r_{n-1}$$
   $$r_{n-1} = r_n q_{n+1}$$
   On rappelle que le dernier reste non nul est $d = PGCD(b, a) = r_n$.
   D'après la question précédente il existe $Q_1, Q_2, \dots, Q_{n+1}$ tels que :
   $$n^b - 1 = (n^a - 1)Q_1 + n^{r_1} - 1 \quad 0 \leq n^{r_1} - 1 < n^a - 1$$
   $$n^a - 1 = (n^{r_1} - 1)Q_2 + n^{r_2} - 1 \quad 0 \leq n^{r_2} - 1 < n^{r_1} - 1$$
   $$n^{r_1} - 1 = (n^{r_2} - 1)Q_3 + n^{r_3} - 1 \quad 0 \leq n^{r_3} - 1 < n^{r_2} - 1$$
   Jusqu'à
   $$n^{r_{n-2}} - 1 = (n^{r_{n-1}} - 1)Q_n + n^{r_n} - 1 \quad 0 \leq n^{r_n} - 1 < n^{r_{n-1}} - 1$$
   $$n^{r_{n-1}} - 1 = (n^{r_{n-1}} - 1)Q_{n+1}$$
   On rappelle que le dernier reste non nul est $PGCD\left(n^b - 1, n^a - 1\right) = n^{r_n} - 1 = n^d - 1$.

Allez à : Exercice 25 :

Correction exercice 26 :

1.
   $$5a - 2b = 5(2n + 3) - 2(5n - 2) = 19$$
   Il s'agit d'une identité de Bézout, donc $PGCD(a, b)$ divise 19, 19 étant premier, $PGCD(a, b)$ vaut 1 ou 19 selon les valeurs de n. Il faut préciser ce premier résultat.
   Cherchons une condition nécessaire et suffisante pour que $PGCD(a, b) = 19$.
   Il existe alors $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$, k et k' premiers entre eux (cela ne servira à rien) tels que :
   $$2n + 3 = 19k \qquad et \qquad 5n - 2 = 19k'$$
   Ce qui entraine que
   $$(5n - 2) - 2(2n + 3) = 19k' - 2 \times 19k = 19(k' - 2k) \Leftrightarrow n - 8 = 19(k' - 2k)$$
   Cette combinaison linéaire est faite de façon à trouver n (plus une constante) dans l'expression de gauche.
   Il existe $k'' \in \mathbb{Z}$ tel que $n = 8 + 19k'' \Leftrightarrow n \equiv 8 \quad [19]$

Réciproque :

si $n = 8 + 19k''$ alors
$$a = 2(8 + 19k'') + 3 = 19 + 2 \times 19k'' = 19(1 + 2k'')$$

$$b = 5(8 + 19k'') - 2 = 38 + 5 \times 19k'' = 19(2 + 5k'')$$

Comme

$$-2(2 + 5k'') + 5(1 + 2k'') = 1$$

C'est une identité de Bézout qui montre que $2 + 5k''$ et $1 + 2k''$ sont premiers entre eux et que donc

$$PGCD(a, b) = 19$$

Conclusion :

$$n \equiv 8 \quad [19] \Leftrightarrow PGCD(a, b) = 19$$

Sinon

$$PGCD(a, b) = 1$$

2. On pose $a = 2n - 1$ et $b = 9n + 4$.
Pour éliminer les « n », on calcule :

$$9a - 2b = 9(2n - 1) - 2(9n + 4) = -17$$

Il s'agit d'une identité de Bézout, donc $PGCD(a, b)$ divise 17, 17 étant premier, $PGCD(a, b)$ vaut 1 ou 17 selon les valeurs de n. Il faut préciser ce premier résultat.
Cherchons une condition nécessaire et suffisante pour que $PGCD(a, b) = 17$.
Il existe alors $k \in \mathbb{Z}$ et $k' \in \mathbb{Z}$, k et k' premiers entre eux (cela ne servira à rien) tels que :

$$2n - 1 = 17k \qquad et \qquad 9n + 4 = 17k'$$

Ce qui entraine que

$$-4(2n - 1) + (9n + 4) = 4 \times 17k + 17k' \Leftrightarrow n + 8 = 17(4k + k')$$

Cette combinaison linéaire est faite de façon à trouver n (plus une constante) dans l'expression de gauche.
Il existe $k'' \in \mathbb{Z}$ tel que : $n = -8 + 17k'' \Leftrightarrow n \equiv -8 \quad [17] \equiv 9 \ [17]$

Réciproque

Si $n = -8 + 17k''$ alors

$$a = 2(-8 + 17k'') - 1 = -17 + 2 \times 17k'' = 17(-1 + 2k'')$$
$$b = 9(-8 + 17k'') + 4 = -68 + 9 \times 17k'' = 17(-4 + 9k'')$$

Comme

$$-9(-1 + 2k'') + 2(-4 + 9k'') = 1$$

C'est une identité de Bézout qui montre que $-1 + 2k''$ et $-4 + 9k''$ sont premiers entre eux et que donc

$$PGCD(a, b) = 17$$

Conclusion

$$n \equiv -8 \ \ [17] \Leftrightarrow PGCD(a, b) = 17$$

Sinon

$$PGCD(a, b) = 1$$

Allez à : Exercice 26 :

Correction exercice 27 :

1. $5a - 2b = 5(2n + 1) - 2(5n + 1) = 3$
2. d divise 3, donc $d = 1$ ou $d = 3$.
3. Si $n \equiv 1 \quad [3]$, $a = 2n + 1 \equiv 3 \quad [3] \equiv 0 \ \ [3]$ donc 3 divise a et $b = 5n + 1 \equiv 6 \quad [3] \equiv 0 \ \ [3]$ donc 3 divise b. 3 est un diviseur commun à a et à b, donc $d \geq 3$, dans ce cas $d = 3$.
Si $n \equiv 0 \quad [3]$ alors $a = 2n + 1 \equiv 1 \quad [3] \not\equiv 0 \ \ [3]$ donc 3 ne divise pas a, 3 n'est pas un diviseur commun à a et à b, donc $d = 1$.
Si $n \equiv 2 \quad [3]$ alors $a = 2n + 1 \equiv 5 \quad [3] \equiv 2 \quad [3] \not\equiv 0 \ \ [3]$ donc 3 ne divise pas a, 3 n'est pas un diviseur commun à a et à b, donc $d = 1$.

Allez à : Exercice 27 :

Correction exercice 28 :

$$2 \times (3n + 1) - 3 \times 2n = 2$$

Le $PGCD(3n + 1, 2n)$ divise 2, donc il vaut 1 ou 2.

Regardons pour quelles valeurs de n ce $PGCD$ vaut 2. Dans ce cas il existe a et b des entiers premiers entre eux tels que $3n+1=2a$ et $2n=2b$, la deuxième conditions entraine que $n=b$, ce que l'on remplace dans $3n+1=2a \Leftrightarrow 2a-3b=1$, une solution particulière de cette équation est $a=-1$ et $b=-1$.

On a

$$\begin{cases} 2a-3b=1 \\ 2\times(-1)+3=1 \end{cases}$$

En soustrayant la seconde ligne à la première

$$2(a+1)-3(b+1)=0 \Leftrightarrow 2(a+1)=3(b+1) \quad (*)$$

2 est premier avec 3 et 2 divise $3(b+1)$, d'après le théorème de Gauss, 2 divise $b+1$, il existe donc $k\in\mathbb{Z}$ tel que $b+1=2k \Leftrightarrow b=-1+2k$, ce que l'on remplace dans $(*)$,

$$2(a+1)=3\times 2k \Leftrightarrow a=-1+3k$$

Puis on remplace l'une ou l'autre des valeurs de a ou de b dans $3n+1=2a$ ou dans $n=b$ pour trouver que

$$n=-1+2k$$

On peut toujours faire une réciproque

$$2\times(3n+1)-3\times 2n=2(3(-1+2k)+1)-6(-1+2k)=2(-3+6k+1)+6-12k=2$$

Cela marche

Conclusion si $n=-1+2k$ (autrement dit si n est impair) $PGCD(3n+1,2n)=2$

Sinon $PGCD(3n+1,2n)=1$

Allez à : Exercice 28 :

Correction exercice 29 :

1.

$$5(14n+3)-14(5n+1)=1$$

Est une identité de Bézout, 1 divise le PGCD de $14n+3$ et de $5n+1$ donc leur PGCD vaut 1, ils sont premiers entre eux.

2.

2.1. $87=14\times 6+3$ et $31=5\times 6+1$ d'après la première question, ils sont premiers entre eux.

2.2. D'après la première question

$$5(14\times 6+3)-14(5\times 6+1)=1 \Leftrightarrow 5\times 87+(-14)\times 31=1 \quad (1)$$

Donc $(u,v)=(5,-14)$ convient.

Il suffit de multiplier (1) par 2.

$$10\times 87+(-28)\times 31=2$$

2.3.

$$\begin{matrix} L_1 \\ L_2 \end{matrix}\begin{cases} 87x+31y=2 \\ 10\times 87+(-28)\times 31=2 \end{cases}$$

$$L_1-L_2:\ 87(x-10)+31(y+28)=0$$

$$87(x-10)=31(-y-28) \quad (2)$$

87 et 31 sont premier entre eux et 87 divise $31(-y-28)$ donc 87 divise $-y-28$, il existe $k\in\mathbb{Z}$ tel que :

$$-y-28=87k \quad (3) \Leftrightarrow y=-87k-28$$

On remplace (3) dans (2)

$$87(x-10)=31\times 87k \Leftrightarrow x-10=31k \Leftrightarrow x=10+31k$$

La réciproque est évidente et l'ensemble des solutions est :

$$\{(10+31k,-28-87k),k\in\mathbb{Z}\}$$

Allez à : Exercice 29 :

Correction exercice 30 :

1.

$$1^2 = 1 \equiv 1 \ \ [8]$$
$$3^2 = 9 \equiv 1 \ \ [8]$$
$$5^2 = 25 \equiv 1 \ \ [8]$$
$$7^2 = 49 \equiv 1 \ \ [8]$$

$0 \leq 1 < 8$ donc le reste de la division euclidienne du carré d'un nombre impair par 8 est 1.

2. $n = 2m, m \in \mathbb{N}^*$

$$x^n + y^n = (x^2)^m + (y^2)^m \equiv 1^m + 1^m \ \ [8] \equiv 2 \ [8]$$
$$z^n = (z^2)^m \equiv 1^m \ \ [8] \equiv 1 \ \ [8]$$

Donc l'équation n'a pas de solution.

Allez à : Exercice 30 :

Correction exercice 31 :

D'après le petit théorème de Fermat $5^6 \equiv 1 \ \ [7]$ car 7 est premier et 5 est premier avec 7.

$$1000 = 166 \times 6 + 4$$

Donc

$$5^{1000} = 5^{6\times 166+4} = (5^6)^{166} \times 5^4 \equiv 1^{166} \times 5^4 \ \ [7] \equiv 5^2 \times 5^2 \ \ [7] \equiv 25 \times 25 \ \ [7] \equiv 4 \times 4 \ \ [7]$$
$$\equiv 16 \ \ [7] \equiv 2 \ \ [7]$$

Comme $0 \leq 2 < 7$, 2 est le reste de la division euclidienne de 5^{1000} par 7.

Allez à : Exercice 31 :

Correction exercice 32 :

$$3^{n+3} - 4^{4n+2} = 3^3 \times 3^n - 4^2 \times (4^4)^n = 27 \times 3^n - 16 \times (16 \times 16)^n \equiv 5 \times 3^n - 5 \times (5 \times 5)^n \ \ [11]$$
$$\equiv 5 \times 3^n - 5 \times 25^n \ \ [11] \equiv 5 \times 3^n - 5 \times 3^n \ \ [11] \equiv 0 \ \ [11]$$

Donc $3^{n+3} - 4^{4n+2}$ est un multiple de 11.

Allez à : Exercice 32 :

Correction exercice 33 :

$$4^n = (3+1)^n = \sum_{k=0}^{n} C_n^k 3^k = C_n^0 + 3C_n^1 + 3^2 C_n^2 + \cdots + 3^n C_n^n = 1 + 3n + 3^2(C_n^2 + \cdots + 3^{n-2} C_n^n)$$
$$= 1 + 3n + 9k$$

Donc 4^n est congru à $1 + 3n$ modulo 9.

$$2^{2n} + 15n - 1 = (2^2)^n + 15n - 1 = 4^n + 15n - 1 \equiv 1 + 3n + 15n - 1 \ \ [9] \equiv 18n \ \ [9] \equiv 0 \ \ [0]$$

Donc $2^{2n} + 15n - 1$ est divisible par 9.

Allez à : Exercice 33 :

Correction exercice 34 :

1. $a_0 = 4^2 - 1 = 16 - 1 = 15$ est un multiple de 15.

On appelle $(H_n) : n \geq 0, a_n = 4^{2n+2} - 1$ est un multiple de 15.

$a_0 = 4^2 - 1 = 16 - 1 = 15$ est un multiple de 15. Donc (H_0) est vraie.

Si a_n est un multiple de 15, il existe $k_n \in \mathbb{N}$ tel que : $a_n = 4^{2n+2} - 1 = 15k_n$ alors

$$a_{n+1} = 4^{2(n+1)+2} - 1 = 4^{2n+2} \times 4^2 - 1 = 16 \times 4^{2n+2} - 1 = 16(15k_n + 1) - 1 = 16 \times 15k_n + 15$$
$$= 15(16k_n + 1)$$

Donc a_{n+1} est un multiple de 15.

Donc (H_n) entraine (H_{n+1}).

Pour tout $n \geq 0$, $a_n = 4^{2n+2} - 1$ est un multiple de 15.

2.
$$b_{n+1}-b_n=4^{2(n+1)+2}-15(n+1)-16-[4^{2n+2}-15n-16]$$
$$=4^{2n+4}-15n-15-4^{2n+2}+15n+16=4^{2n+2}(4^2-1)-15=15\times 4^{2n+2}-15$$
$$=15(4^{2n+2}-1)$$
Or il existe k_n tel que $a_n=4^{2n+2}-1=15k_n$ donc $b_{n+1}-b_n=15\times 15k_n=225k_n$

On en déduit que $b_{n+1}-b_n$ est un multiple de 225.

3. On pose (H_n) pour tout $n\geq 0$, b_n est un multiple de 225

$b_0=4^{2\times 0+2}-15\times 0-16=4^2-16=0$ est un multiple de 225, en effet $0=0\times 225$, (H_0) est vraie.

S'il existe $k'_n\in\mathbb{N}$ tel que $b_n=225k'_n$ alors $b_{n+1}-225k'_n=225k_n$ donc $b_{n+1}=225(k_n+k'_n)$, ce qui signifie que b_{n+1} est un multiple de 225.

Donc (H_n) entraine (H_{n+1})

Pour tout $n\geq 0$, $b_n=4^{2n+2}-15n-16$ est un multiple de 225.

Allez à : Exercice 34 :

Correction exercice 35 :

$$5^{n+2}+3^{n+1}5^{2n}=5^2\times 5^n+3\times 3^n\times (5^2)^n=25\times 5^n+3\times 3^n\times 25^n\ \ [7]$$
$$\equiv 4\times 5^n+3\times 3^n\times 4^n\ \ [7]\equiv 4\times 5^n+3\times 12^n\ \ [7]\equiv 4\times 5^n+3\times 5^n\ \ [7]$$
$$\equiv 7\times 5^n\ \ [7]\equiv 0\ \ [7]$$
Donc pour tout $n\in\mathbb{N}$, $5^{n+2}+3^{n+1}5^{2n}$ est divisible par 7.

Allez à : Exercice 35 :

Correction exercice 36 :

1.

a) $9^k\equiv 1^k\ \ [8]\equiv 1\ \ [8]$, comme $0\leq 1<8$, le reste de la division euclidienne de 9^k par 8 est 1.

b) $3^{2k}+1\equiv 9^k+1\ \ [8]\equiv 2\ \ [8]$, de même le reste de la division euclidienne de $3^{2k}+1$ par 8 est 2.
$3^{2k+1}+1=3\times 9^k+1\equiv 3\times 1+1\ \ [8]\equiv 4\ \ [8]$, le reste est alors 4.

2. Si $n=2k$
$$2^m-3^n=1\Rightarrow 2^m-3^{2k}\equiv 1\ \ [8]\Rightarrow 2^m-(3^2)^k\equiv 1\ \ [8]\Rightarrow 2^m-(9)^k\equiv 1\ \ [8]\Rightarrow 2^m-(1)^k\equiv 1\ \ [8]$$
$$\Rightarrow 2^m\equiv 2\ \ [8]\Rightarrow 2^m=2+8l$$
avec $l\in\mathbb{N}$ donc $2^{m-1}=1+4l$ or si $m\geq 2$, 2^{m-1} est paire et $1+4l$ est impaire, on en déduit que si $n=2k$ alors $m<2$,

Si $n=2k+1$
$$2^m-3^n=1\Rightarrow 2^m-3^{2k+1}\equiv 1\ \ [8]\Rightarrow 2^m-3\times(3^2)^k\equiv 1\ \ [8]\Rightarrow 2^m-3\times (9)^k\equiv 1\ \ [8]$$
$$\Rightarrow 2^m-3\times(1)^k\equiv 1\ \ [8]\Rightarrow 2^m\equiv 4\ \ [8]\Rightarrow 2^m=4+8l\Rightarrow 2^{m-2}=1+2l$$
avec $l\in\mathbb{N}$ donc $2^{m-2}=1+2l$ or si $m\geq 3$, 2^{m-2} est paire et $1+2l$ est impaire, on en déduit que si $n=2k+1$ alors $m<3$.

Que n soit pair ou impair $m\leq 2$

3. Il n'y a que trois cas possibles $m=0$, $m=1$ et $m=2$.

Si $m=0$ alors $2^m-3^n=1\Leftrightarrow 1-3^n=1\Leftrightarrow 3^n=0$ ce qui est impossible.

Si $m=1$ alors $2^m-3^n=1\Leftrightarrow 2-3^n=1\Leftrightarrow 3^n=1\Leftrightarrow n=0$

Si $m=2$ alors $2^m-3^n=1\Leftrightarrow 4-3^n=1\Leftrightarrow 3^n=3\Leftrightarrow n=1$

L'ensemble des solutions est :
$$S=\{(1,0),(2,1)\}$$

Allez à : Exercice 36 :

Correction exercice 37 :

Comme 3 est premier, $a^3 \equiv a \quad [3]$ et $b^3 \equiv b \quad [3]$,

$$a^3 - b^3 \equiv 0 \quad [3] \Leftrightarrow a - b \equiv 0 \quad [3]$$

Allez à : Exercice 37 :

Correction exercice 38 :

7 divise $a^2 + b^2 \Leftrightarrow a^2 + b^2 \equiv 0 \quad [7]$

n	0	1	2	3	4	5	6
n^2	0	1	4	2	2	4	1

La seule solution pour que la somme de deux des nombres (au carré) de la seconde ligne soit congru à 0 modulo 7 est que ces nombres (au carré) soit congru à 0 modulo 7, donc que ces nombres soit congrus à 0 modulo 7.

On a montré que si 7 divise $a^2 + b^2$ alors 7 divise a et b.

Réciproquement si 7 divise a et b alors 7 divise a^2 et b^2 donc $a^2 + b^2$.

Autre solution

Avec le petit théorème de Fermat, comme 7 est premier, pour $a \not\equiv 0 \quad [7]$, $a^6 \equiv 1 \quad [7]$ et pour $b \not\equiv 0 \quad [7]$, $b^6 \equiv 1 \quad [7]$.

Si $a \not\equiv 0 \quad [7]$ et $b \not\equiv 0 \quad [7]$,

$$(a^2 + b^2)^3 = a^6 + 3a^4b^2 + 3a^2b^4 + b^6 \equiv 1 + 3a^2b^2(a^2 + b^2) + 1 \ [7] \equiv 2 + 3a^2b^2(a^2 + b^2) \ [7]$$

Supposons que $a^2 + b^2 \equiv 0 \quad [7]$, l'égalité ci-dessus donne $0 \equiv 2 \quad [7]$, ce qui est faux donc

$$a^2 + b^2 \not\equiv 0 \quad [7]$$

La contraposée de Si $a \not\equiv 0 \quad [7]$ et $b \not\equiv 0 \quad [7]$ alors $a^2 + b^2 \not\equiv 0 \quad [7]$ est :

$a^2 + b^2 \equiv 0 \quad [7]$ entraine $a \equiv 0 \quad [7]$ et $b \equiv 0 \quad [7]$.

La réciproque est évidente.

Allez à : Exercice 38 :

Correction exercice 39 :

$$7 = 1 \times 5 + 2$$
$$5 = 2 \times 2 + 1$$
$$2 = 2 \times 1 + 0$$

Donc $1 = 5 - 2 \times 2 = 5 - 2 \times (7 - 1 \times 5) = -2 \times 7 + 3 \times 5$

On multiplie cette égalité par 3 : $-6 \times 7 + 9 \times 5 = 3$. On soustrayant $7x + 5y = 3$ et $-6 \times 7 + 9 \times 5 = 3$ on trouve que : $7(x + 6) + 5(y - 9) = 0$, ce qui équivaut à $7(x + 6) = -5(y - 9)$, d'après le théorème de Gauss, 7 divise $5(y - 9)$ et $7 \wedge 5 = 1$ donc 7 divise $y - 9$, il existe donc $k \in \mathbb{Z}$ tel que :

$y - 9 = 7k$, ce que je remplace dans $7(x + 6) = -5(y - 9)$ ce qui donne $7(x + 6) = -5 \times 7k$, puis en simplifiant par 7 : $x + 6 = -5k$.

L'ensemble des solution est $\mathcal{S} = \{(-6 - 5k, 9 + 7k), k \in \mathbb{Z}\}$

Allez à : Exercice 39 :

Correction exercice 40 :

$$12x \equiv 5 \ [35] \Leftrightarrow \exists k \in \mathbb{Z}, 12x = 5 + 35k \Leftrightarrow \exists k \in \mathbb{Z}, 12x - 35k = 5$$

$35 = 2 \times 12 + 11$, $12 = 1 \times 11 + 1$ et $11 = 1 \times 11 + 0$

Donc $1 = 12 - 1 \times 11 = 12 - 1 \times (35 - 2 \times 11) = -1 \times 35 + 3 \times 12$

Donc $3 \times 12 \equiv 1 \quad [35]$

$$12x \equiv 5 \ [35] \Rightarrow 3 \times 12x \equiv 3 \times 5 \ [35] \Rightarrow x \equiv 15 \ [35]$$

Réciproque $12 \times 15 = 180 = 5 \times 35 + 5 \equiv 5 \quad [35]$

L'ensemble des solutions est $\mathcal{S} = \{15 + 35k, k \in \mathbb{Z}\}$

Allez à : Exercice 40 :

Correction exercice 41 :

1. On voit que $13 \times 2 - 5 \times 5 = 1$, en multipliant par 3 on trouve que
$$13 \times 6 - 5 \times 15 = 3$$
donc $(6, -15)$ est une solution particulière.
2.
$$\begin{matrix} L_1 \\ L_2 \end{matrix} \begin{cases} 13u + 5v = 1 \\ 13 \times 6 - 5 \times 15 = 1 \end{cases}$$
$L_1 - L_2$ donne $13(u-6) + 5(v+15) = 0$
Ce qui équivaut à
$$13(u-6) = -5(v+15)$$
13 divise $-5(v+15)$ et 13 est premier avec 5, d'après le théorème de Gauss, 13 divise $-(v+15)$, il existe donc $k \in \mathbb{Z}$ tel que
$$-(v+15) = 13k \Leftrightarrow v = -15 - 13k$$
On remplace $-(v+15) = 13k$ dans $13(u-6) = -5(v+15)$, on obtient
$$13(u-6) = 5 \times 13k \Leftrightarrow u = 6 + 5k$$
La réciproque est évidente, donc l'ensemble des couples (u, v) vérifiant $13u + 5v = 3$ est
$$\{(6+5k, -15-13k), k \in \mathbb{Z}\}$$
3. Comme 5 premier, d'après le théorème de Fermat
$$2^4 \equiv 1\ [5]$$
La division euclidienne de 2013 par 4 est $2013 = 4 \times 503 + 1$, donc
$$2^{2013} = 2^{4 \times 503 + 1} = (2^4)^{503} \times 2 \equiv 1^{503} \times 2\ [5] \equiv 2\ [5]$$
$0 \leq 2 < 5$ donc 2 est le reste de la division euclidienne de 2^{2013} par 5
Comme 13 premier, d'après le théorème de Fermat
$$2^{12} \equiv 1\ [13]$$
La division euclidienne de 2013 par 12 est $2013 = 12 \times 167 + 9$, donc
$$2^{2013} = 2^{12 \times 167 + 9} = (2^{12})^{167} \times 2^9 \equiv 1^{167} \times 2^9\ [13] \equiv 2^4 \times 2^4 \times 2\ [13] \equiv 16 \times 16 \times 2\ [13]$$
$$\equiv 3 \times 3 \times 2\ [13] \equiv 18\ [13] \equiv 5\ [13]$$
$0 \leq 5 < 13$ donc 5 est le reste de la division euclidienne de 2^{2013} par 13
4. D'après la question 3, il existe a et b des entiers tels que
$$2^{2013} = 5a + 2 \quad \text{et} \quad 2^{2013} = 13b + 5$$
En faisant la soustraction de la seconde égalité et de la première, on trouve que
$$0 = 13b - 5a + 3 \Leftrightarrow -13b + 5a = 3$$
D'après la question 2 les solutions de $13u + 5v = 3$ sont
$$\{(6+5k, -15-13k), k \in \mathbb{Z}\}$$
On pose $a = v$ et $b = -u$ donc
$$a = -15 - 13k \quad \text{et} \quad b = -6 - 5k$$
Ce que l'on remplace dans
$$2^{2013} = 5a + 2 \quad \text{ou} \quad 2^{2013} = 13b + 5$$
$$2^{2013} = 5(-15 - 13k) + 2 = -73 - 65k$$
On cherche le reste de la division de 2^{2013} par 65, donc ce reste r, vérifie $0 \leq r < 65$, on doit prendre $k = -2$, donc
$$r = -73 + 2 \times 65 = 57$$

Allez à : Exercice 41 :

Correction exercice 42 :

(1) a.
$222 = 2 \times 3 \times 37$ donc 7 et 222 sont premiers entre eux, 7 est premier, on peut appliquer le petit théorème de Fermat
$$222^6 \equiv 1\ \ [7]$$
Puis on divise 333 par 6
$$333 = 6 \times 55 + 3$$
Par conséquent
$$222^{333} = 222^{6 \times 55 + 3} = (222^6)^{55} \times 222^3 \equiv 1^{55} \times 222^3\ [7] \equiv 222^3\ [7]$$

On divise 222 par 7

$$222 = 7 \times 31 + 5$$

$$222^{333} \equiv 222^3\ [7] \equiv (7 \times 31 + 5)^3\ \ [7] \equiv 5^3\ \ [7] \equiv 25 \times 5\ \ [7] \equiv 4 \times 5\ \ [7] \equiv 6\ \ [7]$$

Comme $0 \leq 6 < 7$, 6 est le reste de la division euclidienne de 222^{333} par 7.

$222 = 2 \times 3 \times 37$ donc 11 et 222 sont premiers entre eux, 11 est premier, on peut appliquer le petit théorème de Fermat

$$222^{10} \equiv 1\ \ [11]$$

Puis on divise 333 par 10

$$333 = 10 \times 33 + 3$$

Par conséquent

$$222^{333} = 222^{10\times 33+3} = (222^{10})^{33} \times 222^3 \equiv 1^{33} \times 222^3\ [7] \equiv 222^3\ [7]$$

On divise 222 par 11

$$222 = 11 \times 20 + 2$$

$$222^{333} \equiv 222^3\ [11] \equiv (11 \times 20 + 2)^3\ \ [11] \equiv 2^3\ \ [11] \equiv 8\ \ [11]$$

Comme $0 \leq 8 < 11$, 8 est le reste de la division euclidienne de 222^{333} par 11.

b. Il y a une solution évidente $7 \times (-3) + 11 \times 2 = 1$

c.

$$N \equiv 6\ \ [7]$$

$$N \equiv 8\ \ [11]$$

$$7 \times (-3) + 11 \times 2 = 1 \Rightarrow 11 \times 2 = 1 + 3 \times 7$$

D'après le théorème des restes chinois il existe un unique x modulo $77 = 7 \times 11$ tel que $N \equiv x\ \ [77]$

$$x = 8 - 2 \times 11 \times 2 = 8 - 2 \times (1 + 3 \times 7) = -36 \equiv 41\ [77]$$

Vérifie

$$x = 8 - 4 \times 11 \equiv 8\ \ [11] \qquad \text{et} \qquad x = 6 - 6 \times 7 \equiv 6\ \ [7]$$

41 est la solution car $0 \leq 41 < 77$.

Autre méthode

$$N = 6 + 7k \quad \text{et} \quad N = 8 + 11l$$

Donc

$$6 + 7k = 8 + 11l \Rightarrow 7k - 11l = 2$$

Or

$$7 \times (-3) + 11 \times 2 = 1 \Rightarrow 7 \times (-6) + 11 \times 4 = 2$$

En soustrayant ces deux égalités

$$7(k + 6) - 11(l + 4) = 0 \Rightarrow 7(k + 6) = 11(l + 4)$$

Comme 7 divise $11(l + 4)$ et que 7 et 11 sont premiers entre eux, le théorème de Gauss permet d'affirmer que 7 divise $l + 4$, il existe $n \in \mathbb{Z}$ tel que $l + 4 = 7n \Rightarrow l = -4 + 7l$, ce que l'on remplace dans $N = 8 + 11l = 8 + 11(-4 + 7l) = -36 + 77l = 41 + 77(l - 1)$

41 est la solution car $0 \leq 41 < 77$.

(2) On appelle N le nombre de livres de Toto, d'après l'énoncé

$$N \equiv 7\ \ [20] \qquad \text{et} \qquad N \equiv 7\ \ \ [25]$$

Il existe $k, l \in \mathbb{N}$ tels que $N = 7 + 20k$ et $N = 7 + 25l$ donc $20k = 25l$, on simplifie par 5, par conséquent $4k = 5l$, 4 et 5 sont premiers entre eux, 4 divise $5l$, d'après le théorème de Gauss, 4 divise l, il existe $u \in \mathbb{N}$ tel que $l = 4u$. On en déduit que $N = 7 + 25 \times 4u$, $u = 0$ n'est pas solution car $N < 10$, $u = 1$ est la solution $N = 7 + 100 = 107$

Allez à : Exercice 42 :

Correction exercice 43 :

1.

$$99 = 1 \times 56 + 43$$
$$56 = 1 \times 43 + 13$$
$$43 = 3 \times 13 + 4$$
$$13 = 3 \times 4 + 1$$
$$1 = 13 - 3 \times 4 = 13 - 3 \times (43 - 3 \times 13) = -3 \times 43 + 10 \times 13$$
$$= -3 \times 43 + 10 \times (56 - 1 \times 43) = 10 \times 56 - 13 \times 43$$
$$= 10 \times 56 - 13 \times (99 - 1 \times 56) = -13 \times 99 + 23 \times 56$$
$$1 = -13 \times 99 + 23 \times 56$$

2.

$$\begin{cases} x \equiv 2 \quad [56] \\ x \equiv 3 \quad [99] \end{cases} \Leftrightarrow \exists k, l \in \mathbb{Z}, \begin{cases} x = 2 + 56k \\ x = 3 + 99l \end{cases}$$

$$2 + 56k = 3 + 99l \Leftrightarrow -99l + 56k = 1 \quad L_1$$

Or

$$-13 \times 99 + 23 \times 56 = 1 \quad L_2$$

En faisant la soustraction entre L_1 et L_2

$$99(-l + 13) + 56(k - 23) = 0 \Leftrightarrow 56(k - l) = 99(l - 13)$$

56 et 99 sont premiers entre eux et 56 divise $99(l - 13)$, d'après le théorème de Gauss 56 divise $l - 13$, il existe donc $a \in \mathbb{Z}$ tel que $l - 13 = 56a \Leftrightarrow l = 13 + 56a$, ce que l'on remplace dans $x = 3 + 99l$

$$x = 3 + 99(13 + 56k) = 3 + 99 \times 13 + 99 \times 56k = 1290 + +5544k$$

Allez à : Exercice 43 :

Correction exercice 44 :

On cherche une solution particulière de $13a + 11b = 1$, ce qui est possible puisque $11 \wedge 13 = 1$

$13 = 1 \times 11 + 2$, $11 = 5 \times 2 + 1$ et $2 = 2 \times 1 + 0$

Donc $1 = 11 - 5 \times 2 = 11 - 5 \times (13 - 1 \times 11) = -5 \times 13 + 6 \times 11$

Comme 11 et 13 sont premiers entre eux, on peut appliquer le théorème des restes chinois.

On pose $M = 11 \times 13 = 143$, $M_1 = 13$, $M_2 = 11$, on cherche y_1 tel que

$$M_1 y_1 \equiv 1 \ [11] \Leftrightarrow 13y_1 \equiv 1 \ [11]$$

Et y_2 tel que $M_2 y_2 \equiv 1 \ [13] \Leftrightarrow 11y_2 \equiv 1 \ [13]$, soit, en regardant l'égalité $1 = -5 \times 13 + 6 \times 11$, $y_1 = -5$ et $y_2 = 6$ conviennent. L'unique solution modulo 143 est :

$$x = 6 \times 13 \times (-5) + 3 \times 11 \times 6 \ \ [143] \equiv 6 \times (-65 + 33) \ [143] \equiv -6 \times 32 \ \ [143]$$
$$\equiv -192 \ \ [143]$$

Les solutions dans $\mathbb{Z}$ sont de la forme $x = -186 + 143k$, $k \in \mathbb{Z}$. La plus petite solution positive est :

$$x = -192 + 2 \times 143 = -192 + 286 = 94$$

Allez à : Exercice 44 :

Correction exercice 45 :

1. On cherche les solutions de $2u + 5v = 59 \quad (1)$ avec $u \in \mathbb{Z}$ et $v \in \mathbb{Z}$, comme 2 et 5 sont premier entre eux, il existe u_0 et v_0 tels que $2u_0 + 5v_0 = 1$, il existe une solution évidente $2 \times (-2) + 5 \times 1 = 1$, si ce n'est pas le cas on utilise l'algorithme d'Euclide. En multiplie par 59 : $2 \times (-118) + 5 \times 59 = 59 \quad (2)$,

En soustrayant (1) et (2) on trouve :

$$2(u+118)+5(v-59)=0 \Leftrightarrow 2(u+2)=-5(v-1)$$

2 est premier avec 5 et 2 divise $-5(v-59)$, d'après le théorème de Gauss 2 divise $-(v-59)$, donc il existe $k\in\mathbb{Z}$ tel que $-(v-59)=2k \Leftrightarrow v=-2k+59$, on remplace $-(v-59)=2k$ dans $2(u+118)=-5(v-59)$, on trouve $2(u+118)=5\times 2k \Leftrightarrow u+118=5k \Leftrightarrow u=5k-118$, la réciproque est évidente.

Les solutions de (1) sont $\begin{cases} u=5k-118 \\ v=-2k+59 \end{cases}$ avec $k\in\mathbb{Z}$.

2. Or $u\geq 0$ et $v\geq 0$,

$$\begin{cases} 5k-118\geq 0 \\ -2k+59\geq 0 \end{cases} \Leftrightarrow \begin{cases} k\geq \dfrac{118}{5}=23+\dfrac{3}{5} \\ k\leq \dfrac{59}{2}=29+\dfrac{1}{2} \end{cases} \Leftrightarrow \begin{cases} k\geq 24 \\ k\leq 29 \end{cases}$$

Chaque valeur de $k\in\{24,25,26,27,28,29\}$ donne une solution de l'équation (1) avec $u\geq 0$ et $v\geq 0$.
Soit

$$\{(2,11),(7,9),(12,7),(17,5),(22,3),(27,1)\}$$

Allez à : Exercice 45 :

Correction exercice 46 :

1.

$$\begin{cases} 7x+5y\equiv 2\ \ [8] \\ 5x+4y\equiv 16\ \ [8] \end{cases} \Leftrightarrow \begin{cases} -x+5y\equiv 2\ \ [8] \\ 5x+4y\equiv 0\ \ [8] \end{cases} \Leftrightarrow \begin{cases} x\equiv 5y-2\ \ [8] \\ 5x+4y\equiv 0\ \ [8] \end{cases} \Leftrightarrow \begin{cases} x\equiv 5y-2\ \ [8] \\ 5(5y-2)+4y\equiv 0\ \ [8] \end{cases}$$

$$\Leftrightarrow \begin{cases} x\equiv 5y-2\ \ [8] \\ 29y+4y\equiv 10\ \ [8] \end{cases} \Leftrightarrow \begin{cases} x\equiv 5y-2\ \ [8] \\ y\equiv 2\ \ [8] \end{cases} \Leftrightarrow \begin{cases} x\equiv 10-2\ \ [8] \\ y\equiv 2\ \ [8] \end{cases} \Leftrightarrow \begin{cases} x\equiv 0\ \ [8] \\ y\equiv 2\ \ [8] \end{cases}$$

$$S=\{(8k,2+8k'),k\in\mathbb{Z},k'\in\mathbb{Z}\}$$

2.

$$\begin{cases} 7x+5y\equiv 2\ \ [9] \\ 5x+4y\equiv 16\ \ [9] \end{cases} \Leftrightarrow L_1+L_2 \begin{cases} 7x+5y\equiv 2\ \ [9] \\ 12x+9y\equiv 18\ \ [9] \end{cases} \Leftrightarrow \begin{cases} 7x+5y\equiv 2\ \ [9] \\ 3x\equiv 0\ \ [9] \end{cases} \Rightarrow$$

$$\begin{cases} 2(7x+5y)\equiv 2\times 2\ \ [9] \\ 3x\equiv 0\ \ [9] \end{cases} \Rightarrow \begin{cases} 14x+10y\equiv 4\ \ [9] \\ 3x\equiv 0\ \ [9] \end{cases} \Rightarrow \begin{cases} 5x+y\equiv 4\ \ [9] \\ 3x\equiv 0\ \ [9] \end{cases} \Rightarrow \begin{cases} -x+y\equiv 4\ \ [9] \\ 3x\equiv 0\ \ [9] \end{cases} \Rightarrow$$

$$\begin{cases} y\equiv 4+x\ \ [9] \\ 3x\equiv 0\ \ [9] \end{cases}$$

On ne peut pas en déduire que $x\equiv 0\ \ [9]$, par exemple si $x\equiv 3\ \ [9]$, on a $3x\equiv 0\ \ [9]$ sans que $x\equiv 0\ \ [9]$.

$3x\equiv 0\ \ [9] \Leftrightarrow$il existe $k\in\mathbb{Z}$ tel que $3x=9k \Leftrightarrow x=3k \Leftrightarrow \begin{cases} x\equiv 0\ \ [9] \\ x\equiv 3\ \ [9] \\ x\equiv 6\ \ [9] \end{cases}$

Si $x\equiv 0\ \ [9]$ alors $y\equiv 4\ \ [9]$, si $x\equiv 3\ \ [9]$ alors $y\equiv 4+3\ \ [9]\equiv 7\ \ [9]$, si $x\equiv 6\ \ [9]$ alors $y\equiv 4+6\ \ [9]\equiv 10\ \ [9]\equiv 1\ \ [9]$.

Pour la réciproque, on remplace les trois couples de solutions modulo 9, $(0,4)$, $(3,7)$ et $(6,1)$ dans $\begin{cases} 7x+5y\equiv 2\ \ [9] \\ 5x+4y\equiv 16\ \ [9] \end{cases}$ pour constater que cela marche.

Allez à : Exercice 46 :

Correction exercice 47 :

1.

$$\begin{cases} n\equiv 1\ \ [6] \\ n\equiv 5\ \ [9] \end{cases} \Leftrightarrow \exists(u,v)\in\mathbb{Z}^2, \begin{cases} n=1+6u \\ n=5+9v \end{cases}$$

Cela entraine que $1+6u=5+9v$, ce qui équivaut à $6u-9v=4$, comme le PGCD de 6 et 9 est 3 et que 3 ne divise pas 4, il n'y a pas de solution.

2.

$$\begin{cases} n \equiv 3 \ [6] \\ n \equiv 6 \ [9] \end{cases} \Leftrightarrow \exists (u,v) \in \mathbb{Z}^2, \begin{cases} n = 3 + 6u \\ n = 6 + 9v \end{cases}$$

Cela entraine que $3 + 6u = 6 + 9v$, ce qui équivaut à $6u - 9v = 3$, soit encore $2u - 3v = 1$

Il existe une solution évidente, $u = -1$ et $v = -1$, autrement dit $2(-1) - 3(-1) = 1$

$$\begin{cases} 2u - 3v = 1 \\ 2(-1) - 3(-1) = 1 \end{cases}$$

On fait la soustraction de ces deux équations

$$2(u+1) - 3(v+1) = 0 \Leftrightarrow 2(u+1) = 3(v+1) \ \ (*)$$

2 divise $3(v+1)$ et 2 est premier avec 3 donc d'après le théorème de Gauss, 2 divise $v + 1$, par conséquent il existe $k \in \mathbb{Z}$ tel que $v + 1 = 2k$ (ou $v = -1 + 2k$), ce que l'on remplace dans $(*)$, ce qui donne $2(u+1) = 3 \times 2k$, en simplifiant par 2, $u + 1 = 3k$ (ou $u = -1 + 3k$).

La réciproque étant évidente

$$n = 3 + 6u = 3 + 6(-1 + 3k) = -3 + 18k, \qquad k \in \mathbb{Z}$$

Si on avait prit $n = 6 + 9v$, on aurait trouvé le même ensemble de solution.

Allez à : Correction exercice 47 :

Correction exercice 48 :

1. $x^2 \equiv 1 \ \ [p] \Leftrightarrow x^2 - 1 \equiv 0 \ \ [p] \Leftrightarrow (x-1)(x+1) \equiv 0 \ \ [p] \Leftrightarrow$ il existe $k \in \mathbb{Z}$ tel que :
$$(x-1)(x+1) = kp$$
Si $x - 1$ n'est pas un multiple de p, $x - 1$ est premier avec p, d'après le théorème de Gauss p divise $(x-1)(x+1) = (x-1)\big(x-(p-1)\big)$ entraine que p divise $x + 1$ autrement dit $x \equiv -1 \ \ [p]$
Sinon $x - 1$ est un multiple de p, autrement dit $x \equiv 1 \ \ [p]$
L'ensemble des solutions est :
$S = \{1 + kp, -1 + kp\}$ avec $k \in \mathbb{Z}$.
2. Soit a tel que $2 \le a \le p - 2$, a est premier avec p donc il existe b et l tels que $ab + pl = 1$, d'après Bézout, donc $ab \equiv 1 \ [p]$, en rajoutant kp, $k \in \mathbb{Z}$, à b, on peut prendre $1 \le b \le p - 1$ (les valeurs 0 et p ne sont pas possible), b ne peut pas prendre les valeurs 1 et $p - 1 \equiv -1 \ \ [p]$ car alors $ab \not\equiv \pm 1 \ \ [p]$.
D'après la question 1°) $b \ne a$ car sinon $a = 1$ ou $a = p - 1 \equiv -1 \ \ [p]$.
$$(p-1)! = 2 \times 3 \times \dots \times (p-2) \times (p-1)$$
Dans le produit $2 \times 3 \times \dots \times (p-2)$, il y a $p - 3$ termes (nombre pair) constitué de $\frac{p-3}{2}$ couples du type ab tels que $ab \equiv 1 \ \ [p]$, donc $2 \times 3 \times \dots \times (p-2) \equiv 1 \ \ [p]$, par conséquent
$$(p-1)! \equiv p - 1 \ \ [p] \equiv -1 \ \ [p]$$

Allez à : Exercice 48 :

Correction exercice 49 :

1. $(n-x)^2 = n^2 - 2nx + x^2 \equiv x^2 \ \ [n]$
2. Précisons un peu $\mathbb{Z}/n\mathbb{Z}$, si $m \in \mathbb{Z}$ d'après la division euclidienne, il existe un unique couple $(b,r) \in \mathbb{Z} \times \{0,1,\dots,n-1\}$ tel que $m = bn + r$, r est un reste donc un élément de $\mathbb{Z}/n\mathbb{Z}$.
Soit $r \in \{0,1,\dots,n-1\}$, $c(r)$ est le reste de la division de r^2 par n, donc $r^2 = bn + c(r)$ ce qui équivaut à $r^2 \equiv c(r) \ \ [n]$ et $c(r) \in \{0,1,\dots,n-1\}$.
Comme $c(1) \equiv 1^2 \ \ [n] \equiv 1 \ \ [n]$, on a $c(n-1) \equiv (n-1)^2 \ \ [n] \equiv 1^2 \ \ [n] \equiv c(1)\ [n]$
Puisque $c(n-1) \in \{0,1,\dots,n-1\}$ et $c(1) \in \{0,1,\dots,n-1\}$ et que $c(n-1) \equiv c(1)\ [n]$, on a
$$c(1) = c(n-1)$$
Et pourtant $1 \ne n - 1$, sauf si $n = 2$, mais $n \ge 3$.
Donc c n'est pas injective.
On utilise l'exercice 1, c n'est pas surjective. Sinon on refait une démonstration semblable.
3.

n	0	1	2	3	4	5	6
n^2	0	1	4	$9 \equiv 2 \ \ [7]$	$16 \equiv 2 \ \ [7]$	$25 \equiv 4 \ \ [7]$	$36 \equiv 1 \ \ [7]$

4.
$$x^2 - 6xy + 2y^2 = (x-3y)^2 - 9y^2 + 2y^2 = (x-3y)^2 + 7y^2 \equiv (x-3y)^2 \quad [7]$$

Et $7003 \equiv 3 \quad [7]$, d'après le 3°) il n'y a pas de carré qui soit congru à 3 modulo 7 donc il n'y a pas de solution.

Allez à : Exercice 49 :