Université de Tours
Licence 2 Mathématiques

Contrôle continu 2

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
Justifier les assertions suivantes ou donner un contre-exemple.

1. Soient $d, n \in \mathbb{Z}$. Si $d \mid n^2$, alors $d \mid n$.
2. L'équation
$$21x \equiv 6 \mod 60$$
admet 2 solutions modulo 60.
3. Soient $a, b \in \mathbb{Z}^*$. Alors $\mathbf{pgcd}\,(a, b)$ est la plus petite valeur positive de l'ensemble
$$\{ax + by \mid x, y \in \mathbb{Z}\}.$$
4. $2^{33} - 1$ est divisible par $2^{11} - 1$.

Solution.

1. C'est bien sûr faux. Prenons $d = 9$ et $n = 6$. On a $d \mid n^2$ mais d ne divise pas n.
2. Comme $\mathbf{pgcd}\,(21, 6) = 3$, l'équation admet 3 solutions modulo 60. L'assertion est fausse.
3. C'est faux puisque 0 est la plus petite valeur positive de cet ensemble. On a plus précisément
$$\mathbf{pgcd}\,(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\} \cap \mathbb{N}^*.$$
4. L'assertion est vraie. En effet, on a
$$1 + 2^{11} + 2^{22} = \frac{2^{33} - 1}{2^{11} - 1}$$
donc
$$2^{33} - 1 = (2^{11} - 1) \times (2^{22} + 2^{11} + 1),$$
ce qui prouve que $2^{33} - 1$ est divisible par $2^{11} - 1$.

□

Exercice 2 (Nombre de Frobenius)
L'objectif de l'exercice est de déterminer tous les entiers de l'ensemble

$$\mathbf{E} = \{3u + 4v \mid u, v \in \mathbb{N}\}.$$

1. Montrer que l'équation
$$3u + 4v = 5, \quad u, v \in \mathbb{N}$$
n'a pas de solution.
2. Soit $a \in \mathbb{N}^*$.
   (a) Résoudre l'équation
   $$3u + 4v = a, \quad u, v \in \mathbb{Z}.$$
   (b) Montrer qu'il existe un unique couple d'entiers $u, v \in \mathbb{Z}$ tels que $3u+4v = a$ et $0 \leq v \leq 2$.
   (c) En déduire que si $a > 5$, alors $a \in \mathbf{E}$.
3. Déterminer $\mathbf{E}$.

Solution.

1. On raisonne par l'absurde : supposons au contraire qu'il existe une solution $(u, v) \in \mathbb{N}$. On ne peut pas avoir $u = 0$ ou $v = 0$, clairement. Et ensuite, si $u, v \geq 1$, alors
$$3u + 4v \geq 3 + 4 = 7 > 5,$$
donc (u, v) n'est pas solution. Dans tous les cas, (u, v) n'est pas solution.
2. (a) Comme $\mathbf{pgcd}(3, 4) = 1$, on sait que cette équation admet une infinité de solutions. On a une combinaison de Bézout simple :
$$(-1) \times 3 + 1 \times 4 = 1,$$
de sorte que $(-a, a)$ est une solution particulière de l'équation. Ainsi, l'ensemble des solutions est
$$\mathbf{S} = \{(-a + 4k, a - 3k) \mid k \in \mathbb{Z}\}.$$
   (b) D'après la question précédente, pour tout $k \in \mathbb{Z}$, si on pose $u = -a + 4k$ et $v = a - 3k$, alors $3u + 4v = a$. On a ensuite
   $$0 \leq v \leq 2 \iff 0 \leq a - 3k \leq 2 \iff a - 2 \leq 3k \leq a,$$
   et il existe un unique entier $k \in \mathbb{Z}$ qui vérifie cette condition.
   (c) Supposons que $a > 5$. D'après la question précédente, il existe $u \in \mathbb{Z}$ et $v \in \{0, 1, 2\}$ tel que
   $$3u + 4v = a.$$
   Pour montrer que $a \in \mathbf{E}$, il suffit de montrer que u est positif. On écrit simplement que
   $$3u = a - 4v > 5 - 4v \geq 5 - 8 = -3 \quad \text{donc} \quad 3u > -3.$$
   Ceci assure que $u \geq 0$, donc $a \in \mathbf{E}$.
3. Résumons. D'après la question précédente, tous les entiers strictement supérieurs à 5 appartiennent à $\mathbf{E}$. D'après la première question $5 \notin \mathbf{E}$. Clairement, $0, 3, 4 \in \mathbf{E}$ et $2 \notin \mathbf{E}$. Bref,
$$\mathbf{E} = \{0, 3, 4\} \cup \{n \in \mathbb{N} \mid n \geq 6\}.$$

□

Exercice 3 (Une fonction arithmétique)
On appelle σ la fonction qui, à un entier plus grand que 1, associe la somme de ses diviseurs positifs :

$$\sigma : \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{N} \\ n & \longmapsto & \displaystyle\sum_{d \in \Delta(n)} d. \end{array} \right.$$

On a noté $\Delta(n)$ l'ensemble des diviseurs positifs de n :

$$\Delta(n) = \{d \in [\![1; n]\!], \ \ d \mid n\}.$$

1. Calculer $\sigma(11)$ et $\sigma(28)$.
2. Soient $p \in \mathbb{N}$ un nombre premier et $k \in \mathbb{N}$. Montrer que
$$\sigma(p^k) = \frac{p^{k+1} - 1}{p - 1}.$$
3. Montrer que σ est une *fonction arithmétique*, c'est-à-dire que
$$\forall n, m \in \mathbb{N}^*, \quad \textbf{pgcd}\,(n, m) = 1 \implies \sigma(nm) = \sigma(n)\sigma(m).$$
Indication : Établir une bijection entre $\Delta(nm)$ et $\Delta(n) \times \Delta(m)$.

Soit $n \in \mathbb{N}^*$. On dit que n est **déficient** si $\sigma(n) < 2n$; **parfait** si $\sigma(n) = 2n$; **abondant** si $\sigma(n) > 2n$.

4. Déterminer la nature de 6, 9 et 12.
5. Soit $p \in \mathbb{N}$ un nombre premier. Quelle est la nature de p ?
6. Soit $n \in \mathbb{N}^*$ un entier parfait. On suppose qu'on peut l'écrire $n = 2^k m$, où $k \in \mathbb{N}^*$ et m est un entier impair.
   (a) Montrer que
   $$2^{k+1} m = (2^{k+1} - 1)\sigma(m).$$
   (b) En déduire que $2^{k+1} - 1$ divise m. On note $d \in \mathbb{N}^*$ tel que
   $$m = (2^{k+1} - 1)d.$$
   (c) Vérifier que
   $$\sigma(m) = 2^{k+1} d; \quad n = 2^k (2^{k+1} - 1)d; \quad \sigma(n) = 2^{k+1}(2^{k+1} - 1)d.$$
   (d) On suppose que $d > 1$. Montrer que
   $$\sigma(m) \geq 1 + d + (2^{k+1} - 1)d,$$
   et en déduire que $d = 1$, puis que $\sigma(m) = m + 1$.

Solution.

1. On a
$$\Delta(11) = \{1, 11\} \quad \text{et} \quad \Delta(28) = \{1, 2, 4, 7, 14, 28\}$$
donc
$$\sigma(11) = 12 \quad \text{et} \quad \sigma(28) = 56.$$
2. On a
$$\Delta(p^k) = \{1, p, p^2, \ldots, p^k\}.$$
En effet, si $d \in \mathbb{N}^*$ est un diviseur de p^k, alors en vertu du lemme de Gauss, soit $d = p$, soit d est premier avec p et donc d divise p^{k-1}, et ainsi de suite.. Bref,
$$\sigma(p^k) = 1 + p + p^2 + \ldots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

3. Soient $n, m \in \mathbb{N}^*$ tels que $\mathbf{pgcd}\,(n,m) = 1$. Soit f l'application

$$f : \left| \begin{array}{ccc} \Delta(nm) & \longrightarrow & \Delta(n) \times \Delta(m) \\ x & \longmapsto & (\mathbf{pgcd}\,(x,n)\,, \mathbf{pgcd}\,(x,m)) \end{array} \right.$$

L'objectif est de montrer que f est une bijection. Ceci entrainera que

$$\mathbf{card}(\Delta(nm)) = \mathbf{card}(\Delta(n) \times \Delta(m)) = \mathbf{card}(\Delta(n)) \times \mathbf{card}(\Delta(m))$$

autrement dit, $\sigma(nm) = \sigma(n)\sigma(m)$.

f **est bien définie** puisque pour tout $x \in \Delta(nm)$, $\mathbf{pgcd}\,(x,n)$ est un diviseur de n et $\mathbf{pgcd}\,(x,m)$ est un diviseur de m.

f **est injective.** Soient $a, b \in \Delta(nm)$ tels que $f(a) = f(b)$, autrement dit

$$\mathbf{pgcd}\,(a,n) = \mathbf{pgcd}\,(b,n) \quad \text{et} \quad \mathbf{pgcd}\,(a,m) = \mathbf{pgcd}\,(b,m)\,.$$

Montrons que $a = b$. Écrivons les décompositions en facteurs premiers :

$$n = \prod_{k=1}^{N} p_i^{\nu_i}; \quad m = \prod_{j=1}^{M} q_j^{\mu_j}, \quad \nu_i, \mu_j \in \mathbb{N}^*.$$

Comme n et m sont premiers entre eux, aucun des nombres premiers qui apparaissent dans la décomposition de n sont présents dans celle de m, et inversement. On écrit ensuite a et b sous la forme :

$$a = \prod_{k=1}^{N} p_i^{a_i} \prod_{j=1}^{M} q_j^{\alpha_j};\ b = \prod_{k=1}^{N} p_i^{b_i} \prod_{j=1}^{M} q_j^{\beta_j}, \quad a_i, b_i \leq \nu_i,\ \alpha_j, \beta_j \leq \mu_j.$$

Par suite,

$$\mathbf{pgcd}\,(a,n) = \mathbf{pgcd}\,(b,n) \iff \forall i \in [\![1; N]\!],\ a_i = b_i$$

et

$$\mathbf{pgcd}\,(a,m) = \mathbf{pgcd}\,(b,m) \iff \forall j \in [\![1; M]\!],\ \alpha_j = \beta_j,$$

donc $a = b$.

f **est surjective**. Soit $(a,b) \in \Delta(n) \times \Delta(m)$. Posons $x = ab$. Montrons que $f(x) = (a,b)$, c'est-à-dire que $\mathbf{pgcd}\,(x,n) = a$ et que $\mathbf{pgcd}\,(x,m) = b$. On se contente de montrer que $\mathbf{pgcd}\,(x,n) = a$, l'autre preuve est similaire.
Déjà, a divise $x = ab$ et a divise n donc a divise $\mathbf{pgcd}\,(x,n)$. Ensuite, $\mathbf{pgcd}\,(x,n)$ divise ab et $\mathbf{pgcd}\,(x,n)$ est premier avec b puisque n et m sont premiers entre eux donc $\mathbf{pgcd}\,(x,n)$ divise a. Bref, $\mathbf{pgcd}\,(x,n) = a$. On montre de même que $\mathbf{pgcd}\,(x,m) = b$.
On a bien montré que f est bijective.

4. On a

$$\sigma(6) = 12 = 2 \times 6; \quad \sigma(9) = 13 < 2 \times 9; \quad \sigma(12) = 28 > 2 \times 12$$

donc 6 est parfait, 9 est déficient et 12 est abondant.

5. On a

$$\sigma(p) = p + 1 < 2p$$

donc p est déficient.

6. (a) Comme 2^k sont premiers entre eux,

$$\sigma(n) = \sigma(2^k)\sigma(m) = \frac{2^{k+1} - 1}{2 - 1} \times \sigma(m) = (2^{k+1} - 1)\sigma(m).$$

D'autre part, n est parfait donc $\sigma(n) = 2n = 2^{k+1}m$. Bref :

$$2^{k+1}m = \sigma(n) = (2^{k+1} - 1)\sigma(m).$$

(b) L'égalité précédente assure que $2^{k+1}-1$ divise $2^{k+1}m$. Or comme $2^{k+1}-1$ est impair, on a $\mathbf{pgcd}\left(2^{k+1}-1, 2^{k+1}\right) = 1$. En vertu du lemme de Gauss, $2^{k+1}-1$ divise m.

(c) On insère la définition de d dans l'égalité de la question (a) :

$$2^{k+1}m = (2^{k+1}-1)\sigma(m) \iff 2^{k+1}(2^{k+1}-1)d = (2^{k+1}-1)\sigma(m) \iff 2^{k+1}d = \sigma(m).$$

Ensuite,

$$n = 2^k m = 2^k(2^{k+1}-1)d$$

et

$$\sigma(n) = 2n = 2^{k+1}(2^{k+1}-1)d.$$

(d) Si $d > 1$, alors 1, d et m sont des diviseurs positifs distincts de m donc par définition de σ,

$$\sigma(m) \geq 1 + d + m = 1 + d + (2^{k+1}-1)d.$$

Autrement dit, si $d > 1$, alors

$$\sigma(m) \geq 1 + 2^{k+1}d = 1 + \sigma(m),$$

contradiction. On en déduit que $d \leq 1$ et comme $d \in \mathbb{N}^*$, $d = 1$. Par suite,

$$\sigma(m) = 2^{k+1} = m + 1.$$

□

Exercice 4 (RSA)

1. Écrire $n := 65$ comme produit deux nombres premiers (positifs) p et q.
2. Rappeler la définition de l'indicatrice d'Euler ϕ et montrer que
$$\phi(n) = pq - p - q + 1.$$
3. Trouver l'inverse u de 7 modulo $\phi(n)$.
4. Résoudre alors
$$x^7 \equiv 2 \mod n.$$

Solution.

1. On pose $p = 5$ et $q = 13$ de sorte que $n = pq$.
2. Par définition,
$$\phi(n) = \mathbf{card}(\{k \in [\![1; n]\!] \mid \mathbf{pgcd}\,(k, n) = 1\}).$$
Comme ϕ est une fonction multiplicative et que p et q sont premiers,
$$\phi(n) = \phi(p)\phi(q) = (p-1)(q-1) = pq - p - q - 1 = 48.$$
3. Précisons que comme $\mathbf{pgcd}\,(\phi(n), 7) = 1$, 7 est effectivement inversible modulo $\phi(n)$. Au vu de la combinaison de Bézout
$$(-1) \times \phi(n) + 7 \times 7 = 1,$$
7 est son propre inverse modulo $\phi(n)$: $u = 7$.
4. Dans ces conditions, on sait que l'équation admet une unique solutio modulo n qui est $x = 2^u = 2^7$ puisqu'alors
$$x^7 = (2^7)^7 = 2^{49} = 2^{1+\phi(n)} = 2 \times 2^{\phi(n)} \equiv 2 \mod n.$$
Il ne reste plus qu'à calculer x modulo n. Comme $2^6 = 64$, on a
$$\begin{aligned} 2^7 = 2 \times 64 &\equiv 2 \times (-1) \mod n \\ &\equiv -2 \mod n \\ &\equiv 63 \mod n. \end{aligned}$$
La solution recherchée est $x = 63$.

□