

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 $0 \leq r < b$.

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

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

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

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

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

Prouvons son **unicité** : soient (q, r) et (q', r') deux couples d'entiers tels que : $a = bq + r$, $a' = bq' + r'$ et $0 \leq r, r' < b$. 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 $0 \leq r < b$.

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 événements, 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, $(a \wedge b) \mid a$ et $(a \wedge b) \mid b$. D'où : $(a \wedge b) \mid ka + k'b \quad \heartsuit$.

Ainsi : $N \in (a \wedge b)\mathbb{Z}$. Donc : $a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\mathbb{Z} \quad (\spadesuit)$

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 : $(a \wedge b)\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} \quad (\clubsuit)$

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

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

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 $j \in \llbracket 1, n \rrbracket$) 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 : $N > \max_{p \in \mathcal{P}} p$, donc $N \notin \mathcal{P}$.

Ainsi, $N \in \mathcal{P}$ et $N \notin \mathcal{P}$: contradiction. **Conclusion.** $\mathcal{P}$ 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 $k \in \llbracket 1, p - 1 \rrbracket$). 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 : $\forall p \in \mathcal{P}, \forall m \in \mathbb{N}, m^p \equiv m [p]$ (♠)

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. $\forall p \in \mathcal{P}, \forall m \in \mathbb{Z}, m^p \equiv m \ [p] \ (\spadesuit)$

QUESTION DE COURS 7 — Propriété. Soit p un nombre premier. Alors : $\forall k \in \llbracket 1, p-1 \rrbracket, \quad p \mid \binom{p}{k}$

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 $k \in \llbracket 1, p-1 \rrbracket$, 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 $p \mid k \binom{p}{k}$. Puisque p et k sont premiers entre eux[†], on en déduit par le

lemme de Gauss que $p \mid \binom{p}{k}$. **Conclusion.** $\forall p \in \mathcal{P}, \forall k \in \llbracket 1, p-1 \rrbracket, p \mid \binom{p}{k}$

*. 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 $p \in \mathcal{P}$. Résoudre dans $\mathbb{Z}$ l'équation : $n^2 \equiv 1 \pmod{p}$.

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