Arithmétique dans $\mathbb{Z}$

Dominique Hoareau, domeh@wanadoo.fr

Table des matières

1 En amont. **3**

2 Diviser pour mieux régner. **3**
2.1 Division euclidienne dans $\mathbb{N}$ . . . 3
2.2 Écriture d´un entier en base b. . . . 5
2.2.1 Division euclidienne au service d´un codage des entiers . . . 5
2.2.2 Passage de la base 10 à une base b. . . . 5
2.2.3 Écriture en base b au service de la "potence euclidienne" . . . 6

3 Divisibilité et congruences **6**
3.1 Lorsque la division euclidienne tombe juste 6
3.2 Lorsque la division euclidienne est incongrue 9

4 Diviseurs communs **12**
4.1 Les cavaliers de la (petite) reine . . . 12
4.2 Allez Bizut montre nous tes ..., allez Bézout montre nous ton 14
4.3 Une équation diophantienne incontournable . . . 17

5 Quelques joyaux de la reine **18**
5.1 Décomposition en facteurs premiers . . . 18
5.2 Petit théorème de Fermat . . . 19
5.3 Théorème de Wilson . . . 20

6 Pour aller plus loin **21**
6.1 Éléments marginaux de $\mathcal{Z}$ . . . 21
6.2 Éléments associés . . . 22
6.3 Éléments indivisibles . . . 22
6.4 Notions de *pgcd* et *ppcm* . . . 23
6.5 Anneaux intègres . . . 23
6.6 Anneaux principaux . . . 25
6.6.1 Entre les anneaux euclidiens 25
6.6.2 et les anneaux factoriels, ... 25
6.6.3 le principal, c´est Bézout. . . . 27

Références :
- Mathématiques d´école, Daniel Perrin, Cassini, 2005.
- Merveilleux nombres premiers, J-P. Delahaye, Belin, 2000.
- Découvrir l´arithmétique, P. Damphousse, Opuscules, Ellipses, 2000.
- Diagonales, les cahiers mathématiques du Cned, numéro 2 année 2001-2002 et numéro 2 année 2005-2006.
- http ://www.irem.univ-mrs.fr/activites/superieur/arithmetique.php, R. Rolland.
- http ://perso.orange.fr/maths.rombaldi/Capes/AlgebreCapes.pdf, J-E. Rombaldi.
- http ://mon.univ-montp2.fr/claroline/document/goto/ ?url=%2Fpoly9.pdf&cidReq=ARI

Introduction : Il est aisé de former les entiers lorsqu´on utilise l´addition. On part de 1 et on ajoute à chaque fois 1 au nombre déjà construit. On a $2 = 1 + 1$, puis $3 = 2 + 1 = 1 + 1 + 1$ et ainsi de suite. On peut dire que 1 est un générateur pour $(\mathbb{N}, +)$. Peut-on construire les entiers avec la multiplication ? On apprend très tôt que certains nombres entiers se cassent (ex : $6 = 2 \times 3$) alors que d´autres, comme 7, sont d´un seul tenant. Ces derniers, irréductibles ou insécables, s´appellent nombres premiers et, comme de véritables briques numériques, entrent dans la composition de tous les autres entiers. On tente d´apprivoiser ces êtres aux propriétés mystérieuses...

On propose un exposé niveau TS-Spécialité, dans l´esprit des programmes, c-à-d sous un éclairage algorithmique. Des compléments algébriques, qui règlent, en quelques coups de cuillère à pot, certaines constructions et résolutions de problèmes, sont proposés sous la rubrique «Pour aller plus loin». Dans la dernière partie du texte, on évoque, pour d´autres anneaux, la force «euclidienne» de $\mathbb{Z}$ (algorithme d´Eucide), sa force «principale» (Théorème de Bézout) et sa force «factorielle» (Théorème fondamental de l´arithmétique).

On suppose connus l´ensemble $\mathbb{N}$ des entiers naturels et l´objet $\mathbb{Z}$ des relatifs munis de l´addition, de la multiplication et de la relation d´ordre total notée $\leqslant$. On dispose d´une batterie de bons sous-objets de $\mathbb{Z}$ (comme, par exemple, l´ensemble des entiers pairs) : ce sont les

$$n\mathbb{Z} = \{nq,\ q \in \mathbb{Z}\}$$

dont les éléments, appelés multiples de n, forment une suite arithmétique de raison n.

Question du jury : Qui se cache derrière $2\mathbb{Z}.3\mathbb{Z} = \{xy \in \mathbb{Z},\ x \in 2\mathbb{Z} \text{ et } y \in 3\mathbb{Z}\}$?

Réponse : «Ils se multiplièrent et eurent beaucoup d´enfants.»

Pour aller plus loin :
L´ensemble $\mathbb{Z}$ est un anneau commutatif, unitaire, intègre, et totalement ordonné. Les $n\mathbb{Z}$, dont n constitue un générateur, vérifient

1. la stabilité pour la loi additive : $\forall (k, l) \in n\mathbb{Z},\ k + l \in n\mathbb{Z}$.
2. la stabilité pour le passage à l´opposé : $\forall k \in n\mathbb{Z},\ -k \in n\mathbb{Z}$.
3. la propriété d´absorption : $\forall k \in n\mathbb{Z},\ \forall l \in \mathbb{Z},\ kl \in n\mathbb{Z}$.

donc sont "des" idéaux (monogènes ou principaux) de $\mathbb{Z}$.

Exercice 1 : Si $a, b \in \mathbb{Z}$ vérifient $a + b \in n\mathbb{Z}$ et $ab \in n\mathbb{Z}$, alors $a^2 \in n\mathbb{Z}$.

Corrigé : Il suffit de relier $a+b$, ab et a^2 : a est racine du trinôme $x^2 - (a+b)x + ab$, c-à-d $a^2 = (a+b)a - ab$.

Question du jury : :

1. Pour $n, m \in \mathbb{N}$, donner une condition nécessaire et suffisante pour avoir $n\mathbb{Z} = m\mathbb{Z}$.
2. Sur les traces de Galilée, peut-on mettre en bijection $\mathbb{Z}$ et sa partie stricte $\mathbb{N}$?

Réponse : Il suffit d´envoyer n sur $2n$ si $n \in \mathbb{N}$, sur $-2n - 1$ si $n \in \mathbb{Z}^- \setminus \{0\}$.

1 En amont.

On rappelle une propriété fondamentale de $\mathbb{N}$, qui «irrigue» la suite du texte :

Bon ordre sur $\mathbb{N}$:

1. Toute partie non vide de $\mathbb{N}$ admet un plus petit élément (pour l´ordre usuel).
2. Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.

Voici deux autres incarnations du bon ordre sur $\mathbb{N}$:

1. le théorème de récurrence,
2. la descente infinie de Fermat.

Propriété :

Il n´y a pas de suite strictement décroissante à valeurs dans $\mathbb{N}$.

Preuve : On raisonne par l´absurde. Si tel est le cas, soit (u_n) un tel objet. L´ensemble de ses valeurs est une partie non vide et minorée (par 0) de $\mathbb{N}$ donc admet un minimum, un certain u_N. Puisque (u_n) décroît strictement, $u_{N+1} < u_N$, ce qui contredit le statut de u_N. □

2 Diviser pour mieux régner.

2.1 Division euclidienne dans $\mathbb{N}$

Théorème :

Soit a, b deux entiers naturels avec $b > 0$. Alors il existe un unique couple $(q, r) \in \mathbb{N}^2$ tels que

$$a = bq + r \qquad \text{et} \qquad 0 \leqslant r < b.$$

On dit que a est le dividende, b le diviseur, q le quotient et r le reste dans la division de a par b.

Preuve :
Le lecteur peut rédiger la preuve de l´existence de (q, r) à partir de l´algorithme des différences :

Algorithme :

- Données : a, b dans $\mathbb{N}$ avec $a > b$.
- Variables : q et r.
- Initialisation : $q = 0$ et $r = a$.
  On a la relation $a = bq + r$ à l´entrée de boucle.
- Début boucle : Tant que $r > b$, faire
- Corps de la procédure : $q = q + 1$, $r = r - b$.
  Si on commence un tour de boucle avec $a = bq + r$, à la fin de boucle, on a encore $a = bq + r$: r a diminué de b et simultanément, q augmentant d´une unité, bq augmente de b.
- Fin de boucle : Renvoyer q et r.

La boucle "While" se termine parce que la partie $Q = \{k \in \mathbb{N},\ a - bk \geqslant 0\}$ de $\mathbb{N}$, qui est non vide ($0 \in Q$), possède un plus petit élément.

Pour l´unicité, on envisage deux couples (q, r) et (q', r') qui conviennent : $b(q - q') = r' - r$ avec $0 \leqslant r, r' \leqslant b - 1$. Si $q \neq q'$, $| q - q' | \geqslant 1$ donc $b \mid q - q' | \geqslant b$, $| r' - r | \geqslant b$. Contradiction puisque la distance entre r et r' (compris tous les deux entre 0 et $b - 1$) est inférieure à $b - 1$. Ainsi, $q = q'$, puis $r = a - bq = a - bq' = r'$. □

Exemple :
On effectue la division euclidienne de 347 par 5. Au lieu de, comme le ferait une machine, retrancher (à 347) 5 une première fois, 5 une deuxième fois, ... jusqu´à obtention d´ un reste plus petit que 5, on utilise les bonnes vieilles tables de multiplication :

$$347 = 60 \times 5 + 47, \text{ puis } 347 = 60 \times 5 + 9 \times 5 + 2 = 69 \times 5 + 2.$$

On a évité 69 soustractions successives.

Exercice 2 :
- Anne, ma soeur Anne, ne vois-tu rien venir ?
- Je ne vois rien que le soleil qui poudroie, et l´herbe qui verdoie.

Après avoir listé les premiers éléments positifs de $2\mathbb{Z}$ et $3\mathbb{Z}$, déterminer $2\mathbb{Z} \cap 3\mathbb{Z}$.
Pourquoi $2\mathbb{Z} \cup 3\mathbb{Z}$ n´est-il pas un "bon" sous-objet de $\mathbb{Z}$? Déterminer $2\mathbb{Z} + 3\mathbb{Z}$.

Corrigé : On vérifie que $6\mathbb{Z} \subset 2\mathbb{Z} \cap 3\mathbb{Z}$. Soit à présent $n \in 2\mathbb{Z} \cap 3\mathbb{Z}$. On envisage la division euclidienne de n par 6 : $n = 6q + r$ avec $0 \leqslant r \leqslant 5$. Puisque $r = n - 6q$ avec $n \in 2\mathbb{Z}$ et $-6q \in 2\mathbb{Z}$, $r \in 2\mathbb{Z}$. De même $r \in 3\mathbb{Z}$. Le seul entier entre 0 et 5 multiple de 2 et 3 est 0, donc $n = 6q \in 6\mathbb{Z}$.

On a $2 \in 2\mathbb{Z}$ donc $2 \in 2\mathbb{Z} \cup 3\mathbb{Z}$. De même, $3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$. Or $2+3 = 5$ n´appartient pas à $2\mathbb{Z} \cup 3\mathbb{Z}$. Pour pallier ce défaut de stabilité, on envisage $2\mathbb{Z} + 3\mathbb{Z}$. On peut vérifier que $2\mathbb{Z} + 3\mathbb{Z}$ a toutes les bonnes propriétés de $2\mathbb{Z}$, contient $2\mathbb{Z} \cup 3\mathbb{Z}$ et est le plus petit sous-objet "efficace" de $\mathbb{Z}$ contenant $2\mathbb{Z} \cup 3\mathbb{Z}$. Puisque $2 \times (-1) + 3 \times 1 = 1$, on a $1 \in 2\mathbb{Z} + 3\mathbb{Z}$ et, pour tout $n \in \mathbb{Z}$, $n = n \times 1 = 2 \times (-n) + 3 \times n \in 2\mathbb{Z} + 3\mathbb{Z}$. Puisque l´inclusion $2\mathbb{Z} + 3\mathbb{Z} \subset \mathbb{Z}$ est automatique, on a $2\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}$.

Exercice 3 : (Un sacré concurrent)
Un candidat au CAPES a 461 exercices à caser dans ses leçons d´oral. Un tantinet rigide, il suit deux règles :

1. Il ne commence pas une leçon avant d´avoir fini la précédente.
2. Chaque leçon doit contenir le même nombre d´exercices.

Avant les oraux, le candidat a préparé 14 leçons. Combien d´exercices contiennent les leçons achevées ? Combien d´exercices pour la dernière leçon ?

Corrigé : Puisque $461 \notin 14\mathbb{Z}$, seules 13 leçons sont complètes. On a $461 = 13 \times 35 + 6$ donc une première réponse est : 13 leçons complètes à 35 exercices et 1 leçon à 6 exercices. Y-a-t-il d´autres combinaisons ? On peut essayer de réduire le nombre d´exercices sur les leçons complètes et avoir une incomplète plus étoffée. On a $461 = 13 \times 34 + 19$, ce qui donne un autre couple solution $(34; 19)$. On a $461 = 13 \times 33 + 32$, qui donne une autre solution $(33; 32)$. La tentative "leçon complète à 32 exercices" est infructueuse : puisque $461 = 13 \times 32 + 45 = 14 \times 32 + 13$, il s´agirait de 15 leçons préparées.

Corollaire : «$\mathbb{Z}$ est euclidien.»
Soit $(a, b) \in \mathbb{Z} \times \mathbb{Z}^*$. Alors il existe un couple $(q, r) \in \mathbb{Z}^2$ tel que

$$a = bq + r \text{ avec la mesure du reste : } r = 0 \text{ ou } |\, r \,| < |\, b \,|\,.$$

Remarque : On perd dans $\mathbb{Z}$ l´unicité du quotient et du reste comme le prouvent les égalités

$$24 = 5 \times 4 + 4 \text{ et } 24 = 5 \times 5 - 1.$$

Pour aller plus loin :

Application : (Sous-groupes additifs de $\mathbb{Z}$ et idéaux de l´anneau $\mathbb{Z}$)

1. Les sous-groupes de $(\mathbb{Z},+)$ sont exactement les $n\mathbb{Z}=\{nq,\ q\in\mathbb{Z}\}$, pour $n\in\mathbb{N}$.
2. Les idéaux de $(\mathbb{Z},+,\times)$ sont exactement les $n\mathbb{Z}$. On dit que $\mathbb{Z}$, qui ne possède que des idéaux monogènes, est un anneau principal. Les cas $n=0$ et $n=1$ donnent lieu à $\{0\}$ et $\mathbb{Z}$.

Preuve : Les $n\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$. Réciproquement, soit H un sous-groupe de $\mathbb{Z}$, $H\neq\{0\}$. La partie $H\cap\mathbb{N}^*$ non vide de $\mathbb{N}$ a un plus petit élément qu´on appelle n. Clairement, $n\mathbb{Z}\subset H$. A présent, si $x\in H$, par division euclidienne, x s´écrit $x=nq+r$, avec $0\leqslant r<n$. Ainsi $r=x-nq$ est dans H et dans $\mathbb{N}^*$, et $r=0$ par statut de n. Finalement $x=nq\in n\mathbb{Z}$. On retiendra qu´un générateur d´un sous-groupe $H\neq\{0\}$ de $\mathbb{Z}$ est le plus petit entier naturel non nul qui se trouve dans H.

Un idéal I de $\mathbb{Z}$ est déjà un sous-groupe de $\mathbb{Z}$, donc de la forme $n\mathbb{Z}$, avec $n\in\mathbb{N}$. Puisque, réciproquement, chaque $n\mathbb{Z}$ est un idéal, les idéaux de $\mathbb{Z}$ sont exactement les $n\mathbb{Z}$. □

2.2 Écriture d´un entier en base b.

2.2.1 Division euclidienne au service d´un codage des entiers

Théorème :

Soit $b\in\mathbb{N}$, $b\geqslant 2$. Tout entier $a>0$ s´écrit de façon unique :

$$(✠)\quad a=a_nb^n+\cdots+a_2b^2+a_1b+a_0\quad\text{où } n\in\mathbb{N},\ a_i\in\mathbb{N},\ 0\leqslant a_i<b \text{ et } a_n\neq 0.$$

Dans cette écriture dite en base b, les a_i sont appelés chiffres de a en base b. On note $a=\overline{a_n\cdots a_1a_0}$.

Preuve : Pour l´existence de l´écriture (✠), montrer, par récurrence sur $N\in\mathbb{N}$, la propriété :

$$E(N)\quad \text{Tout entier } a \text{ compris entre 1 et } N \text{ a une écriture } (✠).$$

L´initialisation est facile pour $0\leqslant N<b$. Si $E(N)$ est vraie avec $N\geqslant b-1$, montrer $E(N+1)$ en envisageant la division euclidienne de $N+1$ par b.

Pour l´unicité, montrer, par récurrence, la propriété $U(N)$: Si un entier a compris entre 1 et N a deux écriture

$$a=a_nb^n+\cdots+a_2b^2+a_1b+a_0=a'_mb^m+\cdots+a'_2b^2+a'_1b+a'_0,$$

alors $m=n$ et, pour tout $1\leqslant i\leqslant n$, $a_i=a'_i$. □

Question du jury : Que penser de l´affirmation : «le théorème de la division eulidienne est, tacitement, le résultat mathématique le plus universellement utilisé» ?

Exemple : (d´après D. Perrin, Mathématiques d´école, Cassini, 2005)
Dans la Gaule antique, en Septimanie (où on avait la manie de compter en base 7), le druide Pacorabanix, fort versé en numérologie, avaient prévu la fin du monde pour l´an $\overline{5555}$. Vérifier que ce nombre, remarquable en base 7, l´est encore en base 10. On l´a échappé belle !

2.2.2 Passage de la base 10 à une base b.

Algorithme :
- Données : a, b dans $\mathbb{N}$ avec $a>b\leqslant 2$.
- Variables : $n\in\mathbb{N}$ et $rslt\in\mathbb{N}$.

- Initialisation : $n = 0$ et $rslt = 0$.
- Début boucle : Tant que $a > 0$, faire
- Corps de la procédure :
  - $q = quotient\ de\ a\ par\ b$
  - $r = reste\ de\ a\ par\ b$
  - $rslt \longleftarrow rslt + r \times b^n$
  - $n \longleftarrow n + 1$
  - $a \longleftarrow q$
- Fin de boucle : Renvoyer $rslt$.

Question du jury : : Qu´est-ce qui garantit la fin de boucle ?

Réponse : Descente infinie de Fermat : Dans $\mathbb{N}$, on ne peut pas diviser sans fin sauf par 1, sans être confronté à une contradiction.

Exercice 4 : (La bonne année !)
Donner l´écriture de 2008 en base 7.

2.2.3 Écriture en base b au service de la "potence euclidienne"

On pourra illustrer par la bonne vieille potence l´algorithme suivi par un élève du primaire pour effectuer la division de 347 par 5 :

- Dans 34, combien de fois 5 ? Il y va 6 fois. $6 \times 5 = 30$, qu´on enlève de 34. Il reste 4. On abaisse le chiffre 7 des unités.
- Dans 47, combien de fois 5 ? Il y va 9 fois. $9 \times 5 = 45$, qu´on retranche à 47. Il reste 2, plus petit que 5.
- Conclusion : Le quotient est 69 et le reste et 2.

On justifie l´algorithme. Soit $a, b \in \mathbb{N}$, $b > 0$, q et r les quotient et reste de la division de a par b. On envisage l´entier $a' = 10a + \alpha$ où $0 \leqslant \alpha \leqslant 9$.

1. Quel est le lien entre l´écriture décimale de a et celle de a' ?
2. On veut effectuer la division euclidienne de a' par b.
   (a) Vérifier que $a' = b(10q) + 10r + \alpha$.
   (b) On appelle q' et r' les quotient et reste de la division de $10r + \alpha$ par b. Vérifier que $0 \leqslant q' \leqslant 9$.
   (c) En déduire le quotient et le reste de la division de a' par b.

3 Divisibilité et congruences

3.1 Lorsque la division euclidienne tombe juste ...

Définition :

Pour a et b dans $\mathbb{Z}$, on dit que
- b divise a
- ou b est un diviseur de a
- ou encore a est un multiple de b,

et on note $b \mid a$, lorsque $a \in b\mathbb{Z}$, c-à-d lorsqu´il existe $q \in \mathbb{Z}$ tel que $a = bq$.
Si, pour $x \in \mathbb{Z}$, $\mathcal{D}_x$ désigne l´ensemble des diviseurs de x, on a la correspondance :

$$b \mid a \Leftrightarrow a\mathbb{Z} \ \subset \ b\mathbb{Z} \Leftrightarrow \mathcal{D}_b \ \subset \ \mathcal{D}_a.$$

Remarque : Lien avec l´ordre usuel sur $\mathbb{N}^*$: $\forall a, b \in \mathbb{N}^*,\ b \mid a \ \Rightarrow \ b \leqslant a$.

Exemple : si on écrit une séquence de 3 chiffres et si on répète le motif pour obtenir un entier N de 6 chiffres (en base 10), on est certain d´avoir un multiple de 7. En effet, on peut poser $N = \overline{abcabc}$ et on a

$$N = \overline{abc} \times 1000 + \overline{abc} = 1001 \times \overline{abc} = 7 \times 11 \times 13 \times \overline{abc}.$$

Exercice 5 : Qui ne saute pas n´est pas de Montpellier !
Pour la finale de la coupe de France de football, les dirigeants du Montpellier Hérault proposent de louer des cars afin d´emmener des supporters à Paris. On sait qu´il y aura entre 2000 et 3000 supporters qui feront le déplacement. Pour des raisons pratiques, les dirigeants souhaitent que chaque car contienne le même nombre de passagers. Dans un premier temps, la répartition envisagée correspond à 45 personnes par car mais il reste 6 personnes sans place. On réalise qu´avec un car de moins, tout le monde a une place dans les conditions requises. Déterminer le nombre N de supporters qui feront le déplacement.

Corrigé : Soit s le nombre de supporters par car et n le nombre de cars retenus. On a

$$N = 45(n+1) + 6 = 45n + 51$$

et, puisque $2000 \leqslant N \leqslant 3000$, il vient $44 \leqslant n \leqslant 65$. Par ailleurs, $N = ns$ donc $45n + 51 = ns$, $51 = n(s - 45)$, $n \mid 51$. Ainsi, $n \in \{1, 3, 17, 51\}$ puis $n = 51$ et $N = 2346$.

Exercice 6 : Trouver les entiers $n \in \mathbb{N}^*$ tels que

1. $n \mid n + 8$.
2. $n - 1 \mid n + 11$.
3. $n - 4 \mid 3n + 24$.

Corrigé : Pour 1, si n convient, n est un diviseur de 8 et réciproquement, 1, 2, 4 et 8 conviennent. Pour 2, si $n - 1 \mid n + 11$, $N = n - 1$ divise 12 et on étudie la réciproque. Pour 3, si $n - 4 \mid 3n + 24$, $N = n - 4$ est un diviseur de 36 et réciproquement, ...

Exercice 7 : Quels sont les entiers naturels non nuls n qui vérifient $n + 1 \mid (n^2 + 1)$.

Corrigé : Si n convient, avec $n^2 + 1 = (n+1)n - n + 1 = (n+1)n - (n-1)$, on a $n+1 \mid (n-1)$. Ceci impose $n - 1 = 0$, $n = 1$. Réciproquement, $n = 1$ convient.

Exercice 8 : Quels sont les entiers relatifs n qui vérifient $n - 3 \mid (n^3 - 3)$?
On pourra vérifier l´existence de $q \in \mathbb{Z}$ tel que $n^3 - 3 = q(n - 3) + 24$.

Tout entier naturel supérieur à 2 possède au moins deux diviseurs positifs distincts : 1 et lui-même. Qui sont les entiers minimalistes pour cette règle ?

Définition :

Un entier naturel p est dit nombre premier si $p \neq 1$ et si p n´a que deux diviseurs positifs : 1 et lui-même.
Les nombres 2, 3, 5, 7, 11, 13, 17 sont des nombres premiers.

Exemple : Pour $n \geqslant 2$, une somme S de n entiers impairs consécutifs n´est jamais premier. En effet, on peut écrire

$$S = (2k+1) + (2k+1+2) + (2k+1+2\times 2) + \cdots + (2k+1+2\times(n-1)),\ k \in \mathbb{Z}$$

donc

$$S = n \times (2k+1) + 2 \times (1 + \cdots + (n-1)) = n(2k+1) + n(n-1) = n(2k+n),$$

ce qui garantit que n (distinct de 1 et de S) divise S.

Question du jury : Vrai ou faux : Pour tout entier naturel n, $n^2 + n + 41$ est un nombre premier.

Réponse : Avec $n = 41$, on a $41^2 + 41 + 41 = 41 \times (41 + 1 + 1) = 41 \times 43$.

Exercice 9 : (Un seul mot d´ordre : factoriser)

1. Pour tout entier $n \geqslant 3$, $n^2 + 2n - 3$ n´est pas premier.
2. Même conclusion pour $n^4 + 4$ dès que $n > 1$.

   Commentaire : "I worked on this problem for days, applying in vain all the number theory I knew or could learn. Finally, sufficiently humbled now, I asked the buddy (who had given me the problem) how to solve this problem. He said "Dummy, the polynomial factors !". And indeed it does. It is the difference of two squares in disguise : ... My "irrational exuberance" was quelled and I learned my first painful lesson in humility."
3. Même conclusion pour $n^5 + n^4 + 1$ si $n > 1$.
4. Pour $n, m \in \mathbb{N}^*$, si $n > 1$ ou $m > 1$, alors $n^4 + 4m^4$ n´est pas premier.

Exercice 10 : (D´après baccalauréat Dijon session 1973)

1. Le nombre $2^{11} - 1$ est-il premier ?
2. p et q étant deux entiers naturels non nuls, quel est le reste de la division par $2^p - 1$ du nombre $2^{pq} = 2^{pq}$? En déduire que, si $2^n - 1$ est premier, alors n est premier.

Commentaire : Les nombres $M_n = 2^n - 1$, considérés par Mersenne en 1644 pour la recherche de grands nombres premiers, portent son nom. En 1999, le plus grand nombre premier connu est $M_{6972593}$.

Exercice 11 : «Tout premier positif de $\mathbb{Z}$ est un nombre premier.»
Soit $p \in \mathbb{N}$. On envisage les énoncés :

1. $p \neq 0$, $p \neq 1$ et $\forall a, b \in \mathbb{N} \quad p \mid ab \Rightarrow p \mid a$ ou $p \mid b$.
2. p est un nombre premier.

Montrer que 1. implique 2.

Corrigé : Sous 1., $p \neq 1$. Soit a un diviseur de p dans $\mathbb{N}$. On écrit $p = ab$ et, d´après 1., on peut supposer que $a = p\alpha$, $\alpha \in \mathbb{N}$. Il vient $p = p\alpha b$, $p(1 - \alpha b) = 0$ avec $p \neq 0$ et, puisque $\mathbb{Z}$ est intègre, $\alpha b = 1$, $\alpha \mid 1$, $\alpha = 1$, donc $a = p$ et p est premier.

Exercice 12 : (Une grande plage de nombres composés)
Soit $n \in \mathbb{N}$. En utilisant la quantité $(n + 1)!$, construire n nombres entiers consécutifs non premiers.

Commentaire : Il existe des intervalles arbitrairement longs sans nombre premier. Pourtant, il existe une infinité de nombres premiers (cf infra). On pense même qu´il existe une infinité de nombres premiers p dont le successeur impair $p + 2$ est aussi premier.

Propriété : (Fondamentale)

Tout entier n distinct de 1 admet un diviseur premier p.

Preuve : On suppose $n > 1$. Si $\mathcal{D}_n$ désigne l´ensemble des diviseurs de n, $\mathcal{D}_n \setminus \{1\}$, qui contient n, possède un plus petit élément p. Si $q \mid p$, alors $q \mid n$ et, par conséquent, $q = 1$ ou $q = p$, donc p est un diviseur premier de n. □

Application : (Partie existencielle du théorème fondamental de l´arithmétique)
Tout entier $n \geqslant 2$ peut s´écrire comme un produit de facteurs premiers.

Preuve : Par récurrence, laissée au lecteur. □

Application : (Théorème d´Euclide ou le parangon de la preuve mathématique)
Il existe une infinité de nombres premiers.

Preuve : On raisonne par l´absurde en envisageant la liste (finie) $\{p_1, \cdots, p_n\}$ des nombres premiers. On pose :

$$M = p_1 \times \cdots \times p_n + 1.$$

Soit p un diviseur premier de M. On a $p > p_n$ sous peine de voir $p \mid (M - p_1 \times \cdots \times p_n)$, i.e $p \mid 1$. Enfin, $p > p_n$ est exclu puisque p_n est supposé être le plus grand nombre premier. □

Commentaire : Si on note, pour $x \in \mathbb{R}$, $\pi(x)$ le nombre des nombres premiers au plus égaux à x, la fonction $x \mapsto \pi(x)$, clairement croissante, tend vers $+\infty$ avec x. En 1896, Hadamard et La Vallée-Poussin démontrent une estimation en $+\infty$ conjecturée par Gauss et Legendre :

$$\pi(x) \approx \frac{x}{\ln x}.$$

Application : («Sonwil»)
Soit $p \in \mathbb{N}$ tel que $(p-1)! \equiv -1\,(p)$. Alors p est premier.

Preuve : Si p est composé, on prend n un diviseur premier de p. Puisque $n < p$, $n \mid (p-1)!$ et, puisque $n \mid p$ et $p \mid (p-1)! + 1$, on a $n \mid (p-1)! + 1$. Il vient $n \mid 1$ avec n premier. Contradiction. □

Pour aller plus loin : La divisibilité restreinte à $\mathbb{N}$, qui vérifie

$$\forall a, b, c \in \mathbb{N}, \quad a \mid a \text{ (réfléxivité)}, \quad b \mid a \text{ et } a \mid b \Rightarrow a = b \text{ (antisymétrie)}, \quad c \mid b \text{ et } b \mid a \Rightarrow c \mid a \text{ (transitivité)},$$

est une relation d´ordre partiel sur $\mathbb{N}$.

1. Lien avec l´ordre usuel sur $\mathbb{N}^*$: $\forall a, b \in \mathbb{N}^*,\ b \mid a \ \Rightarrow\ b \leqslant a$.
2. O est le plus grand élément et 1 le plus petit dans $(\mathbb{N}, \mid)$.
3. $\mathbb{N} \setminus \{0; 1\}$ n´a pas de plus petit élément. Sinon, si m convient, $m \mid 2$ et $m \mid 3$ donne $m \mid 1$, $m = 1$, ce qui est exclu.
4. $\mathbb{N} \setminus \{0; 1\}$ n´a pas de plus grand élément. Sinon, si M convient, $2M \notin \{0; 1\}$ et $2M \mid M$, ce qui conduit à $2Mq = M$ avec $q \in \mathbb{N}$. Aussi, puisque $M = 0$ est exclu, $2q = 1$. Impossible dans $\mathbb{N}$.
5. L´application $n \mapsto n\mathbb{Z}$ est bijective et strictement décroissante de $(\mathbb{N}, \mid)$ sur l´ensemble $\mathcal{I}$ des idéaux de $\mathbb{Z}$ muni de l´inclusion.
6. Un nombre premier est un élément minimal parmi les entiers naturels distincts de 1, et p est premier si, et seulement si, $p\mathbb{Z}$ est maximal dans l´ensemble $\mathcal{I} \setminus \{\mathbb{Z}\}$.

3.2 Lorsque la division euclidienne est incongrue ...

Dès l´école primaire, on peut déterminer l´heure du réveil si on sait que le coucher a lieu à 22 heures et que la nuit de sommeil est de 8 heures. Au lycée, on laisse de côté les aiguilles de pendule et on enroule sur un cercle une ficelle pour mesurer les angles orientés. On peut alors affirmer qu´un angle de $\frac{5\pi}{4}$ radians a pour mesure principale $-\frac{\pi}{4}$. En route vers les modules...

Définition :

Soit $n \in \mathbb{N}^*$.
On dit que $a, b \in \mathbb{Z}$ sont congrus modulo n et on écrit (notation introduite par Gauss, en 1801)

$$a \equiv b (\mathrm{mod}\, n) \quad \text{ou} \quad a \equiv b\,(n),$$

si n divise la différence $a - b$, ou encore $a - b \in n\mathbb{Z}$.
En particulier, $b \mid a \Leftrightarrow a \equiv 0\ (b)$.

Exemple : Les entiers pairs sont les éléments de $2\mathbb{Z}$ qui sont congrus à 0 modulo 2. Un nombre écrit dans le système décimal est congru, modulo 10, à son chiffre des unités.

Exercice 13 : (Roméo doute-t-il de l´amour de Juliette ?)
Roméo a une marguerite à 2183 pétales. Il les effeuille un à un en disant toujours dans le même ordre : «un peu», « beaucoup», «passionnément», «à la folie», «pas du tout». Quid de l´amour de Juliette ?

Exercice 14 : (Happy birthday)
Sachant que Roméo a épousé Juliette le premier janvier de l´année bissextile 2000 (qui était un samedi), déterminer le jour de la semaine pour leur $100^{\text{ème}}$ anniversaire de mariage.

Corrigé : Entre le $01-01-2000$ et le $01-01-2100$, les années bissextiles sont les $2000+4k$ où $0 \leqslant k \leqslant 24$ donc le nombre de jours N qui sépare les deux dates est $N = 100 \times 365 + 25$. On écrit

$$N = (7 \times 14 + 2) \times (7 \times 52 + 1) + 7 \times 3 + 4 \equiv 6\,(7).$$

Puisque les multiples de 7 ne modifient pas le nom du jour, le $01-01-2100$ sera un vendredi.

Pour aller plus loin : La congruence modulo $n > 0$, qui vérifie

$$\forall a, b, c \in \mathbb{Z}, \quad a \equiv a \text{ (réfléxivité)}, \quad a \equiv b \Rightarrow b \equiv a \text{ (symétrie)}, \quad a \equiv b \text{ et } b \equiv c \Rightarrow a \equiv c \text{ (transitivité)},$$

est une relation d´équivalence sur $\mathbb{Z}$. L´ensemble quotient est noté $\mathbb{Z}/n\mathbb{Z}$, ses éléments $\bar{k}, k \in \mathbb{Z}$.

Si $k \in \mathbb{Z}$, grâce à la division euclidienne (existence) de k par n, k est congru à l´un des nombres 0, ..., $n-1$. Réciproquement si $k \equiv r\,(n)$ avec $0 \leqslant r \leqslant n-1$, on a $k = nq + r$ et, par unicité du quotient et du reste dans la division euclidienne, r est le reste de k par n. Ainsi, tout nombre k est congru à l´un des nombres 0, ..., $n-1$ et un seul. On peut écrire :

$$\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., \overline{n-1}\} \quad \text{avec } card(\mathbb{Z}/n\mathbb{Z}) = n.$$

Théorème : *Congruences et opérations dans* $\mathbb{Z}$

Soit $n \in \mathbb{N}^*$, $a, a', b, b' \in \mathbb{Z}$ tels que $a \equiv a'\,(n)$ et $b \equiv b'\,(n)$. Alors, modulo n,

1. $a + b \equiv a' + b'$.
2. $ab \equiv a'b'$.

Pour aller plus loin : Les lois de composition interne

$$(\bar{k}, \bar{l}) \mapsto \overline{k+l} \quad \text{et} \quad (\bar{k}, \bar{l}) \mapsto \overline{k \times l}$$

sont ainsi correctement définies, et donnent à $\mathbb{Z}/n\mathbb{Z}$ une structure d´anneau commutatif.

Exemple : Pour tout $n \in \mathbb{N}$, $N = 3^{2n+1} + 2^{n+2}$ est divisible par 7. En effet, $N = 3 \times 9^n + 2^2 \times 2^n$ et, modulo 7, $N \equiv 3 \times 2^n + 4 \times 2^n = 2^n \times (3+4) \equiv 0$.

Question du jury :

1. Retrouver (et démontrer) les critères usuels de divisibilité (par 2, 5, 3, 9 et 11) pour un entier écrit en base 10.
2. Les nombres suivants sont-ils premiers : $10^{37}+1$, $10^{37}-1$? On pourra les regarder modulo 11 et 9.

Exercice 15 : Roméo a écrit son numéro de téléphone sur un papier pour Juliette. Mais il a plu sur le papier et un chiffre est illisible : 02 98 • 3 81 98. Juliette se souvient que Roméo lui a dit : «mon numéro de téléphone est divisible par mon nombre fétiche, le 11». Comment fait Juliette pour retrouver le chiffre manquant ?

Exercice 16 : On sait que l´entier 1221 (écriture en base 10) est divisible par 11 puisque la somme alternée de ses chiffres vaut $1-2+2-1=0$. Montrer, plus généralement, qu´en base $b \geqslant 2$, le nombre $N = 122\cdots21$ à $k \geqslant 3$ chiffres n´est pas premier.

Corrigé : On écrit

$$N = 1+2b+2b^2+\cdots+2b^{k-2}+b^{k-1} = 1+b+b^2+\cdots+b^{k-2}+b[1+b+\cdots+b^{k-2}] = [1+b+\cdots+b^{k-2}](1+b)$$

donc, avec $1+b>1$ et $1+b+\cdots+b^{k-2}>1$, N n´est pas premier.

Exercice 17 :

1. Soit $p>3$ premier. Alors p^2+2 est composé.
2. Si $p=a^2+b^2$ est un entier impair somme de deux carrés, alors $p-1$ est un multiple de 4.

Corrigé : On a $p \equiv 1\,(3)$ ou $p \equiv 2\,(3)$ donc $p^2 \equiv 1\,(3)$, $p^2+2 \equiv 0\,(3)$. Ainsi, $3 \mid (p^2+2)$ et p^2+2 n´est pas premier. Pour la deuxième question, on remarque qu´un carré est 0 ou 1 modulo 4, donc une somme de deux carrés est 0, 1 ou 2. Avec p impair, $p=a^2+b^2$ est 1 modulo 4, d´où le résultat.

Exercice 18 : Dans le groupe additif $\mathbb{Z}/7\mathbb{Z}$, la classe $\bar{1}$ est un générateur puisque, par additions répétées de $\bar{1}$, on construit tous les éléments de $\mathbb{Z}/7\mathbb{Z}$. Quels sont les autres générateurs de $\mathbb{Z}/7\mathbb{Z}$?

Exercice 19 : (D´après baccalauréat Session 1970 Aix-en Provence)

1. Si aucun des trois entiers a, b et c n´est divisible par 3, alors $a^2+b^2+c^2$ est un multiple de 3.
2. En remarquant que $999 = 27\times37$, montrer que pour tout entier positif n

$$10^{3n} \equiv 1\,(37)$$

puis trouver le reste de la division de $10^{10}+10^{20}+10^{30}$ par 37.

Exercice 20 : (Un tour de magie)
On considère le nombre premier $p=5$. Élever au carré, ajouter 11, diviser par 24. Quel est le reste dans la division ? Idem avec $p=31$. Idem avec un nombre premier de votre choix. Est-ce un hasard ?

Exercice 21 : (Vers le petit théorème de Fermat)

1. Pour $a \in \mathbb{Z}$, factoriser a^5-a en faisant apparaître 3 facteurs de degré 1 et 1 facteur de degré 2.
2. En déduire la congruence $a^5 \equiv a\,(5)$.

Exercice 22 : (Chiffre des unités de 2004^{2005}, adapté d´un exercice d´oral de Centrale)

1. Conjecturer les restes des puissances de 4 modulo 10.
2. Montrer, pour tout $n \in \mathbb{N}^*$,

$$\mathcal{P}(n) : \quad 4^{2n} \equiv 6\,(10) \quad \text{et} \quad 4^{2n+1} \equiv 4\,(10).$$

3. Conclure.

Exercice 23 : (Primalité de n^4+4^n, adapté d´un exercice d´oral de Polytechnique)
Soit un entier $n>5$.

1. Le nombre n^4+4^n est-il premier si on suppose que n est pair ?

2. On suppose que n n´est pas congru à 0 modulo 2 et modulo 5. Montrer que $n^4+4^n \equiv 0\,(5)$ puis conclure.

Exercice 24 : (Le scratch du F_5 par Euler)

1. Justifier les congruences $5\times 2^7 \equiv -1\,(641)$ et $-5^4 \equiv 2^4\,(641)$.
2. Montrer que $F_5 = 2^{2^5}+1 = 2^{32}+1$ n´est pas premier.

Commentaire : On admet que F_1, F_2, F_3 et F_4 sont premiers. En 1640, Fermat écrit à Mersenne que tous les nombres F_n, qui portent maintenant son nom, sont premiers. Euler contredit Fermat en 1732. À ce jour, on sait que F_n est composé pour $5 \leqslant n \leqslant 30$ et la conjecture sur les F_n s´est même retournée : on pense maintenant qu´aucun F_n n´est premier à partir de F_5.

Exercice 25 :

- Déterminer tous les entiers premiers p tels que $p+10$ et $p+14$ soient aussi premiers. On pourra envisager toutes les congruences possibles de p modulo 3.
- Déterminer tous les entiers premiers p tels que $4p^2+1$ et $6p^2+1$ soient aussi premiers. On pourra envisager toutes les congruences possibles de p modulo 5.
- Déterminer tous les entiers premiers p tels que $p+2$, $p+6$, $p+8$, $p+12$ et $p+14$ soient aussi premiers. On pourra envisager toutes les congruences possibles de p modulo 5.

4 Diviseurs communs

4.1 Les cavaliers de la (petite) reine

- Anne, ma soeur Anne, ne vois-tu rien venir ?
- Je vois deux cavaliers qui viennent de ce côté mais ils sont encore loin.

Pour aller plus loin : Voici une présentation rapide des notions de *pgcd* et *ppcm*. Pour a et b entiers relatifs, via la division euclidienne, les idéaux $a\mathbb{Z}+b\mathbb{Z}$ et $a\mathbb{Z}\cap b\mathbb{Z}$ s´écrivent (de façon unique) $d\mathbb{Z}$ et $m\mathbb{Z}$ $(d,m\in\mathbb{N})$. On vérifie que :

1. $d\mathbb{Z} = a\mathbb{Z}+b\mathbb{Z}$ est le plus petit idéal de $\mathbb{Z}$ qui contient $a\mathbb{Z}$ et $b\mathbb{Z}$.
2. $m\mathbb{Z} = a\mathbb{Z}\ \cap\ b\mathbb{Z}$ est le plus gros idéal de $\mathbb{Z}$ contenu dans $a\mathbb{Z}$ et $b\mathbb{Z}$.

Par dualité,

1. l´entier d est le plus grand élément au sens de $|$ parmi les diviseurs communs de a et b : il est appelé Plus Grand Commun Diviseur de a et b (notation : $d = a\wedge b$ ou $d = pgcd(a,b)$).
2. l´entier m est le plus petit élément (pour $|$) parmi les multiples de a et b : il est appelé Plus Petit Commun Multiple de a et b ($m = a\vee b$ ou $m = ppcm(a,b)$).

Lorsque $d=1$, on dit que a et b sont premiers entre eux et sur un plateau :

$$\exists u,v\in\mathbb{Z},\ au+bv = 1 \text{ (Relation de Bézout).}$$

Voici une présentation plus pédestre qui repose aussi sur la division euclidienne.

Définition :

Soit $a,b\in\mathbb{N}$ non tous deux nuls.

1. L´ensemble $\mathcal{D}_{a,b}$ des diviseurs positifs communs de a et b est une partie de $(\mathbb{N},\leqslant)$ non vide $(1\in\mathcal{D}_{a,b})$ et majorée par $\min(a,b)$ donc $\mathcal{D}_{a,b}$ admet un plus grand élément pour $\leqslant$. On l´appelle le plus grand commun diviseur de a et b et on le note $pgcd(a,b)$.
2. L´ensemble $\mathcal{M}_{a,b}$ des multiples >0 communs de a et b est une partie de $(\mathbb{N},\leqslant)$ non vide $(ab\in\mathcal{M}_{a,b})$ et minorée par $\max(a,b)$ donc $\mathcal{M}_{a,b}$ admet un plus petit élément pour $\leqslant$. On l´appelle le plus petit commun multiple de a et b et on le note $ppcm(a,b)$.
3. Lorsque le *pgcd* de a et b vaut 1, on dit que a et b sont premiers entre eux et on note $a\wedge b = 1$.

Question du jury : :

1. Pourquoi ne peut-on pas définir $pgcd(0,0)$?
   Pour $a, b > 0$, que valent $pgcd(a,0)$, $pgcd(a,1)$ et $pgcd(a,b)$ lorsque $b \mid a$?
2. Primalité vs primalité relative : Peut-on avoir a et b premiers entre eux avec a et b non premiers ?

Exercice 26 : (Une batterie d´entiers premiers entre eux)
Pour p premier et $a \in \mathbb{Z}$, $a \wedge p = 1$ si, et seulement si, p ne divise pas a.

Corrigé : Si a et p sont premiers entre eux, on ne peut avoir $p \mid a$ sous peine de voir $pgcd(a,p) \geqslant p > 1$. Réciproquement, on suppose que p ne divise pas a. Soit n un diviseur commun de a et p. Puisque $n \mid p$ et p premier, n vaut 1 ou p. Puisque p ne divise pas a, nécessairement $n = 1$, ce qui montre que $\mathcal{D}_{a,p} = \{1\}$ et $pgcd(a,p) = 1$.

Question du jury : :

1. Qu´est-ce que le crible d´Eratosthène ?
2. On choisit 100 nombres premiers entre eux deux à deux compris strictement entre 1 et 199^2. Pourquoi y-a-t-il nécessairement dans cette liste un nombre premier ?

Réponse :

1. On veut les entiers premiers inférieurs à un certain n. On écrit tous les entiers de 2 à n. On marque tous les multiples de 2 sauf 2, puis on répète la manipulation avec le premier nombre plus grand que 2 encore présent, et ainsi de suite. Il est inutile de poursuivre le marquage à partir du premier nombre non marqué $k > \sqrt{n}$. En effet, son premier multiple non marqué est $k \times k > n$.
2. Si les 100 nombres choisis sont composés, chacun a au moins un diviseur premier strictement inférieur à 199. Par le crible d´Eratosthène, après avoir éliminé les multiples de 2 (autres que 2) au nombre de 98 et les multiples de 3, il y a moins de 100 nombres premiers strictement inférieur à 199, donc au moins deux des 100 nombres choisis ont un diviseur premier en commun. Contradiction !

Propriété : (Caractérisation du *pgcd*)

Soit $a, b \in \mathbb{N}$ non tous deux nuls, $d \in \mathbb{N}$. On envisage les trois énoncés :

i) $d \mid a$, $d \mid b$ et, pour tout diviseur δ commun de a et b, $\delta \mid d$.

ii) L´entier d est le *pgcd* de a et b, i.e le plus grand élément de $\mathcal{D}_{a,b}$ pour $\leqslant$.

iii) On peut écrire $a = da'$, $b = db'$ avec $a', b' \in \mathbb{N}$ et $a' \wedge b' = 1$.

Pour aller plus loin : La proposition $i)$ peut se traduire par

« d est, pour $|$, le plus grand élément de $\mathcal{D}_{a,b}$»

ou encore

«d est un minorant de $\{a,b\}$ pour l´ordre $|$ et d est supérieur à tout minorant de $\{a,b\}$»

c-à-d

« d est, pour $|$, la borne supérieure de la partie $\{a,b\}$ de $\mathbb{N}$.»

Sans... : On a $i) \Rightarrow ii) \Rightarrow iii)$.
Avec Bézout (cf infra) : On a $iii) \Rightarrow i)$.

Preuve : instructive, laissée au lecteur. □

4.2 Allez Bizut montre nous tes ..., allez Bézout montre nous ton ...

Soit $a, b \in \mathbb{N}$ non tous deux nuls et $\delta \in \mathbb{N}$. Puisque $\delta\mathbb{Z}$ est stable par "combinaison d´anneau", l´entier δ est un diviseur commun de a et b si, et seulement si, δ est un diviseur commun de $a - b$ et b.

Exercice 27 :
En divisant 6732 et 564 par un même nombre b, on trouve des restes de 24 et 18. Quel peut être b ?

Corrigé : Avec les données, on vérifie que b est un diviseur commun de $6732 - 24 = 6708$ et $564 - 18 = 546$, donc est un diviseur de $d = pgcd(6708, 546)$. Le lecteur courageux montre, par l´algorithme des différences, que $d = 78$. Ainsi, $b \mid 78$ avec la contrainte $b > 24$, ce qui donne $b = 26$, ou 39 ou 78.

Propriété : (Vers l´algorithme d´Euclide)

Soit $a, b \in \mathbb{N}$, $b \neq 0$. On effectue la division euclidienne de a par b :

$$a = bq + r, \quad q, r \in \mathbb{N}, \quad 0 \leqslant r < b.$$

Les diviseurs communs de a et b sont exactement les diviseurs communs de b et $r = a - bq$:

$$\mathcal{D}_{a,b} = \mathcal{D}_{b,r}.$$

Aussi, le *pgcd* de a et b est le *pgcd* de b et r.

Algorithme :
- Données : a, b dans $\mathbb{N}$.
- Variables : $r, s, t \in \mathbb{N}$
- Initialisation : $r = \max(a, b)$, $s = \min(a, b)$ et $t = 0$.
- Début boucle : Tant que $s > 0$, faire
- Corps de la procédure :
  - $t = reste\ de\ r\ par\ s$
  - $r = s$
  - $s = t$
- Fin de boucle : Renvoyer r.

La procédure renvoie le dernier reste non nul. C´est r ! Ce n´est pas s car, à la fin, $s = 0$.

Question du jury : : Qu´est-ce qui garantit la fin de boucle ?

Réponse : Descente infinie de Fermat : Dans $\mathbb{N}$, on ne peut pas construire une suite strictement décroissante d´entiers naturels (suite des restes)... sans être confronté à une contradiction.

Exemple : On applique l´algorithme d´Euclide pour avoir $pgcd(584, 142)$. On a $584 = 142 \times 4 + 16$ donc $pgcd(584, 142) = pgcd(142, 16)$. Nouvelle boucle : $142 = 16 \times 8 + 14$ donc

$$pgcd(584, 142) = pgcd(142, 16) = pgcd(16, 14).$$

Encore un tour : $16 = 14 \times 1 + 2$ donc

$$pgcd(584, 142) = pgcd(142, 16) = pgcd(16, 14) = pgcd(14, 2).$$

Enfin, $14 = 2 \times 7 + 0$. Le dernier reste non nul de l´algorithme est $pgcd(584, 142) = 2$.

Théorème : (Théorème de Bézout)

Soit $a, b \in \mathbb{N}$, non tous deux nuls et $d \in \mathbb{N}$. Les propositions suivantes sont équivalentes :

1. d est le pgcd de a et b
2. $d \mid a$, $d \mid b$ et il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$.

En particulier, a et b sont premiers entre eux ($pgcd(a, b) = 1$) si, et seulement si, a et b sont «Bézout entre eux» :

il existe $u, v \in \mathbb{Z}$, $au + bv = 1$.

Question du jury : :

1. Y-a-t-il unicité du couple (u, v) ?
2. Vrai ou faux : Deux entiers naturels consécutifs sont premiers entre eux.

Réponse :

1. $au + bv = a(u + kb) + b(v - ka)$, pour tout $k \in \mathbb{Z}$.
2. Pour $n \in \mathbb{N}$, n et $n + 1$ sont «Bézout entre eux» puisque $(-1)n + 1(n + 1) = 1$, donc sont premiers entre eux.

Preuve : On montre que 2 $\Rightarrow$ 1. Si il existe $u, v \in \mathbb{Z}$ tels que $d = au + bv$, tout diviseur commun de a et b divise aussi d et, comme d est par ailleurs un diviseur commun de a et b, d est bien le $pgcd(a, b)$. Pour l´autre implication, on suivra

Algorithme : ***(d´Euclide étendu)***

- Données : $a, b \geqslant 0$ non tous deux nuls.
- Initialisation :
  - $r_0 = a$
  - $r_1 = b$
  - $u_0 = 1$
  - $u_1 = 0$
  - $v_0 = 0$
  - $v_1 = 1$

  On a les relations $r_0 = u_0a + V_0b$ et $r_1 = u_1a + v_1b$ à l´entrée de boucle.
- Tant que $R_1 > 0$, faire
  - $q =$ quotient de r_0 par r_1
  - $r =$ reste de r_0 par r_1
  - $u = u_0 - qu_1$ et $v = v_0 - qv_1$
  - $r_0 = r_1$
  - $r_1 = r$
  - $u_0 = u_1$
  - $u_1 = u$
  - $v_0 = v_1$
  - $v_1 = v$

  Si, à l´entrée de boucle, on a $r_0 = u_0a + V_0b$ et $r_1 = u_1a + v_1b$, on les a aussi à la sortie de boucle.
- Fin de boucle.

□

Propriété : (Applications fondamentales de l´identité de Bézout)

1. $c \mid ab$ et $c \wedge a = 1 \Rightarrow c \mid b$ (Lemme de Gauss)
2. Si p est premier, alors $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$. (Lemme d´euclide, $p\mathbb{Z}$ idéal premier de $\mathbb{Z}$)

   Pour aller plus loin : Sous la condition «p premier», l´idéal $p\mathbb{Z}$, s´il contient un produit, contient l´un des deux facteurs. Ceci est encore équivalent à l´intégrité de l´anneau quotient $\mathbb{Z}/p\mathbb{Z}$. La réciproque est fausse, avec $0\mathbb{Z}$ (idéal premier) et 0 (nombre non premier).

3. $a \mid c, b \mid c, a \wedge b = 1 \Rightarrow ab \mid c$.

Question du jury :

1. Deux candidats au CAPES se présentent devant le même jury. Le premier, qui a la tête haute, compte les membres du jury et affirme que leur nombre ne divise pas 7. Le second (moins sur de lui) compte les jambes de ses «bourreaux» attablés et affirme que le nombre obtenu est un multiple de 7. Est-ce possible ?
2. Peut-on relever le défi suivant : écrire en base 10 un carré parfait ($N = n^2$) avec exactement 10 chiffres 0, 10 chiffres 1 et 10 chiffres 2.
3. Existe-t-il une factorielle à 5 zéros exactement dans son écriture décimale ?

Réponse :

1. Soit $n > 1$ le nombre de membres du jury. On a $7 \mid 2n$ et $2 \wedge 7 = 1$ donc, par le lemme de Gauss, $7 \mid n$.
2. Si N convient, on a $3 \mid N$ car la somme des chiffres de N est $30 \in 3\mathbb{Z}$. Par le lemme d´Euclide, $3 \mid n$. Ainsi, $9 \mid n^2$, ce qui est impossible puisque $30 \notin 9\mathbb{Z}$.
3. Si $n!$ convient, $10^5 \mid n!$ donc $5^5 \mid n!$, donc $n > 24$ puisque 24! ne contient que 4 facteurs 5 à pêcher dans 5, 10, 15 et 20. D´autre part, pour $n \geqslant 25$, $n!$ contient au moins 6 facteurs 5 puisque $25 = 5^2$. Avec en plus au moins 6 facteurs 2, puisque $2^6 \wedge 5^6 = 1$, $n!$ est divisible par 10^6 et se termine donc par au moins 6 zéros.

Exercice 28 : Pour $a, b \in \mathbb{N}$, $pgcd(a, b) = 1$ si, et seulement si, $pgcd(a + b, ab) = 1$.

Corrigé : Si $pgcd(a+b, ab) = 1$, soit d un diviseur commun de a et b. On a $d \mid a+b$ et $d \mid ab$ donc $d \mid 1$, donc a et b sont premiers entre eux. Si $pgcd(a + b, ab) \neq 1$, soit d un diviseur premier commun de $a + b$ et ab. On a alors $d \mid a$ ou $d \mid b$. Si $d \mid a$, puisque $d \mid a + b$, d divise aussi b donc a et b ne sont pas premiers entre eux.

Exercice 29 : (Nombres de Fermat et infinité de nombres premiers par Pólya)
Les nombres de Fermat sont définis par $F_n = 2^{2^n} + 1$ où $n \in \mathbb{N}$.

1. Montrer que, pour $n, k \in \mathbb{N}$, F_n divise $F_{n+k} - 2$.
2. En déduire, en considérant un diviseur q commun de F_n et F_{n+k}, que $F_n \wedge F_{n+k} = 1$[1].
3. Conclure que les nombres premiers sont en nombre infini.

Propriété : (Caractérisation du *ppcm*)

Soit $a, b \in \mathbb{N}$, non tous deux nuls et $m \in \mathbb{N}$. On envisage les énoncés :

i) $a \mid m$, $b \mid m$ et, pour tout multiple μ commun de a et b, $m \mid \mu$.

ii) m est le *ppcm* de a et b, i.e le plus petit élément de $\mathcal{M}_{a,b}$ pour $\leqslant$.

1. On a $i) \Rightarrow ii)$.
2. Si, de plus, d est le *pgcd* de a et b, alors $ab = dm$.
3. On a $ii) \Rightarrow i)$.

[1] Variante : Considérer un diviseur premier p (cf infra) commun à F_n et à F_{n+k}, et aboutir à une contradiction avec les deux congruences $2^{2^n} \equiv -1\,(p)$ et $2^{2^{n+k}} = (2^{2^n})^{2^k} \equiv -1\,(p)$.

Preuve : L´implication $i) \Rightarrow ii)$ vient du fait que deux entiers naturels rangés dans un ordre pour la divisibilité sont rangés dans le même ordre pour $\leqslant$.

On relie à présent $m = ppcm(a,b)$ et $d = pgcd(a,b)$. Soit $a', b' \in \mathbb{N}$ tels que $a = da'$, $b = db'$ et $a' \wedge b' = 1$. On montre que $m = da'b'$ (grâce à $i) \Rightarrow ii)$) de sorte que $md = da'b'\ d = ab$. Soit μ un multiple commun de a et b. On écrit

$$\mu = a\alpha = b\beta = da'\alpha = db'\beta \quad \text{donc} \quad a'\alpha = b'\beta.$$

Puisque $a' \wedge b' = 1$, par le lemme de Gauss : $a' \mid \beta$. Avec des notations évidentes, $\beta = a'c$ donc $\mu = db'\ \beta = db'\ a'c$, $da'b' \mid \mu$. Enfin, $da'b' = ab' = a'b$ est multiple commun de a et b, ce qui donne $m = da'b'$.

Si on suppose maintenant que m est le plus petit élément de $\mathcal{M}_{a,b}$, on a clairement $a \mid m$ et $b \mid m$. Pourquoi m divise-t-il tout multiple commun μ de a et b ? On reprend ce qui précède et on conclut. □

Propriété :

Soit $n \in \mathbb{N}$, $n \neq 0$. Pour $k \in \mathbb{N}$, on a les équivalences :

1. Il existe $l \in \mathbb{Z}$ (et même dans $\mathbb{N}$) tel que $lk \equiv 1\,(n)$.
2. Les entiers k et n sont premiers entre eux.
3. $\forall x \in \mathbb{Z},\ \exists 0 \leqslant L \leqslant n-1,\ x \equiv Lk\,(n)$.

Pour aller plus loin : Les éléments inversibles de $(\mathbb{Z}/n\mathbb{Z}, +, \times)$ sont exactement

1. les classes de congruences $\bar{k}$, avec $0 \leqslant k \leqslant n-1$ et $k \wedge n = 1$.
2. les classes $\bar{k}$ qui engendrent le groupe additif $(\mathbb{Z}/n\mathbb{Z}, +)$.

Aussi, si p est premier, alors tout élément non nul de l´anneau $\mathbb{Z}/p\mathbb{Z}$ est inversible :

$\mathbb{Z}/p\mathbb{Z}$ est un corps, en particulier est un anneau intègre.

4.3 Une équation diophantienne incontournable

Un champs (très grand) est modélisé par le plan qu´on munit d´un repère $(O, \vec{i}, \vec{j})$. En chaque point à coordonnées entières autre que O, est posté un chasseur. On suppose que les chasseurs ne tirent qu´à la verticale.

Question du jury : Un oiseau part de O et vole en ligne droite. Peut-on lui trouver une trajectoire rectiligne salutaire ?

Un oiseau vole selon la droite Δ d´équation $ax + by = c$ où $a, b \in \mathbb{Z}$ sont non nuls et $c \in \mathbb{Z}$. Que se passe-t-il ?

Le problème posé est la résolution dans $\mathbb{Z}^2$ de l´équation

$$\mathcal{E} \ :\ ax + by = c \text{ d´inconnues } x, y \in \mathbb{Z}.$$

Pas 1 : L´égalité $ax + by = c$ fait penser à la relation de Bézout. Aussi, on introduit «naturellement» le *pgcd* d de a et b. Il existe alors $a', b' \in \mathbb{Z}^2$ premiers entre eux tels que $a = da'$ et $b = db'$. Pour $(x, y) \in \mathbb{Z}^2$, $ax + by = c \Rightarrow da'x + db'y = c \Rightarrow d \mid c$ donc la condition $d \mid c$ est nécessaire à l´existence de solutions pour $\mathcal{E}$. Par exemple, la droite d´équation $3x + 6y = 5$ est une bonne trajectoire pour l´oiseau.

On suppose désormais que $d = pgcd(a,b)$ divise c, ce qui ramène le problème à la résolution dans $\mathbb{Z}^2$ de l´équation (encore notée $\mathcal{E}$) $ax + by = c$ avec $a \wedge b = 1$.

pas 2 : Par le théorème de Bézout, il existe $(u, v) \in \mathbb{Z}^2$ tels que $au + bv = 1$ donc $auc + bvc = c$, donc $M_0(x_0 = uc, y_0 = vc)$ est une solution particulière de $\mathcal{E}$.

Pas 3 : Pour $(x, y) \in \mathbb{Z}^2$ et $M(x, y)$, $ax + by = c$ si, et seulement si, $ax + by = ax_0 + by_0$, ou encore $a(x - x_0) = -b(y - y_0)$. Géométriquement, $ax + by = c$ revient à dire successivement que $M \in \Delta$, que $\overrightarrow{M_0M}$ est un vecteur directeur de Δ dont un vecteur directeur notoire est $\overrightarrow{u}$ $(-b, a)$.

Si (x, y) est solution de $\mathcal{E}$, $b \mid a(x - x_0)$ avec $a \wedge b = 1$ donc, par le lemme de Gauss, il existe $k \in \mathbb{Z}$ tel que $x - x_0 = kb$, $x = x_0 + kb$. Par substitution, il vient $y - y_0 = -ka$, $y = y_0 - ka$. Réciproquement, tout couple $(x_0 + kb, y_0 - ka)$ avec $k \in \mathbb{Z}$ est solution de $\mathcal{E}$.

Exercice 30 : Donner les solutions entières de $504x + 1188y = 144$.

Autre vision de l´affaire :
Si (x, y) est une solution de $\mathcal{E}$, on a $ax \equiv c\,(b)$ (ou $\overline{ax} = \overline{c}$ dans $\mathbb{Z}/b\mathbb{Z}$) et $by = c\,(a)$. On ramène donc l´équation $\mathcal{E}$ au système de congruences

$$\begin{cases} ax \equiv c\,(b) \\ by = c\,(a) \end{cases}.$$

Puisque a et b sont premiers entre eux, il existe $u, v \in \mathbb{Z}$ tels que $ua + vb = 1$; donc

1. $ua \equiv 1\,(b)$ ou, en langage savant, $\overline{u}$ est l´inverse de $\overline{a}$ dans $\mathbb{Z}/b\mathbb{Z}$.
2. $vb \equiv 1\,(a)$.

Ainsi, $ua\,x \equiv uc\,(b)$, ce qui assure l´existence de $k \in \mathbb{Z}$ tel que $x = uc + kb$. Le même travail modulo a donne : $\exists l \in \mathbb{Z},\ y = vc + la$. Puique $ax + by = c$, il vient $a(uc + kb) + b(vc + la) = c$ donc $c(ua + vb - 1) + ab(k + l) = 0$, $ab(k + l) = 0$, $k = -l$ puisque $a \neq 0$ et $b \neq 0$. Réciproquement, tout couple $(uc + kb, vc - ka)$ est solution de $\mathcal{E}$.

Exercice 31 : Travailler plus ...
Un enseignant donne des cours particuliers de mathématiques sur 27 semaines à raison de 35 heures par semaine. Il travaille avec 2 types d´élèves : les élèves de terminale S nécessitent 15 heures de cours individuels pour se remettre au niveau alors que les élèves de première S 18 heures. Le prix horaire est de 25 euros pour un élève de terminale et 30 euros pour un élève de première. Quelle est la somme maximale perçue par l´enseignant ?

Corrigé : Si x et y désignent le nombre d´élèves de TS et de 1S, on a $15x + 18y = 27 \times 35 = 3 \times 315$ donc

$$5x + 6y = 315\ (E).$$

Pour (x, y) solution de (E), modulo 6, $5x \equiv 315\ (6)$, $-x \equiv 6 \times 52 + 3 \equiv 3\ (6)$, $x \equiv -3 \equiv 3\ (6)$. Ainsi, avec la contrainte $15x \leqslant 27 \times 35 = 945$, on a $x \in \{3; 9; 15; 21; 27; 33; 39; 45; 51; 57; 63\}$. Pour trouver le bon y correspondant, on peut réduire (E) modulo 5 : $6y \equiv y \equiv 0\ (5)$ et, avec la contrainte $18 \times y \leqslant 945$, on a $y \in \{0; 5; \cdots; 50\}$. Réciproquement, $(3; 50)$, $(9; 45)$, $(15; 40)$, $(21; 35)$, $(27; 30)$, $(33; 25)$, $(39; 20)$, $(45; 15)$, $(51; 10)$, $(57; 5)$ et $(63; 0)$ sont solutions de (E). Le revenu maximal est $3 \times 15 \times 25 + 50 \times 18 \times 30$ euros.

5 Quelques joyaux de la reine

5.1 Décomposition en facteurs premiers

Commentaire : Lorsqu´on casse 60 jusqu`à «une» décomposition en nombres premiers, on peut commencer par $60 = 6 \times 10$ ou $60 = 4 \times 15$ ou $\cdots$, et on sait, par expérience, qu´en continuant le procédé, on obtiendra une décomposition achevée indépendante des choix initiaux effectués. Gauss dit : «on suppose à tort tacitement que cette décomposition ne soit possible que d´une seule manière.»

Théorème : (Théorème fondamental de l´arithmétique)

Tout entier $n \geqslant 2$ peut s´écrire comme un produit de facteurs premiers, et ce, de façon unique (à l´ordre près des facteurs).

Exercice 32 : On note $\sqrt{36\mathbb{Z}}$ l´ensemble $\{x \in \mathbb{Z} \setminus \exists n \in \mathbb{N}^*, x^n \in 36\mathbb{Z}\}$. Montrer que $6\mathbb{Z} \subset \sqrt{36\mathbb{Z}}$ et, par contraposée, $\sqrt{36\mathbb{Z}} \subset 6\mathbb{Z}$. Que vaut $\sqrt{11\mathbb{Z}}$?

Exercice 33 : Montrer que $(n, m) \mapsto 2^n(2^m + 1) - 1$ est une bijection entre $\mathbb{N} \times \mathbb{N}$ et $\mathbb{N}$.

Exercice 34 : Montrer qu´il y a au moins autant de nombres irrationnels que de nombres premiers. On pourra considérer $\sqrt{p}$ pour p premier.

Question du jury :

1. Donner des nombres irrationnels célèbres.
2. Peut-on mesurer autrement l´encombrement des nombres irrationnels dans $\mathbb{R}$?

Réponse :

1. Les nombres π (J.H Lambert, 1761) et e (Euler) sont des irrationnels notoires.
2. $\mathbb{R} \setminus \mathbb{Q}$ est une partie dense de $\mathbb{R}$ (topologie) et non dénombrable.

5.2 Petit théorème de Fermat

Théorème : (Petit théorème de Fermat énoncé en 1640, démontré par Euler en 1736)

Pour p premier et $a \in \mathbb{Z}$, on a : $a^p \equiv a\,(p)$. Si p ne divise pas a, la congruence de Fermat devient :

$$a^{p-1} \equiv 1\,(p).$$

Preuve : Pour $a \wedge p = 1$, on note $\Pi_{a,p}$ la multiplication par a modulo p. Avec le lemme de Gauss, on montre :

$$\forall k, k' \in [[1, p-1]], k \neq k' \quad ka \neq k'a\,(p),$$

ce qui fait de $\Pi_{a,p}$ une injection et donc une permutation de $\mathbb{Z}/p\mathbb{Z}$. On a alors $(p-1)! \equiv a2a...(p-1)a$ d´où : $(a^{p-1} - 1)(p-1)! \equiv 0\,(p)$. Par ailleurs, le nombre premier p ne divise aucun des facteurs de $(p-1)!$ donc est premier avec $(p-1)!$. Il vient, toujours avec le lemme de Gauss, $a^{p-1} \equiv 1\,(p)$. □

Exercice 35 : (Une autre preuve)
Soit p un nombre premier.

1. Pour $1 \leqslant k \leqslant p-1$, p divise le coefficient binomial C_p^k.
2. Pour $a, b \in \mathbb{Z}$, $(a+b)^p \equiv a^p + b^p\ (p)$.
3. Par récurrence sur $a \in \mathbb{N}$, $a^p \equiv a\ (p)$.

Question du jury : Vrai ou faux : Le nombre $a = 30^{239} + 239^{30}$ n´est pas un nombre premier.

Réponse : On réduit a modulo 31.

Exercice 36 : Soit $n \geqslant 2$. On pose $a = n^5 - n$. Montrer que $n^3 - n \mid a$ puis que $30 \mid a$.

Corrigé : D´après le petit théorème de Fermat, $5 \mid a$ et, avec $a = n(n^4-1) = n(n^2-1)(n^2+1) = (n^3-n)(n^2+1)$, $3 \mid a$. Puisque 3 et 5 sont premiers entre eux, $15 \mid a$. Enfin, $a = n(n-1)\,(n+1)(n^2+1)$ où n et $n-1$ sont des entiers consécutifs, donc $2 \mid a$. On conclut que $30 \mid a$ puisque 2 et 15 sont premiers entre eux.

Exercice 37 : Pour $n, m \in \mathbb{N}$, $mn(m^{60} - n^{60})$ n´est pas premier.

Corrigé : On écrit $mn(m^{60} - n^{60}) = m^{61}n - mn^{61} = (m^{61} - m)n - m(n^{61} - n)$ et, avec le petit théorème de Fermat, $61 \mid mn(m^{60} - n^{60})$.

Exercice 38 : On considère la suite définie pour $n \geqslant 1$ par $a_n = 2^n + 3^n + 6^n - 1$. Montrer que tout nombre premier divise au moins l´un des a_n.

Corrigé : On a $a_2 = 48$ donc 2 et 3 divisent a_2. Pour $p \geqslant 5$ premier, on évalue $6a_{p-2}$ et on conclut avec le petit théorème de Fermat.

5.3 Théorème de Wilson

Théorème : (Théorème de Wilson)

Pour $p \in \mathbb{N}$, p est premier si, et seulement si, $(p-1)! \equiv -1\,(p)$.

Preuve : On envisage sur $(\mathbb{Z}/p\mathbb{Z})^*$ la relation d´équivalence

$$x \mathcal{R} y \Leftrightarrow y \in \{x, x^{-1}\}.$$

Quelles sont les classes réduites à un singleton ? On a : $x \equiv x^{-1}\,(p) \Leftrightarrow x^2 \equiv 1 \Leftrightarrow (x-1)(x+1) \equiv 0$, et par intégrité de $\mathbb{Z}/p\mathbb{Z}$, $x \equiv 1$ ou $x \equiv -1 \equiv p-1$. Ainsi, en regroupant les facteurs par classe dans le produit $(p-1)!$, on a : $(p-1)! \equiv -1\,(p)$. □

Exercice 39 : (Euclide pour modèle)

Commentaire : Les nombres premiers strictement plus grands que 2, qui sont en quantité infinie d´après Euclide, sont tous impairs, donc de la forme $2k+1$, $k \in \mathbb{N}^*$. Plus généralement, existe-t-il des nombres premiers dans une suite $ak+b$? La première remarque (facile à vérifier) est que, si tel est le cas, les coefficients a et b sont nécessairement premiers entre eux. Le théorème de la progression arithmétique, dû à Dirichlet, affirme que, si $a \wedge b = 1$, alors il existe une infinité de nombres premiers congrus à b modulo a.

Soit $p > 2$ premier.

1. Vérifier que $\frac{p-1}{2} \in \mathbb{N}$.
2. Donner les congruences possibles de p modulo 4. Dans chaque cas, préciser la parité de $\frac{p-1}{2}$.
3. (a) On suppose que $p \equiv 1\,(4)$. Montrer que $\forall 1 \leqslant k \leqslant \frac{p-1}{2},\ \frac{p-1}{2} + k \equiv -\frac{p-1}{2} + (k-1)\,(p)$. En déduire, avec la congruence de Wilson, que -1 est un carré modulo 4.
   (b) On suppose que $p \equiv 3\,(4)$. Montrer que -1 n´est pas un carré modulo p. On pourra raisonner par l´absurde (en écrivant $-1 \equiv x^2\,(p),\ x \in \mathbb{Z}$) et obtenir une contradiction en évaluant x^{p-1} modulo p.
4. Pour montrer qu´il existe une infinité de nombres premiers de la forme $4k+1$, on raisonne par l´absurde en envisageant la liste $\{p_1, \cdots, p_n\}$ des nombres premiers congrus à 1 modulo 4. On pose
$$M = 4(p_1 \cdots p_n)^2 + 1.$$
   (a) Pourquoi M n´est-il pas premier ?
   (b) Soit p un diviseur premier de M. Vérifier que $p \neq 2$, puis que $p \equiv 1\,(4)$.
   (c) Pourquoi -1 est-il un carré modulo 4 ? Conclure.
5. Pour montrer qu´il existe une infinité de nombres premiers de la forme $4k+3$, on raisonne par l´absurde en envisageant la liste $\{p_1, \cdots, p_n\}$ des nombres premiers congrus à 3 modulo 4. On pose $M = 4p_1 \cdots p_n - 1$.
   (a) Pourquoi M n´est-il pas premier ?
   (b) A-t-on : $2 \mid M$?
   (c) Pourquoi M possède-t-il au moins un diviseur premier congru à 3 modulo 4 ?
   (d) Soit p un tel diviseur premier de M. Pourquoi a-t-on : $p > p_n$? Conclure.

6 Pour aller plus loin

RÉFÉRENCE : Cours d´algèbre, chapitre 2, D. Perrin, collection de l´ENS des Jeunes Filles, 1994.

L´arithmétique est l´étude de la divisibilité et on peut parler de divisibilité et de diviseurs dès qu´on est en présence d´un anneau. Soit donc $\mathcal{Z}$ un anneau, commutatif (pour éviter les diviseurs à gauche ... en sortant de l´ascenseur), unitaire (i.e possédant un neutre 1 pour la multiplication) et non nul ($1 \neq 0$). On rappelle que la relation binaire $\mid$ est réflexive et transitive.

6.1 Éléments marginaux de $\mathcal{Z}$

Deux types d´éléments de $\mathcal{Z}$ sont «marginaux» pour la divisibilité :

1. le neutre 0 de l´addition puisque $a \mid 0$ pour tout a de $\mathcal{Z}$. Pour $a \neq 0$, on a toujours $a \times 0 = 0$ et, si de plus $ab = 0$ avec $b \neq 0$, on dit que a et b sont des diviseurs (sous-entendu «spéciaux») de 0. En particulier, tout nilpotent non nul (comme $\bar{2}$ dans $\mathbb{Z}/8\mathbb{Z}$) est un diviseur de 0.
2. les inversibles ou les unités de $\mathcal{Z}$ dont l´ensemble-groupe est noté $U(\mathcal{Z})$.
   (a) Une unité u divise tout $a \in \mathcal{Z}$ puisque $a = u\, u^{-1}a$.
   On dit que u est un diviseur trivial de a.
   (b) Si $a, d, m \in \mathcal{Z}$ et si $u \in U(\mathcal{Z})$, alors $d \mid a \Leftrightarrow d \mid ua$ et $m \in a\mathcal{Z} \Leftrightarrow m \in ua\mathcal{Z}$ de sorte que les ensembles $\mathcal{D}_a$ des diviseurs de a et $a\mathcal{Z}$ des multiples de a coincident, pour toute unité u, avec $\mathcal{D}_{ua}$ et $ua\mathcal{Z}$.

   Exemple :
   (a) Les entiers 1 et -1 sont des inversibles de $\mathbb{Z}$. Si $x \neq 0$ vérifie $\mid x \mid > 1$, alors $x^2 = \mid x \mid^2 > 1$ donc les inversibles de $\mathbb{Z}$ sont exactement 1 et -1.
   (b) Si $\mathcal{Z}$ est l´anneau $\mathbb{Z}[i]$ de Gauss, $U(\mathcal{Z})$ est le groupe $\{1, i, -1, -i\}$ des racines quatrièmes de 1 dans $\mathbb{C}$. En effet, pour $u = m + in \in \mathcal{Z}$, on a les équivalences :
   – $u \in \mathcal{U}(\mathcal{Z})$
   – $\exists (p, q) \in \mathbb{Z}^2 \quad 1 = (mp - nq) + i(np + mq)$
   – $\exists (p, q) \in \mathbb{Z}^2 \quad \begin{cases} 1 = (mp - nq) \\ 0 = np + mq \end{cases}$ (système linéaire aux inconnues p et q, de déterminant $m^2 + n^2$)
   – $\frac{m}{m^2+n^2} \in \mathbb{Z}$ et $\frac{-n}{m^2+n^2} \in \mathbb{Z}$ (formules de Cramer)
   – $m^2 + n^2 = 1$.
   (c) Si P est un polynôme constant de $\mathcal{Z}[X]$ avec $P = a \in U(\mathcal{Z})$, alors P est inversible (et P^{-1} est le polynôme constant a^{-1}). La réciproque est fausse sans qualité supplémentaire de l´anneau $\mathcal{Z}$; Dans $\mathbb{Z}/8\mathbb{Z}[X]$, le polynôme non constant $1 - 2X$ est inversible puisque

$$(1 - 2X)(1 + 2X + 2^2X^2) = 1 - 2^3X^3 = 1 - 8X^3 = 1.$$

Exercice 40 :

1. Si a est nilpotent, alors $1 - a$ est inversible et $(1 - a)^{-1} = 1 + a + \cdots + a^{n-1}$ dès que $a^n = 0$.
2. (a) Pour I idéal de $\mathcal{Z}$, on a les équivalences :
      i. $I = \mathcal{Z}$
      ii. $1 \in I$
      iii. $I \cap U(\mathcal{Z}) \neq \emptyset$.
   (b) Un corps commutatif n´a que deux idéaux : $0\mathcal{Z} = \{0\}$ et $1\mathcal{Z} = \mathcal{Z}$.

6.2 Éléments associés

Afin de réduire une surprésence des unités de $\mathcal{Z}$ et traduire leur caractère négligeable pour $|$, on définit une relation d´équivalence sur $\mathcal{Z}$ en posant

$$a \cong b \Leftrightarrow \exists u \in U(\mathcal{Z})\ b = ua.$$

On dit alors que a et b, égaux à un inversible près, sont associés. La classe de 0 est $\bar{0} = \{0\}$ et celle de 1 est $\bar{1} = U(\mathcal{Z})$. On fait «descendre» $|$ sur l´espace quotient, de façon à raisonner sur les «types» d´éléments comme on raisonne sur les éléments : Si $a \cong a'$, $b \cong b'$ et $a \mid b$, alors $a' \mid b'$ donc la relation $|$ de divisibilité passe bien au quotient $\mathcal{Z}/\cong$ qu´on note (sans surprise) $\mathcal{N}$. La relation induite sur les classes, encore notée $|$ et encore appelée divisibilité, est aussi réflexive et transitive.

6.3 Éléments indivisibles

On cherche dans l´anneau $\mathcal{Z}$ les éléments «indivisibles». On peut formaliser cette notion de deux façons, selon qu´on se place au niveau «moins 1» des diviseurs ou à l´étage «plus 1» des multiples :

1. il y a les insécables ou les atomes.
2. il y a les «casse-casse propre», les éléments qui, lorsqu´ils divisent, divisent sans se répandre, de façon solidaire.

Définition :

1. Un élément a de $\mathcal{Z}$ est dit irréductible s´il est non marginal et à diviseurs triviaux :

   $$a \neq 0, \quad a \notin U(\mathcal{Z}) \quad \text{et les diviseurs de } a \text{ sont exactement les unités et les associés}$$

   ou de façon équivalente :

   $$a \neq 0, \quad a \notin U(\mathcal{Z}), \quad \forall b, c \in \mathcal{Z} \quad a = bc \Rightarrow b \in U(\mathcal{Z}) \text{ ou } c \in U(\mathcal{Z}).$$

2. Un élément a de $\mathcal{Z}$ est dit premier s´il est non marginal et s´il a la Gauss-attitude :

   $$a \neq 0, \quad a \notin U(\mathcal{Z}), \quad \forall b, c \in \mathcal{Z} \quad a \mid bc \Rightarrow a \mid b \text{ ou } a \mid c.$$

Exercice 41 :

1. Dans $\mathbb{Z}/6\mathbb{Z}$, l´élément 2, non nul et non inversible puisque diviseur de 0 ($2 \times 3 = 0$), est non irréductible puisque $2 = 2 \times 4$ avec 4 non inversible ($4 \times 3 = 0$). En revanche, 2 est premier. En effet, si b et c ne sont pas multiples de 2, b et c appartiennent à $\{1, 3, 5\}$ donc $bc \in \{1, 3, 5\}$, ce qui montre bc n´est pas non plus un multiple de 2.
2. Dans $\mathbb{Z}[i\sqrt{5}]$, on pose, pour $z = a + i\sqrt{5}\,b$, $N(z) = z\bar{z} = a^2 + 5b^2$ et on vérifie que $N(zz') = N(z)N(z')$. Si $2 + i\sqrt{5} = zz'$, alors $N(z)$ est un diviseur de $N(2 + i\sqrt{5}) = 9$. Or les équations (en $(a, b) \in \mathbb{Z}^2$) $a^2 + 5b^2 = 1$, $a^2 + 5b^2 = 3$ et $a^2 + 5b^2 = 9$ ont leurs solutions dans $\{(1, 0), (-1, 0), (\pm 2, \pm 1)\}$. Seuls les candidats $\pm(2 - i\sqrt{5})$ ne sont pas des diviseurs effectifs de $2 + i\sqrt{5}$ (Pas de solution dans $\mathbb{Z}^2$ pour le système $\begin{cases} 2a + 5b = 2 \\ -a + 2b = 1 \end{cases}$. Ceci montre que z diviseur de $2 + i\sqrt{5}$ est soit inversible, soit associé à $2 + i\sqrt{5}$: $2 + i\sqrt{5}$ est irréductible. De même, on montre que 3 est irréductible. Avec $(2 + i\sqrt{5})(2 - i\sqrt{5}) = 9$, le non marginal $2 + i\sqrt{5}$ divise 3×3 sans pour autant diviser l´irréductible 3. Ainsi, l´irréductible $2 + i\sqrt{5}$ n´est pas premier.

6.4 Notions de *pgcd* et *ppcm*

Alors que l´objet d´étude est un anneau $\mathcal{Z}$, les «bons» sous-objets sont les idéaux monogènes ou principaux de $\mathcal{Z}$: la phrase $a \mid b$ se traduit par $b\mathbb{Z} \subset a\mathbb{Z}$. On a les définitions :

Définition :

Pour $X \subset \mathcal{Z}$, on dit que X a un *pgcd* si $\{x\mathcal{Z},\ x \in X\}$ admet une borne supérieur dans l´ensemble ordonné $(\Pi(\mathcal{Z}), \subset)$ des idéaux principaux de $\mathcal{Z}$. Dans ce cas, tout $d \in \mathcal{Z}$ qui vérifie $d\mathcal{Z} = \sup_{x\in X} x\mathcal{Z}$ est appelé *pgcd* de X.

Justification de la terminologie :
Si $X = \{a, b\}$ admet un *pgcd*, alors $d \in \mathcal{Z}$ est un *pgcd* de a et b si, et seulement si, $d \mid a$, $d \mid b$ et, pour δ dans $\mathcal{Z}$, δ divise d si δ est un diviseur commun de a et b.

Définition :

Pour $X \subset \mathcal{Z}$, on dit que X a un *ppcm* si $\{x\mathcal{Z},\ x \in X\}$ admet une borne inférieure dans l´ensemble ordonné $(\Pi(\mathcal{Z}), \subset)$ des idéaux principaux de $\mathcal{Z}$. Dans ce cas, tout $m \in \mathcal{Z}$ qui vérifie $m\mathcal{Z} = \inf_{x\in X} x\mathcal{Z}$ est appelé *ppcm* de X.

Remarque : Si $X = \{a, b\}$ admet un *ppcm*, alors $m \in \mathcal{Z}$ est un *ppcm* de a et b si, et seulement si, $a \mid m$, $b \mid m$ et, pour μ dans $\mathcal{Z}$, m divise μ si μ est un multiple commun de a et b.

6.5 Anneaux intègres

i) Relation d´ordre

Il manque à la relation $\mid$ une qualité pour en faire une brave relation d´ordre et ainsi assurer le même statut d´ensembles ordonnés à $(\mathcal{N}, \mid)$ et à $(\Pi(\mathcal{Z}), \subset)$. Ceci amène à supposer $\mathcal{Z}$ intègre, c-à-d sans diviseurs de 0.

Propriété :

Soit $\mathcal{Z}$ un anneau intègre et $\mathcal{N}$ le quotient $\mathcal{Z}/\cong$ où $\cong$ est la relation d´équivalence «être associé».

1. La relation de divisibilité est une relation d´ordre sur $\mathcal{N}$.
   Pour $\mid$, $\mathcal{N}$ admet un plus petit élément $(\bar{1} = U(\mathcal{Z}))$ et un plus grand élément $\bar{0} = \{0\}$.
2. Pour $a, b \in \mathcal{Z}$, $a\mathcal{Z} = b\mathcal{Z}$ si, et seulement si, $\bar{a} = \bar{b}$, ou de façon équivalente, a et b sont associés. Aussi, pour $X \subset \mathcal{Z}$ admettant un *pgcd*, a et b sont des *pgcd* de X si, et seulement si, a et b sont associés.
3. Pour $a \in \mathcal{Z}$, on a les équivalences :
   (a) a est irréductible.
   (b) $\bar{a}$ est minimal dans $\mathcal{N} \setminus \{\bar{0}, \bar{1}\}$.
   (c) $a\mathcal{Z}$ est maximal dans l´ensemble $\Pi(\mathcal{Z}) \setminus \{\bar{1}\}$ des idéaux propres principaux de $\mathcal{Z}$.
4. Tout élément a premier de $\mathcal{Z}$ est irréductible.
5. Pour $a, b \in \mathcal{Z}$, sous réserve d´existence de *pgcd* de $\{a, b\}$, tout représentant de la classe borne inférieure de $\{\bar{a}, \bar{b}\}$ dans $(\mathcal{N}, \mid)$ est un *pgcd* de $\{a, b\}$. Si d est un tel représentant, On dit que $\bar{d}$ est le *pgcd* de a et b.

ii) Caractère héréditaire de l´intégrité

À un anneau $\mathcal{Z}$, sont naturellement attachés
- l´anneau des polynômes $\mathcal{Z}[X]$,
- les anneaux quotients $\mathcal{Z}/I$ où I est un idéal de $\mathcal{Z}$.

Quand $\mathcal{Z}$ a une qualité, on veut savoir si cette qualité est héréditaire, i.e. si elle passe à $\mathcal{Z}[X]$ et à $\mathcal{Z}/I$. Par exemple, la commutativité de $\mathcal{Z}$ est transmise. On suppose que l´anneau $\mathcal{Z}$ est intègre.

Intégrité de $\mathcal{Z}$ et $\mathcal{Z}[X]$:

On introduit

1. l´application degré de $\mathcal{Z}[X]$ dans $\mathbb{N} \cup \{-\infty\}$ avec $d^\circ 0) = -\infty$. Selon les conventions usuelles de calculs, pour $P_1, P_2 \in \mathcal{Z}[X]$, on a
$$d^\circ(P_1 + P_2) \leqslant d^\circ(P_1) + d^\circ(P_2)$$
et, grâce à l´intégrité de $\mathcal{Z}$,
$$d^\circ(P_1 P_2) = d^\circ(P_1) + d^\circ(P_2).$$
2. l´application valuation de $\mathcal{Z}[X]$ dans $\mathbb{N} \cup \{+\infty\}$ avec $\nu(0) = +\infty$. Selon les conventions usuelles de calculs, pour $P_1, P_2 \in \mathcal{Z}[X]$, on a
$$\nu(P_1 + P_2) \geqslant \nu(P_1) + \nu(P_2)$$
et, grâce à l´intégrité de $\mathcal{Z}$,
$$\nu(P_1 P_2) = \nu(P_1) + \nu(P_2).$$

Sous l´hypothèse «$\mathcal{Z}$ intègre», avec le degré, on caractérise les éléments inversibles de l´anneau $\mathcal{Z}[X]$ comme les polynômes constants de terme constant inversible dans $\mathcal{Z}$. Avec l´application valuation, on montre que $\mathcal{Z}[X]$ est aussi intègre et, en définitive, $\mathcal{Z}$ est intègre si, et seulement si, $\mathcal{Z}[X]$ est intègre.

Exercice 42 : (Toujours avec le degré)
Soit $\mathcal{Z}$ un anneau.

1. Pour $a \in \mathcal{Z}$, $P(a) = 0 \Leftrightarrow X - a \mid P$.
2. On suppose que l´anneau $\mathcal{Z}$ est intègre.
   (a) Les polynomes de $\mathcal{Z}[X]$ de degré 1 sont des éléments irréductibles.
   (b) Quelle propriété du corps $\mathbb{C}$ permet d´affirmer que les irréductibles de $\mathbb{C}[X]$ sont exactement les polynômes de degré 1 ?

Intégrité de $\mathcal{Z}$ et $\mathcal{Z}/I$:

L´anneau $\mathbb{Z}$ des entiers relatifs est intègre alors que $\mathbb{Z}/6\mathbb{Z}$ ne l´est pas comme le montre la relation $\bar{2}.\bar{3} = \bar{0}$. Ceci amène à la notion d´idéal premier.

Définition :

Un idéal I de $\mathcal{Z}$ est dit premier si I est propre ($I \neq \mathcal{Z}$) et si $\forall (a, b) \in \mathcal{Z}$, $ab \in I \Rightarrow a \in I$ ou $b \in I$.

Propriété :

Soit $\mathcal{Z}$ un anneau et I un idéal de $\mathcal{Z}$. Les propositions suivantes sont équivalentes :
1. L´anneau $\mathcal{Z}/I$ est intègre.
2. L´idéal I est premier.

Parmi les anneaux intègres, se distinguent les corps. Quels sont les idéaux (premiers) I de $\mathcal{Z}$ tels que $\mathcal{Z}/I$ est un corps ?

Définition :

Un idéal I de $\mathcal{Z}$ est dit maximal si I est propre ($I \neq \mathcal{Z}$) et si I est un élément maximal pour l´inclusion dans l´ensemble $\mathcal{I}$ des idéaux propres de $\mathcal{Z}$:

$$I \neq \mathcal{Z} \text{ et, pour tout } J \in \mathcal{I},\ I \subset J \Rightarrow I = J.$$

Propriété :

Soit $\mathcal{Z}$ un anneau et I un idéal de $\mathcal{Z}$. Les propositions suivantes sont équivalentes :

1. L´anneau $\mathcal{Z}/I$ est un corps.
2. L´idéal I est maximal.

6.6 Anneaux principaux

Quand on fait de l´arithmétique sur l´objet $\mathcal{Z}$, les «bons» sous-objets sont les idéaux (et non les sous-anneaux) de $\mathcal{Z}$. Il est naturel d´espérer une correspondance Arithmétique-Algèbre $\phi : a \mapsto a\mathcal{Z}$ de $\mathcal{Z}$ vers l´ensemble $\mathcal{I}(\mathcal{Z})$ des idéaux de $\mathcal{Z}$. Il y a deux obstructions à la mise en place d´un dictionnaire efficace :

1. ϕ n´est pas injective. Ce problème est résolu si on suppose que $\mathcal{Z}$ est intègre et si on considère $\mathcal{N}$ au lieu de $\mathcal{Z}$. L´application $\bar{a} \mapsto a\mathcal{Z}$, correctement définie, est alors strictement décroissante de $(\mathcal{N}, |)$ dans $(\mathcal{I}(\mathcal{Z}), \subset)$.
2. ϕ n´est pas surjective puisqu´il y a, a priori, plus d´idéaux que d´idéaux principaux.

Ceci amène à supposer que l´anneau $\mathcal{Z}$, supposé intègre, n´a que des idéaux principaux : $\Pi(\mathcal{Z}) = \mathcal{I}(\mathcal{Z})$. On dit alors que $\mathcal{Z}$ est un anneau principal.

6.6.1 Entre les anneaux euclidiens ...

Définition :

Soit $\mathcal{Z}$ un anneau commutatif unitaire non nul. On dit que $\mathcal{Z}$ est un anneau euclidien si $\mathcal{Z}$ est intègre et si $\mathcal{Z}$ est muni d´une application $\delta : \mathcal{Z}^* = \mathcal{Z} \setminus \{0\} \to \mathbb{N}$ vérifiant :

1. $\forall a, b \in \mathcal{Z}^* \quad \delta(a) \leqslant \delta(ab)$.
2. Pour $(a, b) \in \mathcal{Z} \times \mathcal{Z}^*$, il existe $(q, r) \in \mathcal{Z}^2$ tels que
   (a) $a = bq + r$;
   (b) $r = 0$ ou $(r \neq 0$ et $\delta(r) < \delta(b))$.

Autrement dit, un anneau euclidien est un anneau intègre $\mathcal{Z}$ possédant une division et une application croissante sur $\mathcal{Z}^*$ qui mesure les restes.

Propriété :

Tout anneau euclidien est un anneau principal.

Pour la culture : Il existe des anneaux principaux non euclidiens : $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, $\mathbb{R}[X, Y]/(X^2 + Y^2 + 1)$ ...

6.6.2 et les anneaux factoriels, ...

Le caractère principal de $\mathcal{Z}$ agit comme le double effet «Kiss Cool» ...

i) Existence d´une décomposition en facteurs irréductibles

Propriété : (Remontée infinie de Fermat)

Si $\mathcal{Z}$ est un anneau principal, alors

1. toute suite croissante (I_n) d´idéaux de $\mathcal{Z}$ est stationnaire.
2. tout ensemble $\mathcal{E}$ non vide d´idéaux de $\mathcal{Z}$ a un élément maximal pour l´inclusion.

Remarque : Considérer une suite croissante d´idéaux monogènes revient à considérer une suite décroissante de diviseurs et, dans l´anneau $\mathbb{Z}$ des entiers relatifs qu´on ramène à $\mathbb{N}$, c´est le bon ordre qui justifie le caractère stationnaire.

Preuve :

1. Considérer $J = \bigcup_{n\in\mathbb{N}} I_n$, vérifier que J est un idéal de $\mathcal{Z}$, soit un certain $(a) = a\mathbb{Z}$. Il existe alors $N \in \mathbb{N}$ tel que $a \in I_N$, puis, pour $n \geqslant N$, $I_n = I_N = J$.
2. Si $\mathcal{E}$ n´a pas d´élément maximal, soit I_0 dans $\mathcal{E}$. L´ensemble des idéaux contenant I_0 est non vide et non réduit à I_0 puisque I_0 n´est pas maximal, donc on envisage I_1 dans $\mathcal{E}$ qui contient strictement I_0, puis $I_2 \in \mathcal{E}$ qui contient strictement I_1 etc ... Ainsi, on construit une suite strictement croissante d´idéaux de $\mathcal{Z}$, ce qui est absurde.

□

Corollaire :

Soit $\mathcal{Z}$ un anneau principal.

1. Tout élément non marginal x de $\mathcal{Z}$ admet un diviseur irréductible.
2. Tout élément non marginal x de $\mathcal{Z}$ admet une décomposition en produit de facteurs irréductibles.

Preuve :

1. Considérer l´ensemble $\mathcal{E}$ des idéaux propres de $\mathcal{Z}$ qui contiennent x, non vide puisque $x\mathcal{Z} \in \mathcal{E}$. Envisager ensuite un élément maximal I de $\mathcal{E}$, un certain $I = y\mathcal{Z}$, et vérifier que $y \mid x$ et que y est irréductible.
2. On écrit à bon droit $x_0 = x = x_1y_1$ avec y_1 irréductible. Si x_1 est une unité, on conclut. Sinon, $x_1 = x_2y_2$ avec y_2 irréductible. Dans cette construction pas à pas, on a une suite croissante $(x_n\mathcal{Z})$ d´idéaux de $\mathcal{Z}$. Ainsi, il y a arrêt du processus, fin de la dichotomie, c-à-d l´existence de $N \in \mathbb{N}$ tel que $x_N \in \mathcal{U}(\mathcal{Z})$. Il vient $x_0 = x = x_N\, y_1 \cdots y_N$ où chaque y_i est irréductible.

□

ii) Unicité de la décomposition

Propriété :

Si $\mathcal{Z}$ est un anneau principal, tout élément a irréductible (non marginal à diviseurs triviaux) de $\mathcal{Z}$ est premier (non marginal à la Gauss-attitude). Ainsi, dans $\mathcal{Z}$ principal, on a les équivalences :

1. a est irréductible.
2. a est premier non nul.
3. $a\mathcal{Z}$ est non nul et maximal.
4. $a\mathcal{Z}$ est non nul et premier.

Preuve : Si a est irréductible, $(a) = a\mathcal{Z}$ est maximal pour l´inclusion dans l´ensemble des idéaux pricipaux propres de $\mathcal{Z}$, donc dans l´ensemble des idéaux propres de $\mathcal{Z}$. Ainsi, $a\mathcal{Z}$ est premier et $a \neq 0$ est premier. □

Corollaire :

Si $\mathcal{Z}$ est un anneau principal, alors tout élément non marginal x admet une décomposition en produit de facteurs irréductibles, unique à l´ordre près des facteurs et à des facteurs inversibles près. On dit que $\mathcal{Z}$ est un anneau factoriel.

Preuve : On suppose que $x = a_1 \cdots a_r$ et $x = b_1 \cdots b_s$ où a_1, ..., a_r, b_1, ... b_s sont irréductibles. On raisonne par récurrence sur $n = \min(r, s)$. Si $n = 1$, x est irréductible et $x = a_1 = b_1$, $r = s = 1$. On suppose la propriété vraie au rang $n - 1$. L´élément premier a_1 divise le produit $b_1 \cdots b_s$ donc divise (quitte à échanger les indices) l´irréductible b_1 : $a_1 = ub_1$ avec $u \in \mathcal{U}(\mathcal{Z})$. Par intégrité de $\mathcal{Z}$, on a $a_2 \cdots a_r = b_2 \cdots b_s$ à un inversible près. La récurrence s´enclenche et donne $r = s$, $a_i = b_i$ à un inversible près. □

Pour la culture : On admet que

1. le caractère principal ne passe pas aux anneaux de polynômes. On peut avoir en tête le résulat éclairant : $\mathcal{Z}[X]$ est principal si, et seulement si, $\mathcal{Z}$ est un corps.
2. le caractère factoriel passe aux anneaux de polynômes : si $\mathcal{Z}$ est factoriel, alors $\mathcal{Z}[X]$ l´est aussi.

Il existe des anneaux factoriels non principaux : $\mathbb{Z}[X]$, $\mathbb{R}[X, Y] = \mathbb{R}[X][Y]$ ...

iii) Les objets *pgcd* et *ppcm* dans un anneau factoriel

Si $\mathcal{Z}$ est un anneau factoriel, on choisit un et un seul élément dans chaque classe (modulo la relation «être associé») d´irréductibles et forme une partie $\mathcal{P}$ de $\mathcal{Z}$. Dans $\mathbb{Z}$, on choisit l´ensemble $\{2, 3, 5, 7, 11, 13, 17, \cdots\}$ des entiers naturels irréductibles (nombres premiers). Pour tout $x \in \mathcal{Z}$ non nul, on a la décomposition en facteurs irréductibles :

$$x = u \prod_{p \in \mathcal{P}} p^{v_p(x)}, \quad u \in \mathcal{U}(\mathcal{Z}), \quad \text{où la famille dans } \mathbb{N} \ (v_p(x))_{p \in \mathcal{P}} \text{ est presque nulle.}$$

Par unicité de la décomposition,

$$\forall p \in \mathcal{P},\ \forall x, y \in \mathcal{Z},\ x \neq 0,\ y \neq 0,\ v_p(xy) = v_p(x) + v_p(y),$$

puis

$$x \mid y \Leftrightarrow \forall p \in \mathcal{P},\ v_p(x) \leqslant v_p(y),$$

puis

$$x + y \neq 0 \Rightarrow \forall p \in \mathcal{P},\ v_p(x + y) \geqslant \min(v_p(x), v_p(y).$$

Soient $x_1, x_2, \cdots, x_n$ $(n \geqslant 1)$ des éléments non nuls de $\mathcal{Z}$. La partie $X = \{x_1, \cdots, x_n\}$ de $\mathcal{Z}$ admet un *pgcd* et un *ppcm* et

1. $d = \prod_{p \in \mathcal{P}} p^{\min(v_p(x_1), \cdots, v_p(x_n))}$ est un *pgcd* de X,
2. $m = \prod_{p \in \mathcal{P}} p^{\max(v_p(x_1), \cdots, v_p(x_n))}$ est un *ppcm* de X.

6.6.3 le principal, c´est Bézout.

Dans l´anneau (factoriel) $\mathbb{Z}[X]$, on peut se convaincre que $pgcd(2, X) = 1$ alors qu´il est impossible d´écrire $1 = 2P + xQ$ avec $P, Q \in \mathbb{Z}[X]$.

Théorème de Bézout dans un anneau principal :

Soit $\mathcal{Z}$ un anneau principal. Pour $a_1, \cdots, a_n$ dans $\mathcal{Z}$, on a les équivalences :

1. a_1, ..., a_n sont premiers entre eux : $pgcd(a_1, \cdots, a_n) = 1$.
2. a_1, ..., a_n sont «Bézout» entre eux : $\exists \lambda_1, \cdots, \lambda_n \in \mathcal{Z},\ \lambda_1 a_1 + \cdots + \lambda_n a_n = 1$.

Preuve : On suppose que a_1, ..., a_n sont «Bézout» entre eux. L´idéal $(a_1, \cdots, a_n) = (a_1) + \cdots + (a_n)$ est $\mathcal{Z} = (1)$ donc est principal. Il contient chaque (a_i) donc est un majorant de $\{(a_1), \cdots, (a_n)\}$. Enfin, si I est un majorant dans $\Pi(\mathcal{Z})$ de $\{(a_1), \cdots, (a_n)\}$, I contient 1 et coincide donc avec $\mathcal{Z}$. On a montré que $\{(a_1), \cdots, (a_n)\}$ admet un sup dans $\Pi(\mathcal{Z})$, qui est $\mathcal{Z}$, donc $pgcd(a_1, \cdots, a_n) = 1$. Pour l´autre implication, comme $\mathcal{Z}$ est principal, l´ensemble $\Pi(\mathcal{Z})$ des idéaux principaux de $\mathcal{Z}$ est l´ensemble$\mathcal{I}(\mathcal{Z})$ de tous les idéaux de $\mathcal{Z}$. Aussi, le $\sup((a_1), \cdots, (a_n))$ pris dans $\Pi(\mathcal{Z})$ (qui vaut $\mathcal{Z}$ puisque $pgcd(a_1, \cdots, a_n) = 1$) est ici $\sup((a_1), \cdots, (a_n))$ pris dans $\mathcal{I}(\mathcal{Z})$ (qui existe toujours et vaut $(a_1, \cdots, a_n) = (a_1) + \cdots + (a_n)$. Ainsi, $(a_1) + \cdots + (a_n) = \mathcal{Z}$. □

Corollaire : (Théorème de Gauss)

Si $\mathcal{Z}$ est un anneau principal, $a, b, c \in \mathcal{Z}$, alors

$$a \mid bc \text{ et } a \wedge b = 1 \Rightarrow a \mid c.$$