Université de Tours
Licence 2 Mathématiques

Contrôle continu 1

Arithmétique | Semestre 3

L'épreuve dure 2h. Les 4 exercices sont indépendants. La notation tiendra compte de la clarté et de la rigueur de la rédaction. Toute affirmation doit être justifiée.

Exercice 1

1. Soient $a, b, c \in \mathbb{Z}$. Montrer que
$$(a \mid bc \text{ et } \mathbf{pgcd}\,(a,b) = 1) \implies a \mid c.$$
L'implication est-elle encore vraie si a et b ne sont pas premiers entre eux ? Justifier par une démonstration ou par un contre-exemple.
2. Soient $a, b \in \mathbb{Z}$. Montrer que si
$$\exists x, y \in \mathbb{Z}, \quad ax + by = 1,$$
alors a et b sont premiers entre eux.
3. Soit $n \in \mathbb{Z}$. L'assertion suivante est-elle vraie ou fausse ?
$$\forall a, b \in \mathbb{Z}, \quad (a \mid n \text{ et } b \mid n) \implies ab \mid n.$$
Justifier par une démonstration ou par un contre-exemple.
4. Déterminer les entiers $n \in \mathbb{Z}$ tels que $n - 3 \mid 5n - 7$.
5. Déterminer le reste de la division euclidienne de 100^{100} par 3, et par 7.

Solution.

1. Comme $a \mid bc$, il existe $k \in \mathbb{Z}$ tel que $bc = ka$. De plus, comme a et b sont premiers entre eux,
$$\exists u, v \in \mathbb{Z}, \quad au + bv = 1.$$
On multiplie cette égalité par c et on utilise l'hypothèse de divisibilité :
$$c = auc + bvc = auc + vka = a \times (\underbrace{uc + vk}_{\in \mathbb{Z}}),$$
donc c divise a.
Bien sûr l'implication est fausse si a et b ne sont pas premiers entre eux comme le montre le contre-exemple $a = 6$, $b = 4$ et $c = 3$; on a bien a qui divise bc, pourtant a ne divise pas c.
2. Notons $d = \mathbf{pgcd}\,(a,b)$. Comme d divise a et b, d divise aussi $ax + by = 1$. Donc $d = 1$.
3. L'assertion est fausse comme le montre le contre-exemple $n = 12$, $a = 3$ et $b = 6$. On a bien a et b qui divisent n, pourtant ab ne divise pas n.
4. On raisonne par analyse-synthèse.

Analyse. Soit $n \in \mathbb{Z}$ tel que $n - 3 \mid 5n - 7$. On en déduit que $n - 3$ divise aussi
$$5 \times (n-3) - (5n-7) = -8.$$
Par conséquent, $n - 3 \in \{-8, -4, -2, -1, 1, 2, 4, 8\}$ et donc $n \in \{-5, -1, 1, 2, 4, 5, 7, 11\}$.

Synthèse. Le tableau

n	-5	-1	1	2	4	5	7	11
$n-3$	-8	-4	-2	-1	1	2	4	8
$5n-7$	-32	-12	-2	3	13	18	28	48

nous assure que les entiers $\{-5, -1, 1, 2, 4, 5, 7, 11\}$ conviennent.

5. On va chercher à quoi est congru 100^{100} modulo 3 et modulo 7.
Modulo 3. Comme $100 \equiv 1$ [3], on a directement que $100^{100} \equiv 1$ [3], donc le reste de la division euclidienne de 100^{100} par 3 est 1.
Modulo 7. On commence par remarquer que $100 \equiv 2$ [7]. Ensuite :

$$2^2 \equiv 4\ [7]; \quad 2^3 = 8 \equiv 1\ [7].$$

Finalement, en écrivant que $100 = 3 \times 33 + 1$, on conclut :

$$\begin{aligned} 100^{100} &\equiv 2^{100}\ [7] \\ &\equiv 2^{3\times 33+1}\ [7] \\ &\equiv (2^3)^{33} \times 2\ [7] \\ &\equiv 2\ [7]. \end{aligned}$$

Ainsi, le reste de la division euclidienne de 100^{100} est 2.

$\square$

Exercice 2

1. Soient $a, b \in \mathbb{Z}$. On suppose que a et b sont premiers entre eux.
   (a) Montrer que $\mathbf{pgcd}\,(a+b, a-b) = 1$ ou que $\mathbf{pgcd}\,(a+b, a-b) = 2$.
   (b) Supposons que a et b ont la même parité (c'est-à-dire qu'ils sont soit tous les deux pairs, soit tous les deux impairs). Que vaut $\mathbf{pgcd}\,(a+b, a-b)$?
   (c) Que vaut $\mathbf{pgcd}\,(a+b, a-b)$ quand a et b sont de parités différentes ?
2. (a) Soit $(a, b) \in \mathbb{Z}^2 \backslash \{(0,0)\}$. Montrer que $\mathbf{pgcd}\,(a, b) = \mathbf{pgcd}\,(a, a+b)$.
   (b) Soit $(u_n)_n$ la suite de Fibonacci suivante :

   $$u_0 = 0,\ u_1 = 1; \quad \forall n \in \mathbb{N},\ u_{n+2} = u_{n+1} + u_n.$$

   En utilisant la question précédente, montrer par récurrence que

   $$\forall n \in \mathbb{N}, \quad \mathbf{pgcd}\,(u_n, u_{n+1}) = 1.$$

Solution.

1. Soient $a, b \in \mathbb{Z}$. On suppose que a et b sont premiers entre eux.
   (a) Notons $d = \mathbf{pgcd}\,(a+b, a-b)$. Comme d divise $a+b$ et $a-b$, d divise aussi $(a+b)+(a-b) = 2a$ et $(a+b)-(a-b) = 2b$. Par conséquent, d divise $\mathbf{pgcd}\,(2a, 2b) = 2 \times \mathbf{pgcd}\,(a, b) = 2$. Ainsi, $d = 1$ ou $d = 2$.
   (b) Si a et b ont la même parité (ils sont nécessairement tous les deux impairs), alors $a+b$ et $a-b$ sont des entiers pairs donc 2 divise $a+b$ et $a-b$. On en déduit donc que $\mathbf{pgcd}\,(a+b, a-b) = 2$.
   (c) Si a et b sont de parités différentes (l'un est pair, l'autre est impair), alors $a+b$ et $a-b$ sont deux entiers impairs, donc ils ne sont pas divisibles par 2. Par conséquent, $\mathbf{pgcd}\,(a+b, a-b) = 1$.
2. (a) Notons

   $$d = \mathbf{pgcd}\,(a, b)\,; \quad \delta = \mathbf{pgcd}\,(a, a+b)\,.$$

   On va montrer que d divise δ et que δ divise d.
   D'une part, d divise a et b, donc d divise aussi a et $a+b$. Par conséquent, d divise δ.
   D'autre part, δ divise a et $a+b$, donc δ divise aussi a et $(a+b)-a = b$, donc δ divise d.
   On en déduit que $d = \delta$.

(b) Pour tout entier naturel n, on note $P(n)$: $\mathbf{pgcd}\,(u_n, u_{n+1}) = 1$.

Initialisation $(n=0)$**.** La propriété est vraie au rang $n = 0$ car

$$\mathbf{pgcd}\,(u_0, u_1) = \mathbf{pgcd}\,(1, 1) = 1.$$

Hérédité. Soit $n \in \mathbb{N}$. Supposons que $P(n)$ est vraie et montrons que $P(n+1)$ est vraie. En utilisant la question précédente, on a

$$\mathbf{pgcd}\,(u_{n+1}, u_{n+2}) = \mathbf{pgcd}\,(u_{n+1}, u_{n+1} + u_n) = \mathbf{pgcd}\,(u_{n+1}, u_n) = 1,$$

donc $P(n+1)$ est vraie.

Conclusion. La propriété est vraie au rang initial $(n = 0)$, elle est héréditaire, donc elle est vraie pour tout entier naturel.

$\square$

Exercice 3

1. À l'aide de l'algorithme d'Euclide, calculer $\mathbf{pgcd}\,(24, 87)$ et $\mathbf{pgcd}\,(105, 154)$.
2. Résoudre sur $\mathbb{Z}^2$ les équations suivantes :

$$24x + 87y = 9; \qquad 105x + 154y = 5.$$

Solution.

1. On a

$$\begin{aligned} 87 &= 3 \times 24 + 15 \\ 24 &= 1 \times 15 + 9 \\ 15 &= 1 \times 9 + 6 \\ 9 &= 1 \times 6 + 3 \\ 6 &= 3 \times 2 + 0. \end{aligned}$$

Ainsi $\mathbf{pgcd}\,(24, 87) = 3$. De même,

$$\begin{aligned} 154 &= 1 \times 105 + 49 \\ 105 &= 2 \times 49 + 7 \\ 49 &= 7 \times 7 + 0. \end{aligned}$$

Par conséquent, $\mathbf{pgcd}\,(105, 154) = 7$.

2. Comme 3 divise 9, l'équation

$$24x + 87y = 9$$

admet des solutions entières. On détermine une solution particulière en remontant l'algorithme d'Euclide :

$$9 = 24 - 1 \times 15 = 24 - 1 \times (87 - 3 \times 24) = 4 \times 24 + (-1) \times 87.$$

Ainsi, $(4, -1)$ est une solution particulière de l'équation. L'ensemble des solutions est donc

$$\mathbf{S} = \left\{ \left(4 + \frac{87}{\mathbf{pgcd}\,(24, 87)}k, -1 - \frac{24}{\mathbf{pgcd}\,(24, 87)}k\right) \;\middle|\; k \in \mathbb{Z} \right\} = \{(4 + 29k, -1 - 8k) \mid k \in \mathbb{Z}\}.$$

Par contre, l'équation

$$105x + 154y = 5$$

n'admet pas de solution entière car $\mathbf{pgcd}\,(105, 154) = 7$ ne divise pas 5.

$\square$

Exercice 4
Dans cet exercice, on s'intéresse à l'ensemble

$$\mathbb{Z}[\sqrt{7}] := \left\{ a + b\sqrt{7} \mid a, b \in \mathbb{Z} \right\}.$$

1. Soient $z, \zeta \in \mathbb{Z}[\sqrt{7}]$. Montrer que $z + \zeta \in \mathbb{Z}[\sqrt{7}]$ et que $z \times \zeta \in \mathbb{Z}[\sqrt{7}]$.
2. On rappelle que $\sqrt{7} \notin \mathbb{Q}$.
   (a) Soient $a, b \in \mathbb{Z}$. Montrer que
   $$a + b\sqrt{7} = 0 \iff (a = 0 \text{ et } b = 0).$$
   (b) En déduire que pour tous $a, b, \alpha, \beta \in \mathbb{Z}$,
   $$a + b\sqrt{7} = \alpha + \beta\sqrt{7} \iff (a = \alpha \text{ et } b = \beta).$$
3. On définit l'application suivante :
   $$\mathbf{N} : \left| \begin{array}{ccc} \mathbb{Z}[\sqrt{7}] & \longrightarrow & \mathbb{Z} \\ a + b\sqrt{7} & \longmapsto & a^2 - 7b^2. \end{array} \right.$$
   (a) Calculer $\mathbf{N}(1)$ et $\mathbf{N}(2 + 3\sqrt{7})$.
   (b) Montrer que
   $$\forall z, \zeta \in \mathbb{Z}[\sqrt{7}], \quad \mathbf{N}(z \times \zeta) = \mathbf{N}(z) \times \mathbf{N}(\zeta).$$

Soit $z \in \mathbb{Z}[\sqrt{7}]$. Dans la suite de l'exercice, on dit que z **est inversible** si

$$\exists \zeta \in \mathbb{Z}[\sqrt{7}], \quad z \times \zeta = 1.$$

4. Montrer que si $z \in \mathbb{Z}[\sqrt{7}]$ est inversible, alors $\mathbf{N}(z) = 1$ ou $\mathbf{N}(z) = -1$.
5. Montrer que la réciproque est vraie.
   Indication : Remarquer que $\mathbf{N}(a + b\sqrt{7}) = (a + b\sqrt{7})(a - b\sqrt{7})$.
6. En utilisant les questions précédentes, déterminer un élément inversible $z = a + b\sqrt{7}$ avec $a, b \in \mathbb{Z}$ et $1 \leq b \leq 5$. Préciser son inverse.

Solution.

1. On écrit :
   $$z = a + b\sqrt{7}, \quad \zeta = \alpha + \beta\sqrt{7}, \quad a, b, \alpha, \beta \in \mathbb{Z}.$$
   D'une part,
   $$z + \zeta = (\underbrace{a + \alpha}_{\in\mathbb{Z}}) + (\underbrace{b + \beta}_{\in\mathbb{Z}})\sqrt{7} \in \mathbb{Z}[\sqrt{7}],$$
   et d'autre part,
   $$\begin{aligned} z \times \zeta &= (a + b\sqrt{7})(\alpha + \beta\sqrt{7}) \\ &= a\alpha + a\beta\sqrt{7} + \alpha b\sqrt{7} + b\beta\sqrt{7}^2 \\ &= (\underbrace{a\alpha + 7b\beta}_{\in\mathbb{Z}}) + (\underbrace{a\beta + \alpha b}_{\in\mathbb{Z}})\sqrt{7} \in \mathbb{Z}[\sqrt{7}]. \end{aligned}$$
2. On rappelle que $\sqrt{7} \notin \mathbb{Q}$.
   (a) On raisonne par double implication.
   $\Longrightarrow$ Supposons que $a + b\sqrt{7} = 0$. Si $b \neq 0$, alors on peut écrire que
   $$\sqrt{7} = -\frac{a}{b},$$
   donc $\sqrt{7} \in \mathbb{Q}$. Contradiction ! On en déduit que $b = 0$. Par suite, $a = -b\sqrt{7} = 0$.
   $\Longleftarrow$ Ce sens est clair : si $a = 0$ et $b = 0$, alors $a + b\sqrt{7} = 0 + 0 \times \sqrt{7} = 0$.

(b) D'après la question précédente, pour tous $a, b, \alpha, \beta \in \mathbb{Z}$,

$$\begin{aligned} a + b\sqrt{7} = \alpha + \beta\sqrt{7} &\iff (a - \alpha) + (b - \beta)\sqrt{7} = 0 \\ &\iff (a - \alpha = 0 \ \text{ et } \ b - \beta = 0) \iff (a = \alpha \ \text{ et } \ b = \beta). \end{aligned}$$

3. (a) Comme $1 = 1 + 0 \times \sqrt{7}$, on a

$$\mathbf{N}(1) = 1^2 - 7 \times 0^2 = 1.$$

De même,

$$\mathbf{N}(2 + 3\sqrt{7}) = 2^2 - 7 \times 3^2 = 4 - 63 = -59.$$

(b) Soient $z, \zeta \in \mathbb{Z}[\sqrt{7}]$ qu'on écrit :

$$z = a + b\sqrt{7}, \quad \zeta = \alpha + \beta\sqrt{7}; \quad a, b, \alpha, \beta \in \mathbb{Z}.$$

Rappelons que d'après la première question,

$$z \times \zeta = (a\alpha + 7b\beta) + (a\beta + \alpha b)\sqrt{7}.$$

Par conséquent,

$$\begin{aligned} \mathbf{N}(z \times \zeta) &= (a\alpha + 7b\beta)^2 - 7 \times (a\beta + \alpha b)^2 \\ &= (a\alpha)^2 + 14a\alpha b\beta + 49(b\beta)^2 - 7(a\beta)^2 - 14a\alpha b\beta - 7(\alpha b)^2 \\ &= (a\alpha)^2 + 49(b\beta)^2 - 7(a\beta)^2 - 7(\alpha b)^2. \end{aligned}$$

D'autre part,

$$\mathbf{N}(z) \times \mathbf{N}(\zeta) = (a^2 - 7b^2) \times (\alpha^2 - 7\beta^2) = (a\alpha)^2 - 7(a\beta)^2 - 7(\alpha b)^2 + 49(b\beta)^2 = \mathbf{N}(z \times \zeta).$$

4. Supposons que z est inversible. Il existe donc $\zeta \in \mathbb{Z}[\sqrt{7}]$ tel que $z \times \zeta = 1$. Ainsi :

$$z \times \zeta = 1 \implies \mathbf{N}(z \times \zeta) = \mathbf{N}(1) \implies \mathbf{N}(z) \times \mathbf{N}(\zeta) = 1,$$

où on a utilisé les résultats des questions 3.(a) et 3.(b). Comme $\mathbf{N}(z)$ et $\mathbf{N}(\zeta)$ sont des entiers,

$$\mathbf{N}(z) \times \mathbf{N}(\zeta) = 1 \implies (\mathbf{N}(z) = \mathbf{N}(\zeta) = 1 \ \text{ ou } \ \mathbf{N}(z) = \mathbf{N}(\zeta) = -1).$$

5. Réciproquement, supposons que $\mathbf{N}(z) = \pm 1$ et montrons que z est inversible. On note $z = a + b\sqrt{7}$. On raisonne par disjonction de cas.

Cas 1 : $\mathbf{N}(z) = 1$. En suivant l'indication, on a donc

$$1 = \mathbf{N}(z) = (a + b\sqrt{7}) \times (a - b\sqrt{7}).$$

Posons $\zeta = a - b\sqrt{7}$. Alors $\zeta \in \mathbb{Z}[\sqrt{7}]$ et $z \times \zeta = 1$, donc z est inversible.

Cas 2 : $\mathbf{N}(z) = -1$. Encore une fois, on écrit que

$$-1 = \mathbf{N}(z) = (a + b\sqrt{7}) \times (a - b\sqrt{7}) \quad \text{ou encore que} \quad 1 = (a + b\sqrt{7}) \times (-a + b\sqrt{7}).$$

Posons $\zeta = -a + b\sqrt{7}$. Alors $\zeta \in \mathbb{Z}[\sqrt{7}]$ et $z \times \zeta = 1$, donc z est inversible.
Dans tous les cas, on a montré que z est inversible.

6. Il s'agit donc de trouver $a \in \mathbb{Z}$ et $b \in \{1, \ldots, 5\}$ tels que

$$a^2 - 7b^2 = \pm 1.$$

Il faut essayer diverses valeurs... et trouver que par exemple le couple $(a, b) = (8, 3)$ convient. Ainsi, $z = 8 + 3\sqrt{7}$ vérifie

$$\mathbf{N}(z) = 8^2 - 7 \times 3^2 = 1,$$

donc z est inversible. D'après la question précédente, son inverse est $z = 8 - 3\sqrt{7}$.

□