Question de cours.

1. En raisonnant par l'absurde, montrer que le système

$$(S) : \begin{cases} x & \equiv & 5 & [6] \\ x & \equiv & 4 & [8] \end{cases}$$

n'admet pas de solution x dans $\mathbb{Z}$.

2. (a) Enoncer le théorème de Bézout dans $\mathbb{Z}$.
   (b) Soient $a, b \in \mathbb{N}$ premiers entre eux et $c \in \mathbb{Z}$. Montrer que

$$a \mid c,\ b \mid c \quad \Longleftrightarrow \quad ab \mid c.$$

3. On considère le système d'inconnue $x \in \mathbb{Z}$

$$(S) : \begin{cases} x & \equiv & 6 & [17] \\ x & \equiv & 5 & [16] \\ x & \equiv & 4 & [15] \end{cases}$$

   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.
   (b) En déduire la résolution dans $\mathbb{Z}$ du système (S).

Réponse.

1. On suppose par l'absurde qu'il existe $x \in \mathbb{Z}$ tel que

$$x \equiv 5\ [6], \quad x \equiv 4\ [8].$$

Alors il existe $a, b \in \mathbb{Z}$ tels que

$$6a + 5 = x = 8b + 4.$$

Ainsi

$$1 = 5 - 4 = 8b - 6a.$$

Donc, d'après le théorème de Bézout, 8 et 6 sont premiers entre eux ce qui est absurde. Par conséquent il n'existe pas de solution au système (S).

2. (a) Soient $a, b \in \mathbb{Z}$. Alors

$$a \wedge b = 1 \quad \Longleftrightarrow \quad \exists u, v \in \mathbb{Z}, au + bv = 1.$$

   (b) On suppose que $a \mid c$ et $b \mid c$. Donc il existe $k, \ell \in \mathbb{Z}$ tels que

$$c = ak = b\ell.$$

Or $a \wedge b = 1$, donc, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que

$$1 = au + bv.$$

Donc, en multipliant cette égalité par c,

$$c = auc + bvc = aub\ell + bvak = ab(u\ell + vk).$$

Ainsi

$$ab \mid c.$$

Réciproquement si $ab \mid c$ alors nous avons directement

$$a \mid ab \mid c, \quad b \mid ab \mid c.$$

3. (a) On considère $x \in \mathbb{Z}$ tel que

$$x \equiv 6\ [17], \quad x \equiv 5\ [16], \quad x \equiv 4\ [15]$$

i.e. il existe $a, b, c \in \mathbb{Z}$ tels que

$$x = 17a + 6 = 16b + 5 = 15c + 4$$

i.e.

$$x = 17a + 6, \quad 1 = 6 - 5 = -17a + 16b, \quad 1 = 5 - 4 = -16b + 15c.$$

Par exemple si $a = b = c = -1$. Par conséquent

$$x_0 = -17 + 6 = -16 + 5 = -15 + 4 = -11$$

est une solution particulière de (S) dans $\mathbb{Z}$.

(b) Soit $x \in \mathbb{Z}$. Alors

$$x \equiv 6\ [17], \quad x \equiv 5\ [16], \quad x \equiv 4\ [15]$$

si et seulement si

$$x - x_0 \equiv 0\ [17], \quad x - x_0 \equiv 0\ [16], \quad x - x_0 \equiv 0\ [15]$$

si et seulement si

$$17 \mid x - x_0, \quad 16 \mid x - x_0, \quad 15 \mid x - x_0$$

si et seulement si, d'après la question 2 et car $15, 16, 17$ sont premiers entre eux dans leur ensemble,

$$15 \times 16 \times 17 \mid x - x_0.$$

Par conséquent l'ensemble des solutions de (S) est

$$\{x_0 + (15 \times 16 \times 17)k, \quad k \in \mathbb{Z}\} = x_0 + (15 \times 16 \times 17)\mathbb{Z}.$$

Exercice. Soient $n \in \mathbb{N}^*$ et, pour $p \in \mathbb{Z}$,

$$\begin{array}{rccc} \varphi_p : & \mathbb{U}_n & \longrightarrow & \mathbb{U}_n \\ & z & \longmapsto & z^p \end{array}$$

où $\mathbb{U}_n$ est l'ensemble des racines n-ièmes de l'unité. Montrer que φ_p est bijective si et seulement si $p \wedge n = 1$.

Réponse. On procède par double implications.

- On suppose que $p \wedge n = 1$. Alors, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que

$$1 = pu + nv.$$

Alors, pour tout $z \in \mathbb{U}_n$,

$$(\varphi_u \circ \varphi_p)(z) = (\varphi_p \circ \varphi_u)(z) = z^{pu} = z^{pu}(z^n)^v = z.$$

D'où φ_p est bijective et $\varphi_p^{-1} = \varphi_u$.

- Réciproquement on suppose que φ_p est bijective. Or $e^{i\frac{2\pi}{n}} \in \mathbb{U}_n$, donc il existe $z \in \mathbb{U}_n$ (unique) tel que

$$e^{i\frac{2\pi}{n}} = \varphi_p(z) = z^p.$$

Or $z \in \mathbb{U}_n$, donc il existe $k \in \{0, ..., n-1\}$ tel que

$$z = e^{i\frac{2k\pi}{n}}.$$

Ainsi

$$e^{i\frac{2\pi}{n}} = z^p = e^{i\frac{2kp\pi}{n}}.$$

Donc il existe $\ell \in \mathbb{Z}$ tel que

$$\frac{2\pi}{n} = \frac{2kp\pi}{n} + 2\ell\pi$$

i.e.

$$1 = kp + \ell n.$$

Ainsi, d'après le théorème de Bézout, $p \wedge n = 1$.

Exercice. Résoudre dans $\mathbb{Z}^2$ l'équation

$$xy = 3x + 2y.$$

Réponse. Soient $x, y \in \mathbb{Z}$. Alors

$$\begin{aligned}
xy = 3x + 2y &\iff 0 = 3x + 2y - xy = x(3-y) + 2y = x(3-y) - 2(3-y) + 6 = (x-2)(3-y) + 6 \\
&\iff (x-2)(y-3) = 6 \\
&\iff (x-2, y-3) \in \{(1,6), (2,3), (3,2), (6,1), (-1,-6), (-2,-3), (-3,-2), (-6,-1)\} \\
&\iff (x,y) \in \{(3,9), (4,7), (5,5), (8,4), (1,-3), (0,0), (-1,1), (-4,2)\}.
\end{aligned}$$

Question de cours.

1. Soit $(a, b, p) \in \mathbb{Z}^3$. Montrer que
$$p \wedge a = 1 = p \wedge b \quad \Longrightarrow \quad p \wedge (ab) = 1.$$

2. Soit p un nombre premier.

   (a) Montrer que
   $$\forall k \in \{1, ..., p-1\}, \quad p \mid \binom{p}{k} k!.$$
   En déduire que
   $$p \mid \binom{p}{k}.$$

   (b) Montrer que
   $$\forall n \in \mathbb{N}, \quad n^p \equiv n \ [p].$$

   (c) En déduire que, pour tout $n \in \mathbb{N}$, si p ne divise pas n alors $n^{p-1} \equiv 1 \ [p]$.

Réponse.

1. On suppose que
$$p \wedge a = 1 = p \wedge b.$$
Alors, d'après le théorème de Bézout, il existe $u_a, v_a, u_b, v_b \in \mathbb{Z}$ tels que
$$au_a + pv_a = 1 = bu_b + pv_b$$
i.e.
$$au_a = 1 - pv_a, \quad bu_b = 1 - pv_b.$$
Ainsi
$$au_a bu_b = (1 - pv_a)(1 - pv_b) = 1 - p(v_a + v_b - pv_a v_b)$$
i.e.
$$1 = abu_a u_b + p(v_a + v_b - pv_a v_b).$$
Donc, par théorème de Bézout,
$$p \wedge (ab) = 1.$$

2. (a) Soit $k \in \{1, ..., p-1\}$. Alors, comme $k \neq 0$,
$$\binom{p}{k} k! = \frac{p!}{(p-k)!} = p \times (p-1) \times ... \times (p-k+1) = p \prod_{j=1}^{k-1} (p-j).$$
Donc
$$p \mid \binom{p}{k} k!.$$
Or $k < p$ et p premier, donc $p \wedge k! = 1$, d'où
$$p \mid \binom{p}{k}.$$

   (b) On montre par récurrence sur $n \in \mathbb{N}$ que
   $$n^p \equiv n \ [p].$$

   - Pour $n = 0$ nous avons directement
   $$0^p = 0 \equiv 0 \ [p].$$

- On suppose que, pour $n \in \mathbb{N}$,
$$n^p \equiv 1 \ [p].$$
Alors
$$(n+1)^p = \sum_{k=0}^{p} \binom{p}{k} n^k$$
avec, d'après la question précédente,
$$\forall k \in \{1, ..., p-1\}, \quad p \mid \binom{p}{k} \mid \binom{p}{k} n^k.$$
Donc, par hypothèse de récurrence,
$$(n+1)^p \equiv 1 + n^p \ [p] \equiv 1 + n \ [p].$$
Le théorème de récurrence permet de conclure.

(c) Soit $n \in \mathbb{N}$ tel que p ne divise pas n. Or p est premier, donc $p \wedge n = 1$. Ainsi, par théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que
$$1 = pu + nv,$$
d'où
$$nv \equiv 1 \ [p].$$
De plus, d'après la question précédente,
$$n^p \equiv n \ [p].$$
Ainsi
$$n^{p-1} \equiv n^p v \ [p] \equiv nu \ [p] \equiv 1 \ [p].$$

Exercice. Résoudre dans $\mathbb{N}^2$ le système suivant
$$\begin{cases} x + y &= 100 \\ x \wedge y &= 10. \end{cases}$$

Réponse. Soient $x, y \in \mathbb{N}$ tels que
$$x + y = 100, \quad x \wedge y = 10.$$
Alors, comme $x \wedge y = 10$, nous avons
$$x = 10x', \quad y = 10y'$$
avec $x' \wedge y' = 1$. Ainsi
$$100 = x + y = 10(x' + y')$$
i.e.
$$10 = x' + y'.$$
Ainsi, comme $x' \wedge y' = 1$,
$$(x', y') \in \{(1, 9), (3, 7), (7, 3), (9, 1)\}.$$
Donc
$$(x, y) \in \{(10, 90), (30, 70), (70, 30), (90, 10)\}.$$
Réciproquement tous ces couples vérifient le système, donc il s'agit de l'ensemble des solutions.

Exercice.

1. Montrer que, pour tout $n \in \mathbb{N}$, il existe un unique couple d'entiers $(a_n, b_n) \in \mathbb{N}^2$ tel que
$$(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}.$$
2. Pour tout $n \in \mathbb{N}$, calculer $a_n^2 - 2b_n^2$ et en déduire que $a_n \wedge b_n = 1$.

Réponse.

1. Soient $n \in \mathbb{N}$ et $a_n, a'_n, b_n, b'_n \in \mathbb{N}$ tels que

$$a_n + b_n\sqrt{2} = (1+\sqrt{2})^n = a'_n + b'_n\sqrt{2}.$$

Donc, si $b_n \neq b'_n$ alors

$$\sqrt{2} = \frac{a_n - a'_n}{b'_n - b_n} \in \mathbb{Q}$$

ce qui est absurde. Donc $b_n = b'_n$ puis $a_n = a'_n$ ce qui montre l'unicité d'un tel couple. On procède ensuite par récurrence sur $n \in \mathbb{N}$ pour montrer l'existence.

- Pour $n = 0$ nous avons directement

$$(1+\sqrt{2})^0 = 1 = 1 + 0 \times \sqrt{2}.$$

Donc

$$a_0 = 1, \quad b_0 = 0.$$

- On suppose que, pour $n \in \mathbb{N}$, il existe $a_n, b_n \in \mathbb{N}$ tels que

$$(1+\sqrt{2})^n = a_n + b_n\sqrt{2}.$$

Donc

$$(1+\sqrt{2})^{n+1} = (a_n + b_n\sqrt{2})(1+\sqrt{2}) = a_n + 2b_n + (a_n + b_n)\sqrt{2}.$$

Donc

$$a_{n+1} = a_n + 2b_n, \quad b_{n+1} = a_n + b_n.$$

Le théorème de récurrence permet de conclure quant à l'existence d'un tel couple. On aurait également pu utiliser la formule du binôme de Newton sans raisonner par récurrence.

2. Soit $n \in \mathbb{N}$. Alors

$$a_n^2 - 2b_n^2 = (a_n + b_n\sqrt{2})(a_n - b_n\sqrt{2}) = (1+\sqrt{2})^n(1-\sqrt{2})^n = (-1)^n$$

où $a_n - b_n\sqrt{2} = (1-\sqrt{2})^n$ peut être montré par récurrence ou par formule du binôme de Newton. Ainsi, en multipliant cette égalité par $(-1)^n$,

$$a_n((-1)^n a_n) + b_n(2(-1)^{n+1}) = 1.$$

Donc, d'après le théorème de Bézout,

$$a_n \wedge b_n = 1.$$

Question de cours.

1. Enoncer et démontrer le lemme de Gauss.
2. Déterminer le reste de la division euclidienne de $2^6, 2^8$ et 2^{12} par 7.
3. Montrer que
$$\forall n \in \mathbb{N}, \quad 11 \mid 3^{n+3} - 4^{4n+2}.$$

Réponse.

1. Soient $a, b, c \in \mathbb{Z}$ tels que a et b soient premiers entre eux et $a \mid bc$. Alors
$$a \mid c.$$
En effet, $a \mid bc$ donc il existe $w \in \mathbb{Z}$ tel que
$$bc = aw.$$
Et, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que
$$1 = au + bv.$$
Ainsi, en multipliant cette égalité par c, nous obtenons
$$c = cau + cbv = cau + awv = a(cu + wv).$$
Ainsi $a \mid c$.
2. Nous avons $2^6 = 64$. Ainsi, par division euclidienne,
$$2^6 = 64 = 9 \times 7 + 1.$$
Ainsi le reste de la division euclidienne de 2^6 par 7 est 1. Nous pouvions aussi utiliser le fait 7 est premier et 7 ne divise pas 2, d'où
$$2^{7-1} \equiv 1 \ [7].$$
Puis
$$2^8 = 4 \times 2^6 \equiv 4 \times 1 \ [7] \equiv 4 \ [7]$$
et
$$2^{12} = (2^6)^2 \equiv 1^2 \ [7] \equiv 1 \ [7].$$
Donc le reste de la division euclidienne de 2^12 par 7 est également 1.
3. Soit $n \in \mathbb{N}$. Alors
$$3^{n+3} - 4^{4n+2} = 27 \times 3^n - 16 \times 256^n \equiv 5(3^n - 3^n) \ [11] \equiv 0 \ [11].$$
Donc
$$11 \mid 3^{n+2} - 4^{4n+2}.$$

Exercice. Soient $a, b \in \mathbb{Z}$. Montrer que
$$(a + b) \wedge (ab) = 1 \quad \iff \quad a \wedge b = 1.$$

Réponse. On procède par double implications.

- On suppose que $(a + b) \wedge (ab) = 1$. Alors, d'après le théorème de Bézout, il existe $u, v \in \mathbb{Z}$ tels que
$$1 = (a + b)u + abv = a(u + bv) + bu.$$
Donc, encore par théorème de Bézout,
$$a \wedge b = 1.$$
- On suppose que $a \wedge b = 1$. Soit $d \in \mathbb{N}^*$ tel que
$$d \mid a + b, \quad d \mid ab.$$

– Si $d \mid a$ alors
$$d \mid a + b - a = b.$$
Or $a \wedge b = 1$, d'où
$$d = 1.$$

– Si d ne divise pas a alors
$$d \wedge a = 1.$$
En effet pour tout $d' \in \mathbb{N}^*$ tel que $d' \mid d \mid n$ et $d' \mid a$, nous $d' = 1$. Donc, par lemme de Gauss, $d \mid b$. Puis, comme dans le cas précédent, on en déduit que
$$d = 1.$$

Donc
$$(a + b) \wedge (ab) = 1.$$

Exercice. Déterminer les triplets $(a, b, c) \in (\mathbb{N}^*)^3$ tels que
$$a \vee b = 42, \quad a \wedge c = 3, \quad a + b + c = 29.$$

Réponse. Soit $(a, b, c) \in (\mathbb{N}^*)^3$ tel que
$$a \vee b = 42, \quad a \wedge c = 3, \quad a + b + c = 29.$$

Alors
$$a \mid 42 = 2 \times 3 \times 7, \quad b \mid 42 = 2 \times 3 \times 7, \quad 3 \mid a, \quad 3 \mid c.$$

En particulier
$$3 \mid a + c = 29 - b.$$

Or 3 ne divise pas 29, donc 3 ne divise b. De plus 3 est premier, donc $3 \wedge b = 1$. Ainsi, par théorème de Gauss,
$$b \mid 2 \times 7 = 14.$$

Ainsi
$$b \in \{1, 2, 7, 14\}.$$

Or $3 \mid a + c = 29 - b$, donc
$$b \in \{2, 14\}.$$

- Si $b = 2$ alors, comme $a \vee b = 42$,
$$a \in \{3 \times 7, 2 \times 3 \times 7\} = \{21, 42\}.$$
Or $a + c = 29 - b = 27$ avec $a, c \geq 0$, donc
$$a = 21, \quad c = 6.$$

- Si $b = 14 = 2 \times 7$ alors
$$a \in \{3, 2 \times 3, 3 \times 7, 2 \times 3 \times 7\} = \{3, 6, 21, 42\}.$$
Or $a + c = 29 - b = 15$ avec $a, c \geq 0$, donc
$$(a, c) \in \{(3, 12), (6, 9)\}.$$

Réciproquement les triplets
$$(21, 2, 6), (3, 14, 12), (6, 14, 9)\}$$
sont solutions, donc il s'agit de l'ensemble des solutions.