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 : $a = bq + r$.

En outre, puisque $q \in E$, on a $bq \leqslant a$. Et comme q est le plus grand élément de E, on a $q+1 \notin E$, càd : $(q+1)\,b > a$. En résumé : $a - b < bq \leqslant a$. Il s'ensuit que : $0 \leqslant a - bq < b$, soit : $0 \leqslant r < b$.

On a donc 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 $a \in Z$ (et non $a \in \mathbb{N}$), mais on ne demande pas de le prouver ici.

Question de cours 2 — **Exercice.** 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 $27 \wedge 112 = 1$.

Puis "on remonte" les calculs précédents :

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

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 $u = -29$ 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.

Question de cours 3 — **Propriété.** Soit n un entier, $n \geqslant 2$, et $a \in \mathbb{Z}$. L'entier a est inversible modulo n si et seulement si $a \wedge n = 1$.

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

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

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

Question de cours 4 — 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 5 — 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 6 — Théorème de Bezout $\forall\, (a,b) \in \mathbb{Z}^2,\ \exists\, (u,v) \in \mathbb{Z}^2,\ au + bv = a \wedge b$

Preuve. La propriété est immédiate lorsqu'au moins un des deux entiers a ou b est nul. On suppose donc dans la suite de la preuve que a et b sont non nuls.

On considère l'ensemble : $E = \{m \in \mathbb{N}^* \ / \ \exists\, (u,v) \in \mathbb{Z}^2,\ m = au + bv\}$.

Il est assez facile de se convaincre que E est non vide. En effet, puisque a est non nul, E contiendra au moins l'élément a (*resp.* $-a$) si a est positif (*resp.* négatif). Ainsi E est une partie non vide de $\mathbb{N}^*$; elle admet à ce titre un plus petit élément. Notons $d = \min E$.

Observons que d étant un élément de E : $\exists\, (u,v) \in \mathbb{Z}^2,\ au + bv = d$ (♠).

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

Montrons que : $d = a \wedge b$.

➤ On note déjà que $(a \wedge b) \,|a$ et $(a \wedge b) \,|b$, donc : $(a \wedge b) \,|au + bv$, càd : $(a \wedge b) \,|d$.
Il s'ensuit que : $(a \wedge b) \leqslant d$ (♣).

➤ Montrons que d divise a. D'après le théorème de la division euclidienne :

$$\exists ! \, (q, r) \in \mathbb{Z}^2, \ a = dq + r \text{ avec } 0 \leqslant r < d.$$

On a : $r = a - dq = a - (au + bv)$ d'où $r = a\,(1 - uq) + b\,(vq) \in E$. Si r était non nul, alors r serait un élément de E strictement inférieur au minimum d de E : contradiction. Il s'ensuit que $r = 0$. Par conséquent : d divise a.

Un raisonnement analogue permet d'affirmer que : d divise b.

Ainsi d est un diviseur commun à a et b, et à ce titre d est inférieur au plus grand d'entre eux.

Explicitement : $d \leqslant (a \wedge b)$ (♡). On déduit alors de (♣) et de (♡) que : $d = (a \wedge b)$.

D'où, grâce à (♠) : $\boxed{\exists \, (u, v) \in \mathbb{Z}^2, \ au + bv = a \wedge b}$.

Question de cours 7 — 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 $a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\,\mathbb{Z}$: par définition du PGCD, $(a \wedge b) \,|a$ et $(a \wedge b) \,|b$. Il existe donc deux entiers a' et b' tels que $a = (a \wedge b)\,a'$ et $b = (a \wedge b)\,b'$.
Soit $N \in a\mathbb{Z} + b\mathbb{Z}$. Alors il existe deux entiers k et k' tels que : $N = ka + k'b$. D'où : $N = (a \wedge b)\,(ka' + k'b')$, et $N \in (a \wedge b)\,\mathbb{Z}$. Donc : $\boxed{a\mathbb{Z} + b\mathbb{Z} \subset (a \wedge b)\,\mathbb{Z} \ \ (♠)}$

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 : $\boxed{(a \wedge b)\,\mathbb{Z} \subset a\mathbb{Z} + b\mathbb{Z} \ \ (♣)}$

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

Question de cours 8 — Théorème (Lemme de Gauss). Soient a, b et c trois entiers. Si $a|bc$ et $a \wedge b = 1$ alors $a|c$.

Preuve. Puisque $a|bc$, il existe un entier k tel que : $bc = ka$.

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

On en déduit que : $bcv = kav$ d'où : $(1 - au)\,c = a\,(kv)$ soit encore : $a\,(kv + uc) = c$. Puisque a divise le terme de gauche de cette égalité, il divise également celui de droite, càd : $a|c$.

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

Question de cours 9 — **Propriété**. Tout entier $n \geqslant 2$ admet au moins un diviseur premier.

Preuve. Prouvons la propriété $P(n)$: "n admet un diviseur premier" par récurrence sur n entier $\geqslant 2$.

L'initialisation (pour $n = 2$) est immédiate ; passons à l'hérédité. On suppose donc qu'il existe un entier $n \geqslant 2$ tel que $P(k)$ est vraie pour tout entier k compris entre 2 et n, puis on distingue deux cas :

Premier cas : $(n+1)$ est premier. Alors $P(n+1)$ est vérifiée.

Second cas : $(n+1)$ est composé. Alors $(n+1)$ admet un diviseur d dans $\mathbb{N}$, avec $d \in [\![\, 2, n \,]\!]$. Par hypothèse de récurrence (appliquée à l'entier d), il existe un nombre premier p tel que p divise d. Par transitivité de la relation de divisibilité, on en déduit que p divise $(n+1)$. Ainsi $(n+1)$ admet un diviseur premier, et $P(n+1)$ est donc vraie.

Conclusion. Tout entier $n \geqslant 2$ admet un diviseur premier.

Question de cours 10 — **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**. $\forall p \in \mathscr{P},\ \forall k \in [\![\, 1, p-1 \,]\!],\ p | \binom{p}{k}$.

Question de cours 11 — **Théorème**. Soit N un entier $\geqslant 2$. Il existe n nombres premiers $p_1, \ldots, p_n$ et n entiers naturels $\alpha_1, \ldots, \alpha_n$ tels que : $n = \prod_{i=1}^{N} p_i^{\alpha_i}$.

Preuve. Prouvons la propriété $P(n)$: "n admet une décomposition en facteurs premiers" par récurrence sur $n \geqslant 2$.

L'initialisation (pour $n = 2$) est immédiate ; passons à l'hérédité. On suppose donc qu'il existe un entier $n \geqslant 2$ tel que $P(k)$ est vraie pour tout entier k compris entre 2 et n, puis on distingue deux cas :

Premier cas : $(n+1)$ est premier. Alors $P(n+1)$ est vérifiée.

Second cas : $(n+1)$ est composé. Alors $(n+1)$ admet un diviseur premier p, avec $p \in [\![\, 2, n \,]\!]$; et il existe alors un entier naturel k tel que : $n+1 = kp$ (avec k également dans $[\![\, 2, n \,]\!]$). Par hypothèse de récurrence (appliquée à l'entier k), il existe N nombres premiers $p_1, \ldots, p_N$ et N entiers naturels $\alpha_1, \ldots, \alpha_N$ tels que : $k = \prod_{i=1}^{N} p_i^{\alpha_i}$.

On en déduit que : $n+1 = p\prod_{i=1}^{N} p_i^{\alpha_i}$, et on a ainsi écrit $(n+1)$ comme produit de facteurs premiers.

Il s'ensuit que $P(n+1)$ est vraie.

Conclusion. Tout entier n supérieur ou égal à 2 admet une décomposition en facteurs premiers.

---

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