Colle 18 – Questions de cours

Question de cours 1 — **Théorème (division euclidienne).** Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que : $a = bq + r$ et $0 \leqslant r < b$.

Preuve. Soient $a \in \mathbb{N}$, et $b \in \mathbb{N}^*$.

Considérons l'ensemble : $E = \{k \in \mathbb{N} \ / \ kb \leqslant a\}$.

L'ensemble E est une partie non vide ($0 \in E$) et majorée (par a) de $\mathbb{N}$, et admet à ce titre un plus grand élément. On pose : $q = \max E$, et $r = a - bq$. De la sorte, on a évidemment : $a = bq + r$.

De plus : $\begin{cases} qb \leqslant a & \text{(car } q \text{ est un élément de } E) \\ (q+1)b > a & \text{(car } q+1 \text{ n'est plus un élément de } E) \end{cases}$

D'où : $a - b < bq \leqslant a$. Il s'ensuit que : $0 \leqslant a - bq < b$, soit : $0 \leqslant r < b$.

On a établi l'**existence** d'un couple (q, r) d'entiers tels que : $a = bq + r$ et $0 \leqslant r < b$.

Prouvons son **unicité** : soient (q, r) et (q', r') deux couples d'entiers tels que : $a = bq + r$, $a' = bq' + r'$ et $0 \leqslant r, r' < b$. Alors : $bq + r = bq' + r'$ d'où : $r' - r = b(q - q')$. Ainsi $r' - r$ est multiple de b.

Or il résulte des conditions satisfaites par r et r' que : $-b < r' - r < b$.

Comme l'unique multiple de b strictement compris entre $-b$ et b est 0, on en déduit que $r = r'$, puis aisément $q = q'$.

Conclusion. Soient $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$. Il existe un unique couple (q, r) d'entiers tels que : $a = bq + r$ et $0 \leqslant r < b$.

Remarque. L'énoncé reste valide en supposant $a \in \mathbb{Z}$ (et non $a \in \mathbb{N}$), mais on ne demande pas de le prouver ici.

Question de cours 2 — **Corollaire (du th de Bezout).** Soient a et b deux entiers. On a :

$$a\mathbb{Z} + b\mathbb{Z} = (a \wedge b)\,\mathbb{Z}$$

Preuve. ➤ Si au moins l'un des deux entiers a ou b est nul, la propriété est triviale.

➤ Dans la suite des évènements, on suppose donc a et b non nuls. Montrons l'égalité de l'énoncé par double inclusion.

Prouvons $a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\,\mathbb{Z}$: soit $N \in a\mathbb{Z}+b\mathbb{Z}$. Alors il existe deux entiers k et k' tels que : $N = ka+k'b$.

Or, par définition du PGCD, $(a \wedge b) \,|a$ et $(a \wedge b) \,|b$. D'où : $(a \wedge b) \,|ka + k'b$ ♡.
Ainsi : $N \in (a \wedge b)\,\mathbb{Z}$. Donc : $\boxed{a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\,\mathbb{Z} \ \ (\spadesuit)}$

Prouvons $(a \wedge b)\,\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z}$: d'après le théorème de Bezout, il existe deux entiers u et v tels que : $(a \wedge b) = au + bv$.

Soit $N \in (a \wedge b)\,\mathbb{Z}$. Alors il existe un entier k tel que : $N = k\,(a \wedge b)$. Donc : $N = a\,(ku) + b\,(kv)$.

Donc : $N \in a\mathbb{Z} + b\mathbb{Z}$. D'où : $\boxed{(a \wedge b)\,\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} \ \ (\clubsuit)}$

Conclusion. On déduit de ($\spadesuit$) et de ($\clubsuit$) que : $\boxed{(a \wedge b)\,\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}}$.

Question de cours 3 — Propriété. Soient a et b deux entiers, $b \neq 0$. L'entier a est inversible modulo b si et seulement si $a \wedge b = 1$.

Preuve. ➤ Supposons a inversible modulo b : alors il existe un entier m tel que $am \equiv 1\,[b]$. Par définition de congruence, ceci implique qu'il existe un entier k tel que $am = 1 + kb$, d'où : $am - kb = 1$. On en déduit que : $a \wedge b = 1$.

➤ Réciproquement, si $a \wedge b = 1$, alors il existe d'après le théorème de Bezout un couple d'entiers (u, v) tels que : $au + bv = 1$. On en déduit que : $au \equiv 1\,[b]$. Par suite a est inversible modulo b (et u est un inverse de a modulo b).

Conclusion. a est inversible modulo b si et seulement si $a \wedge b = 1$.

Question de cours 4 — Théorème (Lemme de Gauss). Soient a, b et c trois entiers. Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

Preuve. Puisque $a \wedge b = 1$, il existe d'après le théorème de Bezout un couple (u, v) d'entiers tels que : $au + bv = 1$.

Il s'ensuit que : $acu + bcv = c$.

On peut alors observer que $a|acu$ (trivial) et $a|bcv$ (hypothèse). Il s'ensuit que : $a|acu + bcv$, donc : $a|c$.

Conclusion. Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

Question de cours 5 — Théorème (Euclide). Il existe une infinité de nombres premiers.

Preuve. Notons $\mathscr{P}$ l'ensemble des nombres premiers, et supposons que $\mathscr{P}$ soit fini. Il existe alors un entier naturel non nul $n \in \mathbb{N}^*$ tels que $\mathscr{P} = \{p_1, \dots, p_n\}$.

On pose $N = 1 + \prod_{i=1}^{n} p_i$. Supposons que N ne soit pas premier. Alors N admet un diviseur premier ; il existe donc un p_j (pour un certain $j \in [\![1, n]\!]$) qui divise N. Puisque par ailleurs divise clairement $\prod_{i=1}^{n} p_i$, on en déduit que p_j divise 1 : absurde.
Il s'ensuit que N est premier. Or par construction : $N > \max_{p \in \mathscr{P}} p$, donc $N \notin \mathscr{P}$.

Ainsi, $N \in \mathscr{P}$ et $N \notin \mathscr{P}$: contradiction. **Conclusion.** $\mathscr{P}$ est infini.

Question de cours 6 — Théorème (Petit théorème de Fermat).

Soit p un nombre premier. On a : $\forall\, m \in \mathbb{Z},\ m^p \equiv m\ [p]$

Preuve. Fixons p un nombre premier, et prouvons l'assertion $m^p \equiv m\ [p]$ par récurrence sur m, pour tout $m \in \mathbb{N}$.

L'initialisation (pour $m = 0$) est évidente.

Supposons donc la propriété établie à un certain rang m, avec $m \in \mathbb{N}$, et établissons la au rang $m + 1$.

On a : $(m+1)^p = \sum_{k=0}^{p} \binom{p}{k} m^k = m^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} m^k$. Or, p étant premier, on a : $p \mid \binom{p}{k}$ (pour tout $k \in [\![1, p-1]\!]$). Par conséquent : $\sum_{k=1}^{p-1} \binom{p}{k} m^k \equiv 0\ [p]$. Il s'ensuit que : $(m+1)^p \equiv m^p + 1\ [p]$.
L'hypothèse de récurrence permet alors d'affirmer que $(m+1)^p \equiv m + 1\ [p]$, ce qui prouve l'hérédité.
Conclusion intermédiaire : $\forall\, p \in \mathscr{P},\ \forall\, m \in \mathbb{N},\ m^p \equiv m\ [p]$ (♠)

Montrons à présent la propriété pour $m \in \mathbb{Z}_-$. Si m est un entier négatif, alors $(-m) \in \mathbb{N}$ et d'après ce qui précède, on a donc : $(-m)^p \equiv -m\ [p]$. Deux cas sont alors à distinguer, suivant que p est impair ou $p = 2$.

Si p est impair, a $(-m)^p = -m^p$, et on peut alors conclure que $m^p \equiv m\ [p]$.

Et si $p = 2$, alors $(-m)^2 = m^2$. D'où : $m^2 \equiv -m\ [2]$, et on conclut en observant * que $1 \equiv -1\ [2]$.

Conclusion. $\forall p \in \mathscr{P},\ \forall m \in \mathbb{Z},\ m^p \equiv m\ [p]$ (♠)

Question de cours 7 — **Propriété**. Soit p un nombre premier. Alors : $\forall k \in [\![1, p-1]\!],\quad p \mid \binom{p}{k}$

Interprétation. Sur la "ligne p" du triangle de Pascal, p divise tous les coefficients binomiaux (à l'exception des deux extrêmes, qui sont égaux à 1 !).

Preuve. Soit p un nombre premier. Pour tout entier $k \in [\![1, p-1]\!]$, on a : $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$. Il s'ensuit que : $k\binom{p}{k} = p\binom{p-1}{k-1}$. D'où $p | k\binom{p}{k}$. Puisque p et k sont premiers entre eux †, on en déduit par le lemme de Gauss que $p \mid \binom{p}{k}$.

Conclusion. $\forall p \in \mathscr{P},\ \forall k \in [\![1, p-1]\!],\ p | \binom{p}{k}$.

∗. Ou en observant que m et $-m$ ont la même parité, ce qui revient au même.

†. L'entier p étant premier, il est premier avec tout entier qu'il ne divise pas.

Banque d'exercices

Exercice 1 — Pour n un entier naturel, on peut noter : $\overline{a_p \cdots a_1 a_0}$ son écriture décimale, les a_i désignant des entiers compris entre 0 et 9. Cette écriture signifie que : $n = a_p \times 10^p + \cdots + a_1 \times 10 + a_0$.

Etablir que n est multiple de 11 si et seulement si $\sum_{i=0}^{p}(-1)^i a_i$ est multiple de 11.

Exercice 2 — Montrer que l'équation (E) : $5x^2 + 2y^4 = 10^8 + 9$ n'admet aucun couple d'entiers relatifs solution.

Exercice 3 — Déterminer le PGCD, et un couple de coefficients de Bezout pour les entiers 27 et 112. En déduire un inverse de 27 modulo 112, et un inverse de 112 modulo 27.

Exercice 4 — Déterminer explicitement un intervalle de 2024 entiers consécutifs ne contenant aucun nombre premier.

Exercice 5 — Déterminer tous les entiers naturels n tels que $(n-1)$ divise $(n+8)$.

Exercice 6 — Déterminer le reste dans la division euclidienne de 2^{152} par 7.

Exercice 7 — Soit $p \in \mathscr{P}$. Résoudre dans $\mathbb{Z}$ l'équation : $n^2 \equiv 1\ [p]$.

Exercice 8 — Déterminer tous les couples d'entiers naturels tels que : $\begin{cases} x \wedge y &= 15 \\ xy &= 900 \end{cases}$

Banque d'exercices - Corrigés

Exercice 1 — Pour n un entier naturel, on peut noter : $\overline{a_p \cdots a_1 a_0}$ son écriture décimale, les a_i désignant des entiers compris entre 0 et 9. Cette écriture signifie que : $n = a_p \times 10^p + \cdots + a_1 \times 10 + a_0$.

Etablir que n est multiple de 11 si et seulement si $\sum_{i=0}^{p}(-1)^i a_i$ est multiple de 11.

Soit n un entier naturel, d'écriture décimale $\overline{a_p \cdots a_1 a_0}$: $n = \sum_{i=0}^{p} a_i 10^i$.

Notons que : $10 \equiv -1$ [11]. Il s'ensuit que : $\forall\, i \in \mathbb{N},\ 10^i \equiv (-1)^i$ [11].

D'où : $\sum_{i=0}^{p}(-1)^i a_i \equiv \sum_{i=0}^{p}(-1)^i a_i$ [11], soit : $n \equiv \sum_{i=0}^{p}(-1)^i a_i$ [11].

On en déduit que : $(n \equiv 0\ [11]) \iff \left(\sum_{i=0}^{p}(-1)^i a_i = 0\ [11]\right)$.

Conclusion. $(n \in 11\mathbb{Z}) \iff \left(\sum_{i=0}^{p}(-1)^i a_i \in 11\mathbb{Z}\right)$

Exercice 2 — Montrer que l'équation (E) : $5x^2 + 2y^4 = 10^8 + 9$ n'admet aucun couple d'entiers relatifs solution.

Supposons qu'il existe $(x, y) \in \mathbb{Z}^2$ solution de l'équation. Alors, en particulier : $5x^2 + 2y^4 \equiv 10^8 + 9$ [5]

On en déduit que : $2y^4 \equiv 4$ [5].

Or, selon le corollaire du PTF, on a : $y^4 \equiv 1$ [5] (si $y \in \mathbb{Z}\backslash 5\mathbb{Z}$) ou $y^4 \equiv 0$ [5] (si $y \in 5\mathbb{Z}$).

Dans les deux cas, $2y^4$ n'est pas congru à 4 modulo 5.

Conclusion. L'équation $5x^2 + 2y^4 = 10^8 + 9$ n'admet aucun couple d'entiers relatifs solution.

Exercice 3 — Déterminer le PGCD, et un couple de coefficients de Bezout pour les entiers 27 et 112. En déduire un inverse de 27 modulo 112, et un inverse de 112 modulo 27.

On applique l'algorithme d'Euclide aux entiers 27 et 112.

$$112 = 27 \times 4 + 4$$
$$27 = 4 \times 6 + 3$$
$$4 = 3 \times 1 + 1$$
$$3 = 3 \times 1 + 0$$

On en déduit déjà que $\boxed{27 \wedge 112 = 1}$.

Puis "on remonte" les calculs précédents :

$$1 = 4 - 3 \times 1$$
$$1 = 4 - \times(27 - 4 \times 6) = 7 \times 4 - 1 \times 27$$
$$1 = 7 \times (112 - 4 \times 27) - 1 \times 27 \text{ soit finalement :}$$
$$\boxed{1 = 7 \times 112 - 29 \times 27}$$

On a ainsi obtenu une relation de Bezout pour les entiers 27 et 112, càd 2 entiers u et v tels que $27u + 112v = 27 \wedge 112$ avec $\boxed{u = -29 \text{ et } v = 7}$.

On en déduit qu'un inverse de 27 modulo 112 est -29, et qu'un inverse de 112 modulo 27 est 7.

Exercice 4 — Déterminer explicitement un intervalle de 2024 entiers consécutifs ne contenant aucun nombre premier.

L'intervalle $[\![\ 2025! + 2, 2025! + 2025\ ]\!]$ convient, en observant que tout entier de cet intervalle s'écrit $2025! + k$ avec $k \in [\![\ 2, 2025\ ]\!]$, et que $2025! + k$ est manifestement multiple de k...

Conclusion. L'intervalle $[\![\ 2025! + 2, 2025! + 2025\ ]\!]$ est un intervalle de 2024 entiers consécutifs ne contenant aucun nombre premier.

Exercice 5 — Déterminer tous les entiers naturels n tels que $(n-1)$ divise $(n+8)$.

Soit n un entier naturel tel que $(n-1)$ divise $(n+8)$. Alors :

$$(n-1)|(n+8) - (n-1) \text{ soit : } (n-1)|9$$

Il s'ensuit que $(n-1) \in \{-9, -3, -1, 1, 3, 9\}$. En étudiant ces différents cas, et en n'oubliant pas que n est positif par hypothèse, on obtient finalement : $n \in \{0, 2, 4, 10\}$.

Réciproquement, on vérifie sans difficulté que tout entier de $\{0, 2, 4, 10\}$ est effectivement solution de l'équation.

Conclusion. Les entiers naturels tels que $(n-1)$ divise $(n+8)$ sont exactement : 0, 2, 4 et 10.

Exercice 6 — Déterminer le reste dans la division euclidienne de 2^{152} par 7.

Observons que $7 \in \mathscr{P}$ et $2 \wedge 7 = 1$. Selon le corollaire du PTF, on en déduit que : $2^6 \equiv 1\ [7]$.

Il s'ensuit que $2^{150} \equiv 1\ [7]$. D'où : $2^{150} \equiv 4\ [7]$.

Conclusion. Le reste dans la division euclidienne de 2^{152} par 7 est 4.

Exercice 7 — Soit $p \in \mathscr{P}$. Résoudre dans $\mathbb{Z}$ l'équation : $n^2 \equiv 1\ [p]$.

Soit n un entier relatif.

Supposons que : $n^2 \equiv 1\ [p]$. Alors : $(n-1)(n+1) \equiv 0\ [p]$. Donc : $p|(n-1)(n+1)$.

On distingue deux cas :

- **Premier cas**. Si $p|(n-1)$. Alors $n \equiv 1\ [p]$.
- **Second cas**. Si p ne divise pas $(n-1)$, alors $p \wedge (n-1) = 1$ (un nombre premier est premier avec tout entier qu'il ne divise pas). Or : $p|(n-1)(n+1)$. On en déduit que $p|(n+1)$, d'où : $n \equiv -1\ [p]$.

On a ainsi prouvé que : $(n^2 \equiv 1\ [p]) \Longrightarrow (n \equiv 1\ [p] \text{ ou } n \equiv -1\ [p])$.

Réciproque immédiate.

Conclusion. $(n^2 \equiv 1\ [p]) \Longleftrightarrow (n \equiv 1\ [p] \text{ ou } n \equiv -1\ [p])$

Exercice 8 — Déterminer tous les couples d'entiers naturels tels que : $\begin{cases} x \wedge y &= 15 \\ xy &= 900 \end{cases}$

Soit (x, y) un couple d'entiers naturels solution du système. Puisque : $x \wedge y = 15$, il existe deux entiers x' et y' tels que :

$$x = 15x', \qquad y = 15y' \qquad \text{et} \quad x' \wedge y' = 1$$

Alors : $xy = 900 \iff 225x'y' = 900 \iff x'y' = 4$.

On en déduit que : $(x', y') = (1, 4)$ ou $(x', y') = (4, 1)$.

Par suite : $(x, y) = (15, 60)$ ou $(x, y) = (60, 15)$.

Conclusion. Il existe exactement deux couples d'entiers naturels solutions du système : $(15, 60)$ et $(60, 15)$.

Remarque : il existe exactement huit couples d'entiers relatifs solutions du système : $(\pm 15, \pm 60)$ et $(\pm 60, \pm 15)$.