Séquence XXV – Arithmétique (partie 3)

PGCD

Exercice 1

Appliquer l'algorithme d'Euclide à :

1. $a = 2916$ et $b = 792$
2. $a = 2029$ et $b = 393$

Solution de l'exercice 1 **a)** Pour $a = 2916$ et $b = 792$:

$$2916 = 792 \times 3 + 540 \quad (1)$$
$$792 = 540 \times 1 + 252 \quad (2)$$
$$540 = 252 \times 2 + 36 \quad (3)$$
$$252 = 36 \times 7 + 0 \quad (4)$$

Le dernier reste non nul est 36, donc $\text{PGCD}(2916, 792) = 36$.

b) Pour $a = 2029$ et $b = 393$:

$$2029 = 393 \times 5 + 64 \quad (5)$$
$$393 = 64 \times 6 + 9 \quad (6)$$
$$64 = 9 \times 7 + 1 \quad (7)$$
$$9 = 1 \times 9 + 0 \quad (8)$$

Le dernier reste non nul est 1, donc $\text{PGCD}(2029, 393) = 1$.

Exercice 2

Déterminer, grâce à l'algorithme d'Euclide, le PGCD des deux entiers 18 996 et 17 724.

Solution de l'exercice 2 Appliquons l'algorithme d'Euclide :

$$18996 = 17724 \times 1 + 1272 \quad (9)$$
$$17724 = 1272 \times 13 + 1188 \quad (10)$$
$$1272 = 1188 \times 1 + 84 \quad (11)$$
$$1188 = 84 \times 14 + 12 \quad (12)$$
$$84 = 12 \times 7 + 0 \quad (13)$$

Le dernier reste non nul est 12, donc $\text{PGCD}(18996, 17724) = 12$.

Exercice 3

Déterminer le PGCD de 729 et 198, ainsi que de 5103 et 1386.

Solution de l'exercice 3 **Pour 729 et 198 :**

$$729 = 198 \times 3 + 135 \quad (14)$$
$$198 = 135 \times 1 + 63 \quad (15)$$
$$135 = 63 \times 2 + 9 \quad (16)$$
$$63 = 9 \times 7 + 0 \quad (17)$$

Donc $\text{PGCD}(729, 198) = 9$.

Pour 5103 et 1386 :

$$5103 = 1386 \times 3 + 945 \quad (18)$$
$$1386 = 945 \times 1 + 441 \quad (19)$$
$$945 = 441 \times 2 + 63 \quad (20)$$
$$441 = 63 \times 7 + 0 \quad (21)$$

Donc $\text{PGCD}(5103, 1386) = 63$.

Exercice 4

Décomposer en produit de facteurs premiers les deux nombres $a = 2916$ et $b = 792$ et retrouver ainsi leur PGCD.

Solution de l'exercice 4 **Décomposition de 2916 :** $2916 = 4 \times 729 = 4 \times 27^2 = 4 \times (3^3)^2 = 4 \times 3^6 = 2^2 \times 3^6$

Décomposition de 792 : $792 = 8 \times 99 = 8 \times 9 \times 11 = 2^3 \times 3^2 \times 11$

Donc :

$$2916 = 2^2 \times 3^6 \quad (22)$$
$$792 = 2^3 \times 3^2 \times 11 \quad (23)$$

Le PGCD est le produit des facteurs premiers communs avec leur plus petit exposant : $\text{PGCD}(2916, 792) = 2^2 \times 3^2 = 4 \times 9 = 36$ et retrouver ainsi leur PGCD.

Exercice 5

Décomposer en produit de facteurs premiers les deux nombres $a = 51205$ et $b = 97405$ et retrouver ainsi leur PGCD.

Solution de l'exercice 5 **Décomposition de 51205 :** $51205 = 5 \times 10241$. On vérifie que $10241 = 101^2$, donc : $51205 = 5 \times 101^2$

Décomposition de 97405 : $97405 = 5 \times 19481 = 5 \times 139 \times 140 + 1 = 5 \times 193 \times 101$

Donc :

$$51205 = 5 \times 101^2 \quad (24)$$
$$97405 = 5 \times 101 \times 193 \quad (25)$$

Le PGCD est : $\text{PGCD}(51205, 97405) = 5 \times 101 = 505$

Exercice 6

Montrer que, pour tous entiers a et b, $ab + 1$ et $ab + a + 1$ sont toujours premiers entre eux.

Solution de l'exercice 6 Posons $u = ab + 1$ et $v = ab + a + 1 = a(b + 1) + 1$.
Calculons $v - u = (ab + a + 1) - (ab + 1) = a$.
Soit d un diviseur commun de u et v. Alors d divise u, d divise v, et donc d divise $v - u = a$.
Puisque d divise $u = ab + 1$ et d divise a, alors d divise ab. Donc d divise $ab + 1 - ab = 1$.
Par conséquent, $d = 1$, et $\text{PGCD}(ab+1, ab+a+1) = 1$.
Les nombres $ab + 1$ et $ab + a + 1$ sont toujours premiers entre eux.

Exercice 7

Est-il vrai que :

1. Si a et b sont premiers entre eux, alors a^2 et b^2 aussi ?
2. Si a et b sont premiers entre eux, alors $a + b$ et $a \times b$ aussi ?

Solution de l'exercice 7 **a)** Vrai. Si $\text{PGCD}(a, b) = 1$, alors $\text{PGCD}(a^2, b^2) = 1$.
En effet, soit d un diviseur commun de a^2 et b^2. Si p est un facteur premier de d, alors p divise a^2 et p divise b^2. Comme p est premier, si p divise a^2, alors p divise a. De même, si p divise b^2, alors p divise b. Donc p diviserait à la fois a et b, ce qui contredit $\text{PGCD}(a, b) = 1$.
b) Proposition de solution avec le théorème de Bézout (mais d'autres solutions sont possibles, cf photos sur mon téléphone)

On cherche $(\alpha, \beta) \in \mathbb{Z}^2$ tels que :

$$(a+b)\alpha + ab\beta = 1$$

On sait que $au + bv = 1$, donc $(au+bv)^2 = 1$.
Développons :

$$a^2u^2 + 2abuv + b^2v^2 = 1$$

On regroupe astucieusement. L'idée est d'isoler un facteur ab et faire apparaître $(a+b)$ ailleurs.

$$\underbrace{a^2u^2 + b^2v^2}_{\text{à transformer}} + \underbrace{2abuv}_{\text{déjà un multiple de } ab} = 1$$

Pour le premier terme,
on ajoute et retranche $ab(u^2+v^2)$:

$$\begin{aligned} a^2u^2 + b^2v^2 &= a^2u^2 + abu^2 + b^2v^2 + abv^2 - ab(u^2+v^2) \\ &= au^2(a+b) + bv^2(a+b) - ab(u^2+v^2) \\ &= (a+b)(au^2+bv^2) - ab(u^2+v^2) \end{aligned}$$

On remplace dans l'équation de départ :

$$\begin{aligned} (a+b)(au^2+bv^2) - ab(u^2+v^2) + 2abuv &= 1 \\ (a+b)(au^2+bv^2) - ab(u^2-2uv+v^2) &= 1 \end{aligned}$$

D'où l'identité :

$$\boxed{(a+b)(au^2+bv^2) - ab(u-v)^2 = 1}$$

Théorème de Bézout

Exercice 8

Déterminer deux entiers u et v tels que :

$$2029u + 393v = 1$$

On pourra utiliser un exercice précédent...

Solution de l'exercice 8 Utilisons l'algorithme d'Euclide étendu. De l'exercice 1, nous avons :

$$2029 = 393 \times 5 + 64 \quad (26)$$
$$393 = 64 \times 6 + 9 \quad (27)$$
$$64 = 9 \times 7 + 1 \quad (28)$$
$$9 = 1 \times 9 + 0 \quad (29)$$

Remontons les calculs :

$$\begin{aligned} 1 &= 64 - 9 \times 7 && (30)\\ &= 64 - (393 - 64 \times 6) \times 7 && (31)\\ &= 64 - 393 \times 7 + 64 \times 42 && (32)\\ &= 64 \times 43 - 393 \times 7 && (33)\\ &= (2029 - 393 \times 5) \times 43 - 393 \times 7 && (34)\\ &= 2029 \times 43 - 393 \times 215 - 393 \times 7 && (35)\\ &= 2029 \times 43 - 393 \times 222 && (36) \end{aligned}$$

Donc une solution est : $u = 43$ et $v = -222$.
Vérification : $2029\times43+393\times(-222) = 87247-87246 = 1$

Exercice 9

Montrer que pour tout entier k, les nombres $2k+1$ et $9k+4$ sont toujours premiers entre eux.

Solution de l'exercice 9 Nous allons utiliser l'identité de Bézout en trouvant des entiers u et v tels que : $u(2k+1) + v(9k+4) = 1$
Essayons de trouver une relation. Calculons : $9(2k+1) - 2(9k+4) = 18k + 9 - 18k - 8 = 1$
Donc nous avons : $9(2k+1) + (-2)(9k+4) = 1$
D'après l'identité de Bézout, ceci prouve que $\text{PGCD}(2k+1, 9k+4) = 1$ pour tout entier k.
Les nombres $2k+1$ et $9k+4$ sont donc toujours premiers entre eux.

Exercice 10

Montrer avec l'Identité de Bézout et de son corollaire que si a, b et k sont des entiers non nuls, alors :

$$\text{pgcd}(ka\,;\,kb) = |k| \times \text{pgcd}(a\,;\,b)$$

Solution de l'exercice 10 Posons $d = \text{pgcd}(a, b)$ et $\delta = \text{pgcd}(ka, kb)$.

Étape 1 : Montrons que δ divise $|k| \times d$
D'après l'identité de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tels que :

$$au + bv = d$$

En multipliant par k :

$$k(au + bv) = kd$$

$$(ka)u + (kb)v = kd$$

Donc kd est une combinaison linéaire de ka et kb. Par conséquent $\delta \mid kd$.
Comme $\delta \mid kd$ et $\delta \mid -kd$, on a nécessairement

$$\delta \mid |k|d$$

Étape 2 : Montrons que $|k| \times d$ divise δ
Par définition, $d = \text{pgcd}(a, b)$, donc $d \mid a$ et $d \mid b$.
Cela signifie qu'il existe a' et b' entiers tels que $a = d \times a'$ et $b = d \times b'$.
Donc

- $ka = k \times d \times a' = (k \times d) \times a'$
- $kb = k \times d \times b' = (k \times d) \times b'$

On en déduit que $kd \mid ka$ et $kd \mid kb$.
Donc kd est un diviseur commun de ka et kb.
Par conséquent, kd divise le pgcd de ka et kb, c'est-à-dire $kd \mid \delta$.
Comme $kd \mid \delta$ et $-kd \mid \delta$, on a nécessairement $|k|d \mid \delta$.

Conclusion
On a montré $\delta \mid |k|d$ et $|k|d \mid \delta$, donc :

$$ka \wedge kb = |k| \times (a \wedge b)$$

Exercice 11

Déterminer les entiers n compris entre 400 et 1000 vérifiant $n \wedge 5880 = 84$.

Solution de l'exercice 11 Si $\text{PGCD}(n, 5880) = 84$, alors on peut écrire $n = 84k$ et $5880 = 84 \times 70$ où $\text{PGCD}(k, 70) = 1$.
En effet, $5880 = 84 \times 70$.
Pour que $400 \leq n \leq 1000$, il faut : $400 \leq 84k \leq 1000$ $\frac{400}{84} \leq k \leq \frac{1000}{84}$ $4{,}76... \leq k \leq 11{,}90...$
Donc $k \in \{5, 6, 7, 8, 9, 10, 11\}$.
Il faut aussi $\text{PGCD}(k, 70) = 1$. Or $70 = 2 \times 5 \times 7$.
Les valeurs de k premières avec 70 sont celles qui ne sont divisibles ni par 2, ni par 5, ni par 7 : - $k = 5$: divisible par 5, donc non. - $k = 6$: divisible par 2, donc non. - $k = 7$: divisible par 7, donc non. - $k = 8$: divisible par 2, donc non. - $k = 9$: $\text{PGCD}(9, 70) = 1$, donc oui. - $k = 10$: divisible par 2 et 5, donc non. - $k = 11$: $\text{PGCD}(11, 70) = 1$, donc oui.
Les solutions sont : $n = 84 \times 9 = 756$ et $n = 84 \times 11 = 924$.

Exercice 12

1. Calculer a et b dans $\mathbb{N}^2$ tels que

$$\begin{cases} a + b = 360 \\ a \wedge b = 18 \end{cases}$$

2. Calculer a et b dans $\mathbb{Z}^2$ tels que

$$\begin{cases} a \times b = 2700 \\ a \wedge b = 6 \end{cases}$$

3. Déterminer les entiers naturels a et b vérifiant

$$\begin{cases} a^2 \times b = 2304 \\ a \wedge b = 4 \end{cases}$$

4. Déterminer les entiers naturels a et b, dont le PGCD est 9 et tels que

$$4a^2 - b^2 = 7695$$

Solution de l'exercice 12 **a)** Si $\text{PGCD}(a, b) = 18$, on peut écrire $a = 18a'$ et $b = 18b'$ avec $\text{PGCD}(a', b') = 1$.
L'équation devient : $18a' + 18b' = 360$, soit $a' + b' = 20$.
Les couples (a', b') d'entiers naturels premiers entre eux tels que $a' + b' = 20$ sont : $(1, 19)$, $(3, 17)$, $(7, 13)$, $(9, 11)$, $(11, 9)$, $(13, 7)$, $(17, 3)$, $(19, 1)$.
Les solutions sont donc : $(18, 342)$, $(54, 306)$, $(126, 234)$, $(162, 198)$, $(198, 162)$, $(234, 126)$, $(306, 54)$, $(342, 18)$.
b) Si $\text{PGCD}(a, b) = 6$, on écrit $a = 6a'$ et $b = 6b'$ avec $\text{PGCD}(a', b') = 1$.
L'équation devient : $36a'b' = 2700$, soit $a'b' = 75$.
$75 = 3 \times 5^2$. Les couples (a', b') premiers entre eux sont : $(1, 75)$, $(3, 25)$, $(5, 15)$, $(15, 5)$, $(25, 3)$, $(75, 1)$.
Les solutions sont : $(6, 450)$, $(18, 150)$, $(30, 90)$, $(90, 30)$, $(150, 18)$, $(450, 6)$.
c) Si $\text{PGCD}(a, b) = 4$, on écrit $a = 4a'$ et $b = 4b'$ avec $\text{PGCD}(a', b') = 1$.
L'équation devient : $(4a')^2 \times 4b' = 2304$, soit $64a'^2b' = 2304$, donc $a'^2b' = 36$.
$36 = 2^2 \times 3^2$. Pour que $a'^2b' = 36$ avec $\text{PGCD}(a', b') = 1$: - Si $a' = 1$, alors $b' = 36$, mais $\text{PGCD}(1, 36) = 1$ - Si $a' = 2$, alors $b' = 9$, et $\text{PGCD}(2, 9) = 1$ - Si $a' = 3$, alors $b' = 4$, et $\text{PGCD}(3, 4) = 1$ - Si $a' = 6$, alors $b' = 1$, et $\text{PGCD}(6, 1) = 1$
Les solutions sont : $(4, 144)$, $(8, 36)$, $(12, 16)$, $(24, 4)$.
d) Si $\text{PGCD}(a, b) = 9$, on écrit $a = 9a'$ et $b = 9b'$ avec $\text{PGCD}(a', b') = 1$.
L'équation devient : $4(9a')^2 - (9b')^2 = 7695$, soit $324a'^2 - 81b'^2 = 7695$. Divisant par 81 : $4a'^2 - b'^2 = 95$.
On a $(2a')^2 - b'^2 = 95$, soit $(2a' - b')(2a' + b') = 95$.
$95 = 5 \times 19$. Les décompositions possibles sont : - $2a' - b' = 1$ et $2a' + b' = 95$: $a' = 24$, $b' = 47$ - $2a' - b' = 5$ et $2a' + b' = 19$: $a' = 6$, $b' = 7$

Vérifions que $\mathrm{PGCD}(a', b') = 1$: - $\mathrm{PGCD}(24, 47) = 1$ - $\mathrm{PGCD}(6, 7) = 1$
Les solutions sont : $(216, 423)$ et $(54, 63)$.

Théorème de Gauss

Exercice 13

1. Soit $P(x) = x^2 + ax + b$, avec a et b entiers. Montrer que si r est une racine rationnelle de $P(x)$, alors r est entier.
2. En déduire que, pour tout n entier naturel, $\sqrt{n}$ est soit un entier soit un nombre irrationnel.

Solution de l'exercice 13 **a)** Supposons que $r = \frac{p}{q}$ soit une racine rationnelle de $P(x)$, avec p et q entiers, $q \neq 0$, et $\text{PGCD}(p, q) = 1$ (fraction irréductible).

Alors $P(r) = 0$, soit : $\left(\frac{p}{q}\right)^2 + a\left(\frac{p}{q}\right) + b = 0$

Multipliant par q^2 : $p^2 + apq + bq^2 = 0$

D'où : $p^2 = -q(ap + bq)$

Ceci montre que q divise p^2. Comme $\text{PGCD}(p, q) = 1$, on a aussi $\text{PGCD}(p^2, q) = 1$. Donc q divise p^2 et $\text{PGCD}(p^2, q) = 1$ implique $q = \pm 1$.

Ainsi $r = \frac{p}{\pm 1} = \pm p$ est un entier.

b) Soit n un entier naturel. Considérons l'équation $x^2 = n$, soit $x^2 - n = 0$.

C'est un polynôme de la forme $x^2 + 0 \cdot x + (-n)$ avec des coefficients entiers.

D'après la partie a), si $\sqrt{n}$ est rationnel, alors $\sqrt{n}$ est entier.

Par contraposée : si $\sqrt{n}$ n'est pas entier, alors $\sqrt{n}$ n'est pas rationnel, donc $\sqrt{n}$ est irrationnel.

Conclusion : pour tout entier naturel n, $\sqrt{n}$ est soit un entier, soit un nombre irrationnel.

Exercice 14

Déterminer les entiers naturels a et b tels que : $a + b = ab$.

Coup de pouce : On pourra cherche deux méthodes : l'une par factorisation, l'autre en se rappelant que deux entiers consécutifs sont premiers entre eux.

Solution de l'exercice 14 L'équation $a+b = ab$ peut se réécrire : $a + b - ab = 0$ $a(1 - b) + b = 0$ $a(1 - b) = -b$

Si $b = 1$, alors $a \times 0 = -1$, ce qui est impossible.

Si $b \neq 1$, alors : $a = \frac{-b}{1-b} = \frac{b}{b-1}$

Pour que a soit un entier naturel, il faut que $b-1$ divise b.

Or $b = (b - 1) + 1$, donc $b - 1$ divise b si et seulement si $b - 1$ divise 1.

Comme $b - 1$ est un entier et divise 1, on a $b - 1 \in \{-1, 1\}$.

- Si $b - 1 = -1$, alors $b = 0$. Mais on cherche b entier naturel, donc $b \geq 1$. - Si $b - 1 = 1$, alors $b = 2$, et $a = \frac{2}{2-1} = 2$.

Vérification : $a + b = 2 + 2 = 4$ et $ab = 2 \times 2 = 4$

La seule solution est $(a, b) = (2, 2)$.

Exercice 15

Est-il vrai que :

1. Si un entier naturel n est congru à 1 modulo 7, alors le PGCD de $3n + 4$ et de $4n + 3$ est égal à 7 ?
2. Il n'existe pas d'entiers relatifs x et y tels que : $3x - 24y = 14$?
3. S'il existe un couple de nombres entiers relatifs (u, v) tel que $ua + vb = 3$, alors $a \wedge b = 3$
4. Si les entiers x et y sont premiers entre eux, alors les coefficients de l'identité de Bézout correspondante sont aussi premiers entre eux.

Solution de l'exercice 15 **a)** Faux. Si $n \equiv 1\,[7]$, alors $n = 7k + 1$ pour un entier k.

$3n + 4 = 3(7k + 1) + 4 = 21k + 7 = 7(3k + 1)$

$4n + 3 = 4(7k + 1) + 3 = 28k + 7 = 7(4k + 1)$

Donc $\text{PGCD}(3n+4, 4n+3) = 7 \cdot \text{PGCD}(3k+1, 4k+1)$.

Or $\text{PGCD}(3k + 1, 4k + 1) = \text{PGCD}(3k + 1, (4k + 1) - (3k + 1)) = \text{PGCD}(3k + 1, k)$.

En général, ce PGCD n'est pas égal à 1, donc l'affirmation est fausse. **VRAI d'APRES SERGE**

b) Vrai. L'équation $3x - 24y = 14$ n'a pas de solution car $\text{PGCD}(3, 24) = 3$ et 3 ne divise pas 14.

c) Faux. Si $ua + vb = 3$, alors tout diviseur commun de a et b divise 3. Donc $\text{PGCD}(a, b)$ divise 3, mais n'est pas nécessairement égal à 3.

Contre-exemple : $a = 6$, $b = 9$, $u = -1$, $v = 1$. On a $(-1) \times 6 + 1 \times 9 = 3$, mais $\text{PGCD}(6, 9) = 3$.

En fait, dans cet exemple, c'est vrai ! Prenons plutôt : $a = 3$, $b = 6$, $u = 1$, $v = 0$. On a $1 \times 3 + 0 \times 6 = 3$, mais $\text{PGCD}(3, 6) = 3$.

L'affirmation est en fait vraie dans ce cas aussi. Reformulons : l'affirmation est vraie.

d) Faux. Contre-exemple : $x = 3$, $y = 5$ sont premiers entre eux. L'identité de Bézout donne : $2\times3+(-1)\times5 = 1$. Les coefficients sont 2 et -1, et $\text{PGCD}(2, 1) = 1$, donc ils sont premiers entre eux.

Autre exemple : $x = 6$, $y = 35$. On a $6\times6+(-1)\times35 = 1$, donc les coefficients 6 et -1 donnent $\text{PGCD}(6, 1) = 1$.

En fait, il semble que ce soit souvent vrai... Contre-exemple : $x = 21$, $y = 35$. $\text{PGCD}(21, 35) = 7 \neq 1$, donc ils ne sont pas premiers entre eux. **VRAI D'APRES SERGE**

Exercice 16

Déterminer dans $\mathbb{Z}^2$, grâce à l'algorithme d'Euclide puis le théorème de Gauss, l'ensemble des solutions entières de l'équation :

1. $39a - 45b = 6$
2. $4a - 6b = 7$

Solution de l'exercice 16 **a)** Pour $39a - 45b = 6$:
Calculons d'abord PGCD$(39, 45)$: $45 = 39 \times 1 + 6$ $39 = 6 \times 6 + 3$ $6 = 3 \times 2 + 0$
Donc PGCD$(39, 45) = 3$.
Puisque 3 divise 6, l'équation a des solutions.
Divisons l'équation par 3 : $13a - 15b = 2$.
Trouvons une solution particulière de $13a - 15b = 1$: $15 = 13 \times 1 + 2$ $13 = 2 \times 6 + 1$
Donc : $1 = 13 - 2 \times 6 = 13 - (15 - 13) \times 6 = 7 \times 13 - 6 \times 15$
Pour $13a - 15b = 2$, une solution particulière est $(a_0, b_0) = (14, 12)$.
Vérification : $13 \times 14 - 15 \times 12 = 182 - 180 = 2$
L'ensemble des solutions est : $(a, b) = (14 + 15k, 12 + 13k)$ où $k \in \mathbb{Z}$.
b) Pour $4a - 6b = 7$:
PGCD$(4, 6) = 2$. Puisque 2 ne divise pas 7, l'équation n'a pas de solution dans $\mathbb{Z}^2$.

Exercice 17

Alain vend à Béatrice 22 chaises identiques. Béatrice les paie en lui donnant 17 tables identiques, auxquelles elle ajoute 4 euros. Déterminer le prix d'une chaise et le prix d'une table, sachant que le prix d'une chaise est un nombre entier impair d'euros, inférieur à 100, et que le prix d'une table est un nombre entier d'euros, supérieur à 100.

Solution de l'exercice 17 Soit c le prix d'une chaise et t le prix d'une table.
L'équation est : $22c = 17t + 4$, soit $22c - 17t = 4$.
Calculons PGCD$(22, 17) = 1$ (car 17 est premier et ne divise pas 22).
L'équation a donc des solutions. Trouvons une solution particulière de $22c - 17t = 1$:
Par l'algorithme d'Euclide étendu : $22 = 17 \times 1 + 5$ $17 = 5 \times 3 + 2$ $5 = 2 \times 2 + 1$
Donc : $1 = 5 - 2 \times 2 = 5 - (17 - 5 \times 3) \times 2 = 7 \times 5 - 2 \times 17$ $= 7 \times (22 - 17) - 2 \times 17 = 7 \times 22 - 9 \times 17$
Pour $22c - 17t = 4$, une solution particulière est $(c_0, t_0) = (28, 36)$.
L'ensemble des solutions est : $(c, t) = (28 + 17k, 36 + 22k)$ où $k \in \mathbb{Z}$.
Conditions : - c impair et $c < 100$ - $t > 100$
Pour $c = 28 + 17k$ impair : $28 + 17k \equiv 1\,[2]$, soit $17k \equiv 1\,[2]$, donc k impair.
Pour $t = 36 + 22k > 100$: $k > \frac{64}{22} \approx 2{,}9$, donc $k \geq 3$.
Pour $c = 28 + 17k < 100$: $k < \frac{72}{17} \approx 4{,}2$, donc $k \leq 4$.
Avec k impair et $3 \leq k \leq 4$, on a $k = 3$.
Solution : $c = 28 + 17 \times 3 = 79$ euros, $t = 36 + 22 \times 3 = 102$ euros.
Vérification : $22 \times 79 = 1738$ et $17 \times 102 + 4 = 1738$

Exercice 18

Résoudre la congruence : $7x \equiv 2\,[9]$.

Solution de l'exercice 18 Nous devons résoudre $7x \equiv 2\,[9]$, c'est-à-dire trouver x tel que $7x - 9y = 2$ pour un entier y.

Calculons PGCD$(7, 9) = 1$ (car 7 est premier et ne divise pas 9).

Puisque 1 divise 2, l'équation a des solutions.

Trouvons l'inverse de 7 modulo 9. Il faut résoudre $7u \equiv 1\,[9]$.

Par l'algorithme d'Euclide étendu : $9 = 7 \times 1 + 2$ $7 = 2 \times 3 + 1$

Donc : $1 = 7 - 2 \times 3 = 7 - (9 - 7) \times 3 = 4 \times 7 - 3 \times 9$

Ainsi $7 \times 4 \equiv 1\,[9]$, donc $7^{-1} \equiv 4\,[9]$.

La solution est : $x \equiv 4 \times 2 \equiv 8\,[9]$.

L'ensemble des solutions est : $x \equiv 8\,[9]$, soit $x = 8 + 9k$ où $k \in \mathbb{Z}$.

Exercice 19

Résoudre les systèmes de congruences :

1. $\begin{cases} x \equiv 8\,[9] \\ x \equiv 4\,[5] \end{cases}$ 2. $\begin{cases} x \equiv 5\,[18] \\ x \equiv -1\,[12] \end{cases}$

Solution de l'exercice 19 $8 + 9a = 4 + 5b$, et c'est le retour de Diophante.

Exercice 20

Retrouver une date de naissance

Partie A : Introduction

Soit l'équation $(E) : 31m + 12j = N$, où N est un entier donné et m et j deux entiers relatifs.

1. (a) Déterminer la solution particulière de l'équation $31m + 12j = 1$ donnée par l'algorithme d'Euclide.
   (b) Justifier que $(7\,;-18)$ est aussi une solution particulière de $31m + 12j = 1$.
   (c) En déduire une solution particulière de l'équation $31m + 12j = N$.
2. Résoudre : $(E) : 31m + 12j = N$.
3. En déduire que si $(m_0\,;\,j_0)$ est solution de (E), alors $m_0 \equiv 7N\,[12]$ et $j_0 \equiv -18N\,[31]$.

Partie B : Application

Monsieur A affirme à Madame B : « Multipliez votre jour de naissance par 12, votre mois de naissance par 31, additionnez les deux nombres trouvés et donnez-moi le résultat N, je pourrai retrouver votre jour et votre mois de naissance ». On note m_0 le mois de naissance de M$^{\text{me}}$ B et j_0 son jour de naissance. Le problème est donc de trouver $(m_0\,;\,j_0)$ solution de (E) telle que m_0 soit un entier compris entre 1 et 12 et j_0 soit un entier compris entre 1 et 31.

1. Déduire de ce qui précède une méthode pour retrouver le mois de naissance m_0 et le jour de naissance j_0.

2. Quelle réponse donner si $m_0 \equiv 0\,[12]$? Et si $j_0 \equiv 0\,[31]$?
3. Mme B donne $N = 242$, quels sont ses jour et mois de naissance ?

Solution de l'exercice 20 Partie A :

1a) Appliquons l'algorithme d'Euclide à 31 et 12 : $31 = 12\times2+7$ $12 = 7\times1+5$ $7 = 5\times1+2$ $5 = 2\times2+1$
Remontons : $1 = 5 - 2 \times 2 = 5 - (7 - 5) \times 2 = 3 \times 5 - 2 \times 7 = 3 \times (12 - 7) - 2 \times 7 = 3 \times 12 - 5 \times 7 = 3 \times 12 - 5 \times (31 - 12 \times 2) = 13 \times 12 - 5 \times 31$
Donc : $31 \times (-5) + 12 \times 13 = 1$.
Une solution particulière est $(m, j) = (-5, 13)$.
1b) Vérifions : $31 \times 7 + 12 \times (-18) = 217 - 216 = 1$
1c) Pour $31m + 12j = N$, une solution particulière est $(7N, -18N)$.
2) L'ensemble des solutions de $31m + 12j = N$ est : $(m, j) = (7N + 12k, -18N - 31k)$ où $k \in \mathbb{Z}$.
3) Si (m_0, j_0) est solution, alors $m_0 = 7N + 12k$ et $j_0 = -18N - 31k$. Donc : $m_0 \equiv 7N\,[12]$ et $j_0 \equiv -18N\,[31]$.

Partie B :

1) Méthode : - Calculer $m_0 \equiv 7N\,[12]$ et ajuster pour que $1 \leq m_0 \leq 12$ - Calculer $j_0 \equiv -18N\,[31]$ et ajuster pour que $1 \leq j_0 \leq 31$
2) - Si $m_0 \equiv 0\,[12]$, alors $m_0 = 12$ (décembre) - Si $j_0 \equiv 0\,[31]$, alors $j_0 = 31$
3) Pour $N = 242$: $m_0 \equiv 7 \times 242 \equiv 1694 \equiv 2\,[12]$ (car $1694 = 141 \times 12 + 2$) $j_0 \equiv -18 \times 242 \equiv -4356\,[31]$
$-4356 = -141 \times 31 + 15$, donc $j_0 \equiv 15\,[31]$.
Puisque $1 \leq 2 \leq 12$ et $1 \leq 15 \leq 31$, nous avons :
Mme B est née le 15 février ($m_0 = 2$, $j_0 = 15$).
Vérification : $31 \times 2 + 12 \times 15 = 62 + 180 = 242$

PPCM

Exercice 21

La machine allemande G-Schreiber était une machine à chiffrer utilisée par l'Allemagne pendant la Seconde Guerre Mondiale. Elle était constituée (entre autres) de dix roues comprenant respectivement 47, 53, 59, 61, 64, 65, 67, 69, 71 et 73 positions. A chaque fois qu'un caractère était tapé, il était chiffré à l'aide d'un algorithme « un peu compliqué » utilisant la position des roues, puis toutes les roues tournaient d'une position. Combien fallait-il taper de caractères pour revenir à la position initiale des roues ?

Solution de l'exercice 21 Les nombres de position de chaque roue, 47, 53, 59, 61, 64, 65, 67, 69, 71 et 73, sont des nombres premiers entre eux. Avant de revenir à la position initiale, il faut que chaque roue ait fait un ou plusieurs tours complets. Ainsi, il faut que le nombre de caractères entré soit un multiple de 47, et un multiple de 53, etc... Puisque les nombres sont premiers entre eux, le plus petit nombre de caractères à entrer avant de revenir à la position initiale, qui est le plus petit multiple commun de 47, 53, 59, 61, 64, 65, 67, 69, 71 et 73, est :

$$47 \times 53 \times 59 \times 61 \times 64 \times 65 \times 67 \times 69 \times 71 \times 73$$

Ce nombre vaut 89 362 231 892 952 069.

Exercice 22

Résoudre dans $\mathbb{N}^2$ les systèmes suivants. On posera $d = x \wedge y$ et $m = x \vee y$ et on donnera la réponse sous forme d'un tableau.

a) $\begin{cases} xy = 1512 \\ x \vee y = 252 \end{cases}$ b) $\begin{cases} xy = 300 \\ x \vee y = 60 \end{cases}$

Solution de l'exercice 22 On utilise la relation fondamentale : $xy = \text{pgcd}(x, y) \times \text{ppcm}(x, y)$, c'est-à-dire $xy = d \times m$.

a) $\begin{cases} xy = 1512 \\ \text{ppcm}(x, y) = 252 \end{cases}$

D'après la relation fondamentale :

$$d = \frac{xy}{m} = \frac{1512}{252} = 6$$

Posons $x = 6x'$ et $y = 6y'$ où x' et y' sont premiers entre eux (car $d = \text{pgcd}(x, y) = 6$).
Alors :

$$xy = 36x'y' = 1512 \Rightarrow x'y' = 42$$

Et :

$$\text{ppcm}(x, y) = 6x'y' = 252 \Rightarrow x'y' = 42$$

Il faut trouver les couples (x', y') premiers entre eux tels que $x'y' = 42$.
Décomposition : $42 = 2 \times 3 \times 7$
Les couples (x', y') premiers entre eux sont :

- $(1, 42)$ donc $(x, y) = (6, 252)$
- $(2, 21)$ donc $(x, y) = (12, 126)$
- $(3, 14)$ donc $(x, y) = (18, 84)$
- $(6, 7)$ donc $(x, y) = (36, 42)$
- $(7, 6)$ donc $(x, y) = (42, 36)$
- $(14, 3)$ donc $(x, y) = (84, 18)$
- $(21, 2)$ donc $(x, y) = (126, 12)$
- $(42, 1)$ donc $(x, y) = (252, 6)$

x	y	d	m
6	252	6	252
12	126	6	252
18	84	6	252
36	42	6	252
42	36	6	252
84	18	6	252
126	12	6	252
252	6	6	252

b) $\begin{cases} xy = 300 \\ \text{ppcm}(x, y) = 60 \end{cases}$

D'après la relation fondamentale :

$$d = \frac{xy}{m} = \frac{300}{60} = 5$$

Posons $x = 5x'$ et $y = 5y'$ où x' et y' sont premiers entre eux.
Alors :

$$xy = 25x'y' = 300 \Rightarrow x'y' = 12$$

Et :

$$\text{ppcm}(x, y) = 5x'y' = 60 \Rightarrow x'y' = 12$$

Il faut trouver les couples (x', y') premiers entre eux tels que $x'y' = 12$.
Décomposition : $12 = 2^2 \times 3$
Les couples (x', y') premiers entre eux sont :

- $(1, 12)$ donc $(x, y) = (5, 60)$
- $(3, 4)$ donc $(x, y) = (15, 20)$
- $(4, 3)$ donc $(x, y) = (20, 15)$
- $(12, 1)$ donc $(x, y) = (60, 5)$

x	y	d	m
5	60	5	60
15	20	5	60
20	15	5	60
60	5	5	60

Exercice 23

Déterminer tous les couples $(a\,;\,b) \in \mathbb{N}^2$ dont le ppcm m et le pgcd d vérifient la relation :

$$8m = 105d + 30$$

Solution de l'exercice 23 On utilise la relation fondamentale : $ab = d \times m$.
De la relation $8m = 105d + 30$, on tire :

$$m = \frac{105d + 30}{8}$$

Pour que m soit un entier naturel, il faut que $105d+30 \equiv 0\,[8]$.
Or $105d + 30 \equiv d + 6\,[8]$
Donc $d + 6 \equiv 0\,[8]$, c'est-à-dire $d \equiv 2\,[8]$.
Les valeurs possibles de d sont : $d \in \{2, 10, 18, 26, 34, ...\}$
Calculons les premières valeurs :

- Si $d = 2$: $m = \frac{210+30}{8} = \frac{240}{8} = 30$
- Si $d = 10$: $m = \frac{1050+30}{8} = \frac{1080}{8} = 135$
- Si $d = 18$: $m = \frac{1890+30}{8} = \frac{1920}{8} = 240$

Pour chaque couple (d, m) vérifiant $8m = 105d + 30$, posons $a = dx'$ et $b = dy'$ où x' et y' sont premiers entre eux.
Alors $\text{ppcm}(a, b) = dx'y' = m$, donc $x'y' = \frac{m}{d}$.
Cas $d = 2$, $m = 30$:
$x'y' = \frac{30}{2} = 15 = 3 \times 5$
Couples (x', y') premiers entre eux : $(1, 15), (3, 5), (5, 3), (15, 1)$
Donc : $(a, b) \in \{(2, 30), (6, 10), (10, 6), (30, 2)\}$
Cas $d = 10$, $m = 135$:
$x'y' = \frac{135}{10} = 13.5$: pas entier, donc pas de solution.
On constate qu'il faut aussi que d divise m. De $8m = 105d + 30$, on a $8m - 105d = 30$.
Pour que d divise m, examinons : si $d|m$ alors $d|8m$ donc $d|30$.
Les diviseurs de 30 sont : $1, 2, 3, 5, 6, 10, 15, 30$.
Parmi ceux-ci, lesquels vérifient $d \equiv 2\,[8]$?
Seul $d = 2$ convient.
Donc les solutions sont :

$$\boxed{(a, b) \in \{(2, 30), (6, 10), (10, 6), (30, 2)\}}$$

Théorème de Fermat

Exercice 24

1. Montrer que, pour tout entier naturel n non nul, $n^3 - n$ est divisible par 3.
2. Soit p un nombre premier différent de 2, démontrer que $N = \sum_{k=0}^{p-2} 2^k$ est divisible par p.

Solution de l'exercice 24 1. Le corollaire du théorème de Fermat affirme : Pour tout entier naturel a et tout nombre premier p, on a : $a^p \equiv a\,[p]$
Donc $a^p - a \equiv 0\,[p]$, c'est à dire $a^p - a$ est divisible par p.
$n \in \mathbb{N}^*$ et 3 est un nombre premier, donc $n^3 - n$ est divisible par 3.
Remarques : on peut aussi justifier par une factorisation ou un raisonnement par récurrence.
2. $N = 2^0 + 2^1 + 2^2 + \ldots + 2^{p-2}$ est la somme des $(p-1)$ premiers termes de la suite géométrique de raison 2 et de premier terme $2^0 = 1$
Donc : $N = \frac{1-2^{p-1}}{1-2} = 2^{p-1} - 1$
p est un nombre premier différent de 2 donc p est premier avec 2.
On utilise le théorème de Fermat : 2^{p-1} est divisible par p
Par suite : N est divisible par p.

Exercice 25

Démontrer que, pour tout entier naturel strictement positif n, $N = n^{13} - n$ est divisible par 13, 7, 5, 3 et 2.

Solution de l'exercice 25 13 est un nombre premier, donc d'après le corollaire du théorème de Fermat : $n^{13} - n$ est divisible par 13.
$n^{13} - n = n(n^{12} - 1)$
$12 = 2^2 \times 3$
Le nombre 12 a 6 diviseurs
$D_{12} = \{1; 2; 3; 4; 6; 12\}$
$12 = 2 \times 6$
$n^{12} = (n^6)^2$
$n^{13} - n = n(n^{12} - 1) = n(n^6 - 1)(n^6 + 1) = (n^7 - 1)(n^6 + 1)$
7 est un nombre premier, donc d'après le corollaire du théorème de Fermat : $n^7 - n$ est divisible par 7.
Par suite, $n^{13} - n$ est divisible par 7.
$12 = 3 \times 4$
$n^{12} = (n^4)^3$
$n^{13} - n = n(n^{12} - 1) = n[(n^4)^3 - 1]$
On utilise le résultat de l'exercice précédent :
$(n^4)^3 - 1$ est un multiple de $n^4 - 1$. Donc il existe $K \in \mathbb{N}$ tel que : $(n^4)^3 - 1 = (n^4 - 1)K$
$n^{13} - n = n(n^{12} - 1) = n[(n^4)^3 - 1] = n(n^4 - 1)K = (n^5 - 1)K$
5 est un nombre premier, donc d'après le corollaire du théorème de Fermat : $n^5 - n$ est divisible par 5.
Par suite, $n^{13} - n$ est divisible par 5.
$12 = 2 \times 6$
$n^{12} = (n^2)^6$
$n^{13} - n = n(n^{12} - 1) = n[(n^2)^6 - 1]$
On utilise le résultat de l'exercice précédent :
$(n^2)^6 - 1$ est un multiple de $n^2 - 1$. Donc il existe $K' \in \mathbb{N}$ tel que : $(n^2)^6 - 1 = (n^2 - 1)K'$
$n^{13} - n = n(n^{12} - 1) = n(n^2 - 1)K' = (n^3 - n)K'$

3 est un nombre premier, donc d'après le corollaire du théorème de Fermat : $n^3 - n$ est divisible par 3.
Par suite, $n^{13} - n$ est divisible par 3.
$n^{13} - n = n(n^{12} - 1)$
On utilise le résultat de l'exercice précédent :
$n^{12} - 1$ est un multiple de $n - 1$. Donc il existe $K'' \in \mathbb{N}$ tel que : $n^{12} - 1 = (n - 1)K''$
$n^{13} - n = n(n^{12} - 1) = n(n - 1)K'' = (n^2 - n)K''$
2 est un nombre premier, donc d'après le corollaire du théorème de Fermat : $n^2 - n$ est divisible par 2.
Par suite, $n^{13} - n$ est divisible par 2.

Exercice 26

On se propose de montrer, grâce à un contre-exemple, que la réciproque du corollaire du théorème de Fermat est fausse.

1. Décomposer 561 en produit de facteurs premiers.
2. Démontrer que, si x est un entier alors, pour tout $n \in \mathbb{N}^*$, $a^n - 1$ est un multiple de $a - 1$
3. Démontrer que $a^{561} - a$ est divisible par 3 puis par 11, puis par 17.
4. En déduire que, pour tout entier naturel a, $a^{561} - a \equiv 0\,[561]$
5. Conclure.

Solution de l'exercice 26

1.

$$\begin{aligned} 561 &= 3 \times 187 \\ &= 3 \times 11 \times 17 \end{aligned}$$

2. $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + 1)$
   Si x est un entier alors $x^{n-1} + x^{n-2} + \ldots + 1$ est un entier et $x - 1$ est un entier.
   Conséquence : $(x^n - 1)$ est un multiple de $(x - 1)$
3. On sait que $a^{561} - a = a(a^{560} - 1)$
   On considère la décomposition de 560 en produit de facteurs premiers

$$560 = 2^4 \times 5 \times 7$$

   560 a donc $5 \times 2 \times 2 = 20$ diviseurs de 560

$$D_{560} = \{1; 2; 4; 5; 7; 8; 10; 14; 16; 20; 28; 35; 40; 56; 70; 80; 140; 280; 560\}$$

   - $560 = 2 \times 280$
     $a^{560} = (a^2)^{280}$
     On pose $x = a^2$ et $n = 280$
     $a^{560} - 1$ est un multiple de $a^2 - 1$. Donc il existe $K \in \mathbb{N}$ tel que : $a^{560} - 1 = (a^2 - 1)K$
     Par suite,

$$\begin{aligned} a^{561} - a &= a(a^{560} - 1) \\ a^{561} - a &= a(a^2 - 1)K \\ a^{561} - a &= (a^3 - a)K \end{aligned}$$

     Or $a^3 - a$ est divisible par 3
     Donc, $a^{561} - a$ est divisible par 3
   - $560 = 10 \times 56$
     $a^{560} = (a^{10})^{56}$
     On pose $x = a^{10}$ et $n = 56$
     $a^{560} - 1$ est un multiple de $a^{10} - 1$. Donc il existe $K' \in \mathbb{N}$ tel que : $a^{560} - 1 = (a^{10} - 1)K'$
     Par suite,

$$\begin{aligned} a^{561} - a &= a(a^{560} - 1) \\ a^{561} - a &= a(a^{10} - 1)K' \\ a^{561} - a &= (a^{11} - a)K' \end{aligned}$$

     Or $a^{11} - a$ est divisible par 11. Donc, $a^{561} - a$ est divisible par 11
   - $560 = 16 \times 35$
     $a^{560} = (a^{16})^{35}$
     On pose $x = a^{16}$ et $n = 35$
     $a^{560} - 1$ est un multiple de $a^{16} - 1$. Donc il existe $K'' \in \mathbb{N}$ tel que : $a^{560} - 1 = (a^{16} - 1)K''$
     Par suite,

$$\begin{aligned} a^{561} - a &= a(a^{560} - 1) \\ a^{561} - a &= a(a^{16} - 1)K'' \\ a^{561} - a &= (a^{17} - a)K'' \end{aligned}$$

     Or $a^{17} - a$ est divisible par 17
     Donc, $a^{561} - a$ est divisible par 17
4. Les nombres 3, 11 et 17 sont trois nombres premiers donc premiers entre eux 2 à 2.
   $a^{561} - a$ est divisible par 3, 11 et 17.
   Donc $a^{561} - a$ est divisible par $3 \times 11 \times 17 = 561$
   Par suite :

$$\begin{aligned} a^{561} - a &\equiv 0\,[561] \\ a^{561} &\equiv a\,[561] \end{aligned}$$

   et pourtant 561 n'est pas un nombre premier.
   Donc la réciproque du corollaire du théorème de Fermat n'est pas vraie.

Exercice 27

On suppose qu'il existe des entiers naturels non nuls m, n et a tels que : $(4m+3)(4n+3) = 4a^2+1$

1. Soit p un nombre premier quelconque divisant $4m+3$. Montrer que p est impair et que : $(2a)^{p-1} \equiv (-1)^{\frac{p-1}{2}} [p]$
2. En utilisant le théorème de Fermat, montrer que $p \equiv 1 [4]$
3. En utilisant la décomposition de $4m+3$ en facteurs premiers, obtenir une contradiction.

Solution de l'exercice 27

1. $4m \equiv 0 [2]$
$4m+3 \equiv 3 [2]$
$4m+3 \equiv 1 [2]$
$4m+3$ n'est pas divisible par 2 donc $p \neq 2$ et donc p est impair.
p est impair donc $p = 2q+1$ avec $q \in \mathbb{N}$
p est un diviseur de $4m+3$
$4m+3$ est un diviseur de $4a^2+1$
Donc p est un diviseur de $4a^2+1$
Par suite,

$$\begin{aligned} 4a^2+1 &\equiv 0 [p] \\ 4a^2 &\equiv -1 [p] \\ (2a)^2 &\equiv -1 [p] \\ (2a)^{2q} &\equiv (-1)^q [p] \end{aligned}$$

Or, $2q = p-1$
$q = \frac{p-1}{2}$
On a donc :

$$(2a)^{p-1} \equiv (-1)^{\frac{p-1}{2}} [p]$$

2. Pour pouvoir utiliser le théorème de Fermat, on doit vérifier que p et $2a$ sont premiers entre eux.
p étant un nombre premier il suffit de vérifier que p n'est pas un diviseur de $2a$.
On suppose que $2a \equiv 0 [p]$
On a alors $4a^2 \equiv 0 [p]$
et donc $4a^2+1 \equiv 1 [p]$
Or, on a vu dans la question précédente que : $4a^2+1 \equiv 0 [p]$
Donc p n'est pas un diviseur de $2a$ et p et $2a$ sont premiers entre eux.
D'après le théorème de Fermat :

$$\begin{aligned} (2a)^{p-1} - 1 &\equiv 0 [p] \\ (2a)^{p-1} &\equiv 1 [p] \end{aligned}$$

Or d'après la première question, $(2a)^{p-1} \equiv (-1)^{\frac{p-1}{2}} [p]$
On a donc : $(-1)^{\frac{p-1}{2}} \equiv 1 [p]$
Cela signifie que $\frac{p-1}{2}$ est un nombre pair.
Or $q = \frac{p-1}{2}$
Donc q est un nombre pair.
Il existe $q' \in \mathbb{N}$ tel que $q = 2q'$
$p = 2q+1$
$p = 4q'+1$
et donc $p \equiv 1 [4]$
3. $4m+3 = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m}$
$p_1, p_2, \ldots, p_m$ sont des nombres premiers distincts.
et $\alpha_1, \alpha_2, \ldots, \alpha_m$ sont des entiers naturels non nuls.
$p_1, p_2, \ldots, p_m$ sont des nombres premiers qui divisent $4m+3$
D'après la question précédente :

$$p_1 \equiv 1 [4] \quad p_2 \equiv 1 [4] \quad \ldots \quad p_m \equiv 1 [4]$$

Donc :

$$p_1^{\alpha_1} \equiv 1 [4] \quad p_2^{\alpha_2} \equiv 1 [4] \quad \ldots \quad p_m^{\alpha_m} \equiv 1 [4]$$

Par suite :

$$p_1^{\alpha_1} \times p_2^{\alpha_2} \times \ldots \times p_m^{\alpha_m} \equiv 1 [4]$$

$$4m+3 \equiv 1 [4]$$

Or,

$$\begin{aligned} 4m &\equiv 0 [4] \\ 4m+3 &\equiv 3 [4] \end{aligned}$$

Il y a contradiction, il n'existe pas des entiers naturels non nuls m, n et a tels que : $(4m+3)(4n+3) = 4a^2+1$

Exercice 28

On chercher à déterminer tous les entiers relatifs N tels que :

$$\begin{cases} N \equiv 5\,[13] \\ N \equiv 1\,[17] \end{cases}$$

1. Vérifier que 239 est solution de ce système.
2. Soit N un entier relatif solution de ce système. Démontrer que N peut s'écrire sous la forme $N = 1 + 17x = 5 + 13y$ où x et y sont deux entiers relatifs vérifiant la relation

$$17x - 13y = 4$$

3. Résoudre l'équation $17x - 13y = 4$ où x et y sont des entiers relatifs.
4. En déduire qu'il existe un entier relatif k tel que $N = 18 + 221k$.
5. Démontrer que

$$N \equiv 18\,[221] \iff \begin{cases} N \equiv 5\,[13] \\ N \equiv 1\,[17] \end{cases}$$

Remarque : Cette dernière équivalence est basée sur un théorème appelé **Théorème chinois des restes**. Voir l'article de Philippe Julien sur le sujet.

Solution de l'exercice 28

1. $239 = 18 \times 13 + 5$ donc $239 \equiv 5\,[13]$
   $239 = 14 \times 17 + 1$ donc $239 \equiv 1\,[17]$
   Donc 239 est solution du système.
2. N est un entier relatif solution du système donc :
   $N \equiv 1\,[17]$. Il existe $x \in \mathbb{Z}$ tel que $N = 1 + 17x$
   $N \equiv 5\,[13]$. Il existe $y \in \mathbb{Z}$ tel que $N = 5 + 13y$
3. $17x - 13y = 4$
   Le couple $(1; 1)$ est une solution particulière de l'équation car :

$$17 \times 1 - 13 \times 1 = 17 - 13 = 4$$

$$\begin{aligned} 17x - 13y = 4 &\Leftrightarrow 17x - 13y = 4 = 17 \times 1 - 13 \times 1 \\ &\Leftrightarrow 17(x-1) = 13 \times (y-1) \end{aligned}$$

   17 divise $13(y-1)$
   $\text{pgcd}(17; 13) = 1$
   D'après le théorème de Gauss, 17 divise $(y-1)$
   Donc il existe $k \in \mathbb{Z}$ tel que $y - 1 = 17k$
   Pour tout $k \in \mathbb{Z}$ si $y - 1 = 17k$, alors :

$$\begin{aligned} 17(x-1) = 13(y-1) &\Leftrightarrow 17(x-1) = 13 \times 17k \\ &\Leftrightarrow x - 1 = 13k \end{aligned}$$

   Conclusion :
   Pour tout $k \in \mathbb{Z}$, $y - 1 = 17k$ et $x - 1 = 13k$

$$\begin{cases} x = 13k + 1 \\ y = 17k + 1 \end{cases} \qquad k \in \mathbb{Z}$$

$$S = \{(13k + 1; 17k + 1); k \in \mathbb{Z}\}$$

4. $N = 1 + 17x = 5 + 13y$
   $17x - 13y = 4$
   D'où,

$$\begin{aligned} N &= 1 + 17x \\ &= 1 + 17(13k + 1) \\ &= 1 + 221k + 17 \\ &= 18 + 221k \end{aligned}$$

   ou

$$\begin{aligned} N &= 5 + 13y \\ &= 5 + 13(17k + 1) \\ &= 5 + 221k + 13 \\ &= 18 + 221k \end{aligned}$$

5. Si $\begin{cases} N \equiv 5\,[13] \\ N \equiv 1\,[17] \end{cases}$ alors d'après les questions précédentes, il existe $k \in \mathbb{Z}$ tel que $N = 18 + 221k$, c'est à dire $N \equiv 18\,[221]$
   Réciproquement, si $N \equiv 18\,[221]$ alors il existe $K \in \mathbb{Z}$ tel que $N = 18 + 221K$
   $N = 18 + 221K$
   $N = 18 + 13 \times 17K$
   Donc : $N \equiv 18\,[13]$
   Comme $18 \equiv 5\,[13]$
   On a donc : $N \equiv 5\,[13]$
   De même :
   $N = 18 + 221K$
   $N = 18 + 13 \times 17K$
   Donc : $N \equiv 18\,[17]$
   Comme $18 \equiv 1\,[17]$
   On a donc : $N \equiv 1\,[17]$
   Par conséquent, N est solution du système

$$\begin{cases} N \equiv 5\,[13] \\ N \equiv 1\,[17] \end{cases}$$