Université de Provence 2011–2012

Mathématiques Générales I

Parcours PEIP

Cours : Nombres entiers

Dans ce cours, nous admettons la construction et les propriétées essentielles des nombres entiers, de l'adition et de la multiplication.

1 Dénombrements

2 Arithmétique

2.1 Division euclidienne

Proposition 1. *Pour tout $n, k \in \mathbb{Z}^*$, il existe d'uniques $q, r \in \mathbb{N}$ tels que $n = qk + r$ avec $0 \leq r < |k|$.*

Démonstration. Commençons par montrer l'existence dans le cas $n > 0$. On considère la suite arithmétique $(a_s)_{s\in\mathbb{N}}$ de raison $|k|$ et de terme initial 0. Cette suite converge vers $+\infty$ et débute en $0 < n$, il existe donc un rang $\widetilde{q} \in \mathbb{N}$ tel que $a_q = \widetilde{q}|k| \leq n$ et $a_{q+1} = (\widetilde{q}+1)|k| > n$. On pose $q = \text{signe}(k)\widetilde{q}$ et $r = n - qk$. On a alors bien $n = qk + r$, $r = n - \widetilde{q}|k| \geq n - n = 0$ et $r = n - \widetilde{q}|k| < n - (n - |k|) = |k|$.
On suppose maintenant $n < 0$. On travaille alors avec la même suite mais on considère maintenant un rang $\widetilde{q} \in \mathbb{N}$ tel que $a_q = (\widetilde{q}-1)|k| < |n|$ et $a_{q+1} = \widetilde{q}|k| \geq |n|$. Comme précédemment on pose $q = -\text{signe}(k)\widetilde{q}$ et $r = n - qk$. On a toujours $n = qk + r$ et, cette fois encore, $-r = |n| - \widetilde{q}|k| \leq 0$ et $-r = |n| - \widetilde{q}|k| > |n| - |n| - |k| = -|k|$.

Pour montrer l'unicité, on suppose que l'on a $n = qk + r = q'k + r'$ avec $0 \leq r, r' < k$. Mais alors $|r - r'| = |(q' - q)k| = |q' - q||k|$ est soit nul soit plus grand que k. Or, par l'encadrement de r et r', on sait que $-k < r - r' < k$. On en déduit que $|r - r'| = 0$, c'est-à-dire que $r = r'$ et de fait $qk = n - r = n - r' = q'k$, d'où $q = q'$. □

Définition 2. Avec les notations de la proposition précédente, on appelle *q quotient* et *r reste de la division euclidienne de n par k.*

Définition 3. On dit qu'un entier $k \in \mathbb{Z}^*$ divise un entier $n \in \mathbb{Z}^*$ si le reste de la division euclidienne de n par k est nul. On dit alors également que n est divisible par k, que k est un diviseur de n, ou encore que n est un multiple de k. On note cela $k|n$.

Remarques 4.
– Par unicité du reste de la division euclidienne, un entier non nul k divise un autre entier nul n si et seulement si il existe $q \in \mathbb{Z}^*$ tel que $n = qk$.
– Les entiers 1 et -1 divisent tous les entiers non nuls.

Proposition 5. *Pour tout $n \in \mathbb{Z}^*$, les diviseurs de n sont, en valeur absolue, majorés par $|n|$.*

Démonstration. Si k est un diviseur de n, alors il existe $q \in \mathbb{Z}^*$ tel que $kq = n$, mais alors $|k| = \frac{|n|}{|q|} \leq |n|$. □

Définition 6. On dit que deux entiers $n_1, n_2 \in \mathbb{Z}^*$ sont premiers entre eux si 1 et -1 sont les deux seuls diviseurs communs à n_1 et n_2.

Théorème 7 (théorème de Bézout)**.** *Deux entiers $n_1, n_2 \in \mathbb{Z}^*$ sont premiers entre eux si et ssi il existe $a_1, a_2 \in \mathbb{Z}$ tels que $a_1 n_1 + a_2 n_2 = 1$.*

Démonstration. Soit $n_1, n_2 \in \mathbb{Z}^*$ deux entiers premiers entre eux. Quitte à échanger n_1 et n_2, on peut supposer que $|n_1| > |n_2|$. Montrons l'existence de tels a_1 et a_2 par récurrence généralisée sur $|n_2| \in \mathbb{N}^*$.

i. Le résultat est vrai pour $n_2 = \pm 1$: on peut prendre $a_1 = -1$ et $a_2 = n_2(n_1 + 1)$.

ii. On suppose le résultat vrai jusqu'au rang $n \in \mathbb{N}^*$ et on suppose que $|n_2| = n + 1$. On fait la disivison euclidienne $n_1 = qn_2 + r$ de n_1 par n_2. On remarque alors que
   - le reste r est non nul : autrement $|n_2| = n + 1 \geq 2$ serait un diviseur commun à n_1 et n_2.
   - $|r| \leq n$: r étant le reste de la division euclidienne de n_1 apr n_2, on a $|r| < |n_2| = n + 1$.
   - r et n_2 sont premiers entre eux : tout diviseur commun à r et n_2 est aussi un diviseur de $n_1 = qn_2 + r$. Les entiers n_1 et n_2 étant premiers entre eux, les seuls diviseurs communs à r et n_2 sont donc 1 et -1.

   Par hypothèse de récurrence, on peut donc trouver $b_1, b_2 \in \mathbb{Z}$ tels que $b_1 n_2 + b_2 r = 1$. Mais alors $b_1 n_2 + b_2(n_1 - qn_2) = 1$ et en posant $a_1 = b_2$ et $a_2 = b_1 - qb_2$, on obtient bien $a_1 n_1 + a_2 n_2 = 1$.

iii. D'après le principe de raisonnement par récurrence généralisée, la propriété est donc vraie pour toute valeur de $|n_2| \in \mathbb{N}^*$ et donc pour tout $n_2 \in \mathbb{Z}^*$.

Réciproquement, si l'on a $a_1 n_1 + a_2 n_2 = 1$ pour certains $a_1, a_2 \in \mathbb{Z}$, alors tout diviseur commun à n_1 et n_2 sera également un diviseur de 1. Les seuls possibilités seront donc 1 et -1. □

Remarque 8. La démonstration du théorème de Bézout donne uns startégie récursive pour construire explicitement une relation de Bézout entre n_1 et n_2.

Exemple 9. Pour donner une relation de Bézout entre $n_1 = 1783$ et $n_2 = 243$, on commence par diviser euclidiennement 1783 par 243 :

$$1783 = 7.243 + 82 \rightsquigarrow 82 = 1783 - 7.243.$$

On cherche ensuite une relation de Bézout entre 243 et le reste 82 (avec l'idée de remplacer plus tard 82 par la combinaison linéaire de 1783 et 243 ci-dessus). Pour cela, on divise euclidiennement 243 par 82 :

$$243 = 2.82 + 79 \rightsquigarrow 79 = 243 - 2.82.$$

Puis récursivement, on calcule :

$$\begin{aligned} 82 = 1.79 + 3 &\rightsquigarrow 3 = 82 - 1.79 \\ 79 = 26.3 + 1 &\rightsquigarrow 1 = 79 - 26.3. \end{aligned}$$

On a ainsi obtenu 1, exprimé en fonction de 79 et 3. On remplace 3 d'après l'égalité précédente. On obtient :

$$1 = 79 - 26.(82 - 1.79) = 79 - 26.82 + 26.79 = -26.82 + 27.79.$$

Puis en remontant un à un les calculs, on obtient :

$$\begin{aligned} 1 &= -26.82 + 27.(243 - 2.82) = 27.243 - 80.82 \\ &= 27.243 - 80.(1783 - 7.243) = 587.243 - 80.1783. \end{aligned}$$

2.2 Décomposition en facteurs premiers

Définition 10. On dit $p \in \mathbb{N}^*$ est premier si il possède exactement 4 diviseurs, à savoir 1, -1, p et $-p$.

Remarque 11. Les entiers 1 et -1 ne sont pas premiers car ils ne posèdent que deux diviseurs.

Lemme 12 (lemme de Gauss)**.** *Si $a, b \in \mathbb{Z}^*$ sont premiers entre eux et $a|bc$ avec $c \in \mathbb{Z}^*$, alors $a|c$.*

Démonstration. D'après le théorème de Bézout, il existe $p, q \in \mathbb{Z}$ tels que $ap+bq = 1$. Mais donc $c = acp+bcq$. Or a divise bc, il existe donc $r \in \mathbb{Z}^*$ tel que $bc = ra$. Cela donne donc $c = acp + ra = (cp + r)a$ et donc a divise c. □

Corollaire 13. *Soit $a, b \in \mathbb{Z}^*$. Si p est premier et si $p|ab$, alors $p|a$ ou $p|b$.*

Démonstration. Si p ne divise pas a alors, parmi les 4 diviseurs de p, seuls 1 et -1 divisent également a. Les entiers a et p sont premiers entre eux et d'après le lemme de Gauss, p divise b. □

Corollaire 14. *Soit $(a_i)_{i\in[\![1,s]\!]}$ une suite finie d'entiers non nuls. Si p est premier et si $p|(\prod_{i=1}^{s} a_i)$, alors il existe $i \in [\![1, s]\!]$ tel que $p|a_i$.*

Théorème 15. *Soit $n \in \mathbb{N}^* \setminus \{1\}$, alors il existe*
- *un unique entier $k \in \mathbb{N}^*$;*
- *une unique suite strictement croissante de k nombres premiers positifs $p_1 < p_2 < \cdots < p_k$;*
- *une unique suite de k entiers strictement positifs $\alpha_1, \alpha_2, \cdots, \alpha_k$;*

tels que $n = \prod_{i=1}^{k} p_i^{\alpha_i}$.

Démonstration. Montrons d'abord l'existence d'une telle décomposition par l'absurde. On suppose donc qu'il existe des entiers n'en possédant pas et note n_0 le plus petit d'entre eux. Il ne peut pas être premier car il serait alors à lui-même une décomposition en facteurs premiers. Il existe donc $k \in$
$llbracket2, n_0 - 1]\!]$ qui divise n_0 et donc, $k' \in$
$llbracket2, n_0 - 1]\!]$ tel que $n_0 = kk'$. Par minimalité de n_0, k et k' admettent des décompositions en facteurs premiers, mais alors n_0 aussi, à savoir le produit des décompositions de k et de k'. Cela contredit notre hypothèse de départ et donc tout nombre entier admet une décomposition en facteurs premiers.

Montrons maintenant qu'une telle décomposition est unique. Là encore, on va raisonner par l'absurde et suposer qu'il existe des entiers plus grand que 1 possédant plusieurs décompositions en facteurs premiers. On note n_0 le plus petit d'entre eux. On a alors $n_0 = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{i=1}^{l} q_i^{\beta_i}$ avec $k, l \in \mathbb{N}^*$, $p_1 < \cdots < p_k$ et $q_1 < \cdots < q_l$ des nombres premiers et $\alpha_i, \beta_j \in \mathbb{N}^*$ pour tous indices. Quitte à échanger les deux rôles, on peut supposer $p_1 \leq q_1$. Clairement $p_1|n_0 = \prod_{i=1}^{l} q_i^{\beta_i}$ donc d'après le second corollaire du lemme de Gauss, il existe $i_0 \in [\![1, l]\!]$ tel que $p_1|q_{i_0}$. Or $1 < p_1 \leq q_1 < q_i$ pour tout $i \in [\![2, l]\!]$. La seule possibilité est donc $i_0 = 1$ et $p_1 = q_1$. Mais alors $\frac{n_0}{p_1} = p_1^{\alpha_1-1}\prod_{i=2}^{k} p_i^{\alpha_i} = q_1^{\beta_1-1}\prod_{i=2}^{l} q_i^{\beta_i}$. Or, $\frac{n_0}{P_1}$ est un entier strictement compris entre 1 et n_0. Par minimalité de n_0, il ne possède qu'une unique décomposition en facteurs premiers. On a donc $k = l$, $\alpha_1 - 1 = \beta_1 - 1$ et pour tout $i \in [\![2, l]\!]$, $p_i = q_i$ et $\alpha_i = \beta_i$. Mais alors les deux écritures de n_0 sont nécessairement identiques, ce qui contredit notre hypothèse de départ. De tels décompositions sont donc toujours uniques. □

2.3 Pgcd & Ppcm

Lemme 16. *Pour tout $n \in \mathbb{Z}^*$, il n'existe qu'un nombre fini de diviseurs de n. L'entier 1 en est toujours un.*

Démonstration. C'est une conséquence directe de la proposition 5. □

Définition 17. Pour tout $n, m \in \mathbb{Z}^*$, on appelle plus grand diviseur commun, noté ppcm(n, m) ou $n \wedge m$ le plus grand entier qui soit simultanément un diviseur de n et un diviseur de m.

Remarque 18. Dire que deux entiers $n, m \in \mathbb{Z}^*$ sont premiers entre eux, cela revient à dire que $n \wedge m = 1$.

Lemme 19. *Pour tout $n, m \in \mathbb{Z}^*$, l'entier nm est toujours un multiple commun à n et à m.*

Définition 20. Pour tout $n, m \in \mathbb{Z}^*$, on appelle plus petit multiple commun, noté pgcd(n, m) ou $n \vee m$ le plus petit entier positif qui soit simultanément un multiple de n et de m.

Proposition 21. *Soit $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ et $m = \prod_{i=1}^{k} p_i^{\beta_i}$ deux entiers strictement positifs décomposées sur un même jeu de facteurs premiers $p_1, \cdots, p_k$ (certains α_i ou β_i peuvent donc être nuls). Alors $n \wedge m = \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$ et $n \vee m = \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$*

Démonstration. On a

$$\text{- } n = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)} \times \prod_{i=1}^{k} p_i^{\alpha_i - \min(\alpha_i,\beta_i)} \qquad \text{- } m = \prod_{i=1}^{k} p_i^{\min(\alpha_i,\beta_i)} \times \prod_{i=1}^{k} p_i^{\beta_i - \min(\alpha_i,\beta_i)}$$

$$\text{- } \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} = n \times \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i) - \alpha_i} \qquad \text{- } \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i)} = m \times \prod_{i=1}^{k} p_i^{\max(\alpha_i,\beta_i) - \beta_i}.$$

Les candidats pour $n \wedge m$ et $n \vee m$ sont donc bien, respectivement, des diviseurs et des multiples de n et de m. Réciproquement, si p premier apparait dans la décomposition en facteurs premiers de $n \wedge m$ avec une puissance $\gamma \geq 1$, alors $p^\gamma | (n \wedge m)$. Or $n | (n \wedge m)$ et $m | (n \wedge m)$, donc $p^\gamma | n$ et $p^\gamma | m$. Cela signifie que γ est plus petit que la puissance de p dans, d'une part, la décomposition de n et, d'autre part, celle de m. Au final, γ est plus petit que le plus petit de ces deux nombres. En faisant ce raisonnement pour tous les nombres premiers, on obtient que $n \wedge m \leq \prod_{i=1}^{k} p_i^{\min(\alpha_i, \beta_i)}$, ce qui permet de conclure concernant $n \wedge m$.
Pour $n \vee m$, on commence, pour tout nombre premier p, par noter δ_p la puissance de p dans la décomposition de $n \vee m$. Pour tout $i \in [\![1, k]\!]$, $p_i^{\alpha_i} | (n \vee m)$ et $p_i^{\beta_i} | (n \vee m)$ car, d'une part, $p_i^{\alpha_i} | n$ et $n | (n \vee m)$ et d'autre part, $p_i^{\beta_i} | m$ et $m | (n \vee m)$. Or $p_i^{\alpha_i}$ et $p_i^{\beta_i}$ sont premiers avec tous les nombres premiers différents de p_i. D'après le lemme de Gauss, on a donc $p_i^{\alpha_i} | p_i^{\delta_{p_i}}$ et $p_i^{\beta_i} | p_i^{\delta_{p_i}}$. Autrement dit, $\alpha_i, \beta_i \leq \gamma_{p_i}$ ou encore $\gamma_{p_i} \geq \max(\alpha_i, \beta_i)$. On en déduit que $n \vee m \geq \prod_{i=1}^{k} p_i^{\max(\alpha_i, \beta_i)}$, ce qui permet de conclure. □

Corollaire 22. *Pour tout $n, m \in \mathbb{N}^*$, on a $(n \wedge m) \times (n \vee m) = nm$.*

2.4 $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 2$ un entier.

Définition 23. On dit que deux entiers $p, q \in \mathbb{Z}$ sont congrus modulo n si les restes des divisions euclidiennes de p et q par n sont les même. On note alors $p \equiv q\ [n]$.

Proposition 24. *Soit $p \in \mathbb{Z}$. Alors*

i. tout $q \in \mathbb{Z}$ est congru à p modulo n si et ssi $n | (p - q)$.

ii. il existe un unique $q \in [\![1, n-1]\!]$ tel que $p \equiv q\ [n]$.

Démonstration. On note $p = kn + r$ et $q = k'n + r'$ les divisions euclidiennes de p et q par n. Si $p \equiv q\ [n]$, alors $r = r'$ et $q - p = (k - k')n$ est un multiple de n. Réciproquement, si $q - p = sn$ avec $s \in \mathbb{Z}$, alors $q = p + sn = (k + s)n + r$. Par unicité de la division euclidienne, on a $r' = r$.

La division euclidienne donne bien un unique élément dans $[\![0, n-1]\!]$ congru à p modulo n. □

Définition 25. Pour tout $p \in \mathbb{Z}$, on note $\overline{p}^n$ l'unique entier compris entre 0 et $n-1$ congru à p modulo n. Lorsqu'il n'y a pas d'ambiguité sur la valeur de n — typiquement dans tout ce qui suit — on omettra le n dans la notation, c'est-à-dire que l'on notera $\overline{p}$ pour $\overline{p}^n$.

Proposition 26. *Un entier $p \in \mathbb{Z}$ est divisible par n si et ssi $\overline{p} = 0$.*

Définition 27. On appelle $\mathbb{Z}/n\mathbb{Z}$ l'ensemble $[\![0, n-1]\!]$ muni des opérations $+_n \colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ et $\cdot_n : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ définies, pour tous $a, b \in \mathbb{Z}/n\mathbb{Z}$ par

$$a +_n b := \overline{a + b} \quad \text{et} \quad a.{}_n b := \overline{ab}$$

où l'addition et la multiplication dans les membres de droites sont celles de $\mathbb{Z}$.

Exemple 28. On définit $\mathbb{Z}/5\mathbb{Z}$ comme les entiers $\{0, 1, 2, 3, 4\}$ munis des opérations

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

et

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Proposition 29. *Soit $p_1, p_2, q_1, q_2 \in \mathbb{Z}$ tels que $p_1 \equiv q_1\ [n]$ et $p_2 \equiv q_2\ [n]$. Alors $p_1 + p_2 \equiv q_1 + q_2\ [n]$ et $p_1 p_2 \equiv q_1 q_2\ [n]$.*

Démonstration. Puisque $p_1 \equiv q_1\ [n]$ et $p_2 \equiv q_2\ [n]$, il existe $k_1, k_2 \in \mathbb{Z}$ tels que $p_1 - q_1 = k_1 n$ et $p_2 - q_2 = k_2 n$. On a alors $(p_1 + p_2) - (q_1 + q_2) = (p_1 - q_1) + (p_2 - q_2) = (k_1 + k_2)n$ et $p_1 p_2 - q_1 q_2 = (p_1 - q_1)p_2 + q_1(p_2 - q_2) = (k_1 p_2 + q_1 k_2)n$. □

Corollaire 30. *Pour tout $p, q \in \mathbb{Z}$, on a $\overline{p + q} = \overline{p} +_n \overline{q}$ et $\overline{pq} = \overline{p}.{}_n\overline{q}$.*

Démonstration. On a clairement $p \equiv \overline{p}$ et $q \equiv \overline{q}$, et donc $p + q \equiv \overline{p} + \overline{q}$ et $p.q \equiv \overline{p}.\overline{q}$. □

Corollaire 31. *Toutes les règles de calculs dans $\mathbb{Z}$ sont valables dans $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Pour un calcul faisant intervenir des éléments $a_1, \cdots, a_k$ de $\mathbb{Z}/n\mathbb{Z}$, on choisit des entiers $p_1, \cdots, p_k$ tels que $a_i = \overline{p_i}$ pour tout $i \in [\![1, k]\!]$. On écrit les différentes étapes du calcul dans $\mathbb{Z}$ avec les $p_1, \cdots, p_k$, et on passe tout à la barre du modulo n. D'après la proposition 30, la barre se scindera successivement à chaque addition et à chaque multiplication au-dessus des deux termes de l'opération pour, au final, venir coiffer chacun des p_i et les retransformer en a_i. □

Remarque 32. Combiné avec la proposition 26, cela permet de résoudre rapidement certains problème de divisibilité.

Exemple 33. Pour montrer que, pour tout $n \in \mathbb{N}$, 7 divise $3^{2n+1} + 2^{n+2}$, on peut constater que $3^{2n+1} + 2^{n+2} = 3.(3^2)^n + 2^n.2^2 = 3.9^n + 4.2^n \equiv 3.2^n + (-3).2^n \equiv 0\ [7]$.