Correction math pour l'info
Partiel mai 2013.

Sylviane SCHWER

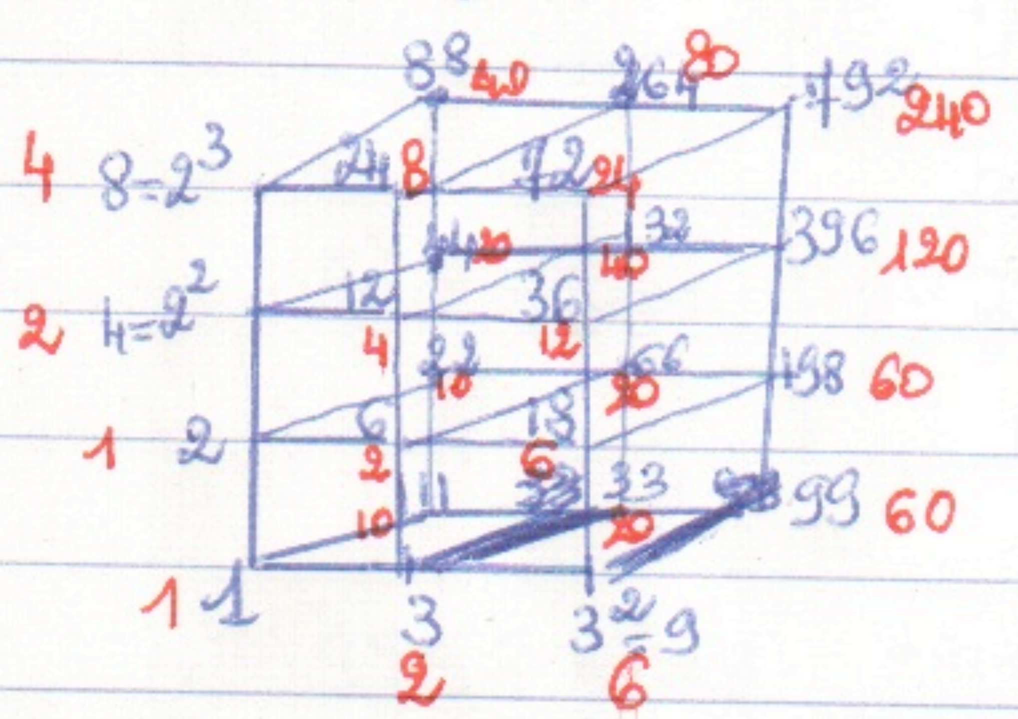
Exo 1 ① d'après les propriétés de divisibilité 792 est divisible par 11, 9 et 2 et l'on trouve $792 = 11 \times 3^2 \times 2^3$

② $m \in \mathbb{N}$ $m | 792$ ssi $m = 11^\alpha 3^\beta 2^\gamma$ avec $0 \leq \alpha \leq 1$
$m \in \mathbb{Z}$ $m | 792$ ssi $m = \pm 11^\alpha 3^\beta 2^\alpha$ $\quad 0 \leq \beta \leq 2$
$0 \leq \gamma \leq 3$

donc $\# D_{\mathbb{N}}(792) = 2 \times 3 \times 4 = 24$
$\# D_{\mathbb{Z}}(792) = 2 \# D_{\mathbb{N}}(792) = 48$

③ l'indicatrice d'Euler $\varphi(p) = p-1$ si $p \in \mathbb{P}$
$\varphi(p^\alpha) = (p-1)p^{\alpha-1}$ $\quad p \in \mathbb{P}$
$(*)$ $\varphi(ab) = \varphi(a)\varphi(b)$ $\quad a, b \in \mathbb{N}$

Il suffit donc de calculer les indicateurs des nombres en bordure du diagramme pour obtenir par $(*)$ les autres



④ On a vu devoir n°4 et en cours que ~~le~~ nombre de sous groupes de $\mathbb{Z}/n\mathbb{Z}$ est le nombre de diviseurs de n donc il y a 24 sous groupes dans $(\mathbb{Z}/n\mathbb{Z}, +)$.

Exo 2 : ① $18118 1 \wedge 181 = 181$ donc pas de solutions entières à 1

② $9600 \wedge 181 = 1$ donc il existe des solutions entières

En utilisant l'algorithme de Bezout, on obtient
$9600 = 181 \times 53 + 7$; $181 = 7 \times 25 + 6$; $7 = 6 \times 1 + 1$

puis $1 = 7 - 6 \times 1 = 7 - [181 - 7 \times 25] = 7 \times 26 - 1 \times 181 = (9600 - 181 \times 53) \times 26 - 1 \times 181$ soit $\boxed{1 = 9600 \times 26 - 1379 \times 181}$ donc $(26, -1379)$ est une solution.

On en déduit que $181^{-1} \equiv -1379 \ (9600)$ d'où $[181]^{-1}_{9600} = [8221]_{9600}$.
$\equiv -1379 + 9600 \ (9600)$

Exo 3 ① $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ $\qquad$ $g\ \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

(a) $x \mapsto x+b$ est bijective $\forall b \in \mathbb{Z}/n\mathbb{Z}$ de réciproque $x \mapsto x-b$

(b) $x \mapsto ax+b$ " " ssi $a \wedge n = 1$ " " $x \mapsto a'(x-b)$

avec $aa' \equiv 1\ (n)$

(c) $x \mapsto x^a$ " " si $a \wedge \varphi(n) = 1$ de réciproque $x \mapsto x^{a'}$

avec $aa' \equiv 1\ [\varphi(n)]$

② une clé RSA de la forme $(p \times q, e)$ signifie que pour envoyer un message crypté au fournisseur de cette clé, il faut utiliser la fonction

$f : \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/pq\mathbb{Z}$ $\quad p, q \in \mathbb{P}$

$x \mapsto x^e$ avec f bijective pour le décodage.

d'après ①(c) $e \wedge \varphi(pq) = 1$ soit $e \wedge (p-1)(q-1) = 1$

(b) $9797 = 101 \times 97 \in \mathbb{P} \times \mathbb{P}$ $\quad \varphi(9797) = 100 \times 96 = 9600$

d'après exo 2.2 $\quad 9600 \wedge 181 = 1$ donc nous avons bien une clé RSA

③ Bob utilise $\left\{ \begin{array}{l} f : \mathbb{Z}/9797\mathbb{Z} \to \mathbb{Z}/9797\mathbb{Z} \\ x \mapsto x^{181} \end{array} \right.$

Alice utilise $\left\{ \begin{array}{l} f : \mathbb{Z}/9797\mathbb{Z} \to \mathbb{Z}/9797\mathbb{Z} \\ x \mapsto x^{8221} \end{array} \right.$ d'après l'exo 2 et Exo 3.1 ~~et 3.2~~

④ $9796 \equiv -1\ (9797)$ donc il transmet $\left[9796^{181}\right]_{9797} \equiv \left[(-1)^{181}\right]_{9797} = [-1]_{9797}$

il transmet donc 9796.

Exo 4 ① $(A^*, \cdot, \varepsilon)$ et $(\mathbb{N}^2, +, (0,0))$ sont deux monoïdes.

Montrons que ϕ est un morphisme, c'est-à-dire qu'il transporte la structure de A^* dans $\mathbb{N}^2$, il suffit pour cela de vérifier que

- $\phi(f \cdot g) = \phi(f) + \phi(g)$ or $|fg|_a = |f|_a + |g|_a$ et $|fg|_b = |f|_b + |g|_b$ donc
- $\phi(\varepsilon) = (0,0)$, ce qui est évident

$\phi(fg) = (|fg|_a, |fg|_b) = (|f|_a + |g|_a, |f|_b + |g|_b) = (|f|_a, |g|_a) + (|f|_b, |g|_b) = \phi(f) + \phi(g)$.

ϕ est bien un morphisme de monoïdes.

2. $\ker\phi = \{ f \in A^* \mid \phi(f) = (0,0) \}$

$f \in \ker\phi$ ssi $|f|_a = |f|_b = 0$ ssi $f = \varepsilon$ donc $\ker\phi = \{\varepsilon\}$

3. $\forall (n,m) \in \mathbb{N}^2$ $\quad \varphi(a^n b^m) = \varphi(b^m a^n) = (n,m)$ et $a^n b^m \neq b^m a^n$ si $n \neq 0$ et $m \neq 0$.

donc φ est surjective mais non injective. ⚠ comparer avec les morphismes de groupes !

4. $\mathbb{N}^2$ est dénombrable, φ surjective (et non injective) $\Rightarrow \#A^* \geq \# \mathbb{N}^2$

dire que ϕ est non injective ne signifie pas (i) qu'il n'existe pas de fonction injective de A^* dans $\mathbb{N}^2$ (ii) ou qu'il existe une fonction injective de A^* dans $\mathbb{N}^2$

on ne peut donc rien conclure du résultat de 3 sur la dénombrabilité de A^*.

5. $\phi^{-1}[(n,p)]$ est l'ensemble des mots de A^* ayant exactement n lettres a et n lettres b. Tous ces mots sont de longueur $n+p$ et sont obtenus en plaçant les n lettres a dans les $n+p$ places possibles : $x_1 x_2 \dots x_{n+p}$

Il y en a donc $\binom{n+P}{n}$

6. A^* est une union dénombrable d'ensembles finis, A^* est donc dénombrable.

7. $f \in A^\omega$ $\quad f : x_0 x_1 \dots x_n \dots \quad x_i \in \{a,b\}$

Supposons que A^ω est dénombrable. Il existe donc une bijection de $\mathbb{N}$ dans A^ω qui permet de numéroter les éléments de A^ω. Utilisons alors cette numérotation pour lister les éléments de A^ω

$w_0 = x_{0,0}\, x_{0,1}\, x_{0,2} \dots x_{0,n} \dots$

$w_1 = x_{1,0}\, x_{1,1}\, x_{1,2} \dots x_{1,n} \dots$

$w_2 = x_{2,0}\, x_{2,1}\, x_{2,2} \dots x_{2,n} \dots$

$\vdots$

$w_n = x_{n,0}\, x_{n,1}\, x_{n,2} \dots x_{n,n} \dots$

$\vdots$

Nous allons utiliser l'argument de la diagonale de Cantor pour construire une suite infinie $x_0 \dots x_n \dots$ qui est égal à un mot de A^ω mais qui diffère au moins par un élément de tous les éléments de la liste, ce qui prouvera qu'il n'existe aucune bijection de $\mathbb{N}$ dans A^ω, i.e. que A^ω est non dénombrable.

posons $x_i = a$ si $x_{ii} = b$ sinon $x_i = b$ $\forall i \in \mathbb{N}$

$f = x_0 \dots x_i \dots \in A^\omega$ et $\forall i \in \mathbb{N}$ $f \neq \omega_i$ ☒

5 ① χ est injective car $\chi(U)=\chi(V) \Leftrightarrow \chi_U=\chi_V \Leftrightarrow \forall x\in E\ \chi_U(x)=\chi_V(x)$

$\Leftrightarrow x\in U$ ssi $x\in V \Leftrightarrow U=V$

χ est surjective car $\forall f\in\{0,1\}^E\quad f^{-1}(1)\subseteq E$ ie $f^{-1}(1)\in \mathcal{P}(E)$

et $\chi[f^{-1}(1)]=f$

② $i(x)=i(y) \Leftrightarrow \{x\}=\{y\} \Leftrightarrow x=y$ donc i est injective

$\phi\in 2^E=\mathcal{P}(E)$ et $i^{-1}(\phi)\notin E$ donc i n'est pas surjective

③ a) $2^E=\mathcal{P}(E)$ est par χ en bijection avec $\{0,1\}^E$, ensemble des fonctions de E dans $\{0,1\}$ de cardinal $2^{\#E}$ donc 2^E est fini de cardinal $2^{\#E}$

b) Dans le cas fini, i injective non surjective $\Rightarrow \#E < \#2^E$

donc $n<2^n$

④ Soit a_f un antécédent de $\{x\in E, x\notin f(x)\}$, $f(a_f)=\{x\in E, x\notin f(x)\}$

soit $a_f\in f(a_f)$ soit $a_f\notin f(a_f)$, puisque tout élément de E - donc en particulier a_f - est ou n'est pas dans une partie quelconque de E - donc en particulier $f(a_f)$. Or les deux cas sont contradictoires avec la définition même de $f(a_f)$.

⚠ Cette question est une occurrence du Paradoxe de Russell

⑤ et on vient de démontrer qu'il n'existe pas de surjection de E dans $\mathcal{P}(E)$, donc

⑥ $\#E < \#\mathcal{P}(E)$

⑦ d'après ③ si E est fini, $\mathcal{P}(E)$ est fini

d'après ⑥ si E est au moins dénombrable, $\mathcal{P}(E)$ est non dénombrable.

⑧ $\chi_{U\cap V}(x)=1$ ssi $x\in U\cap V$

$(\chi_U\cdot\chi_V)(x)=\chi_U(x)\cdot\chi_U(x)=1$ ssi $\chi_U(x)=1$ et $\chi_V(x)=1 \Leftrightarrow$

$x\in U$ et $x\in V \Leftrightarrow x\in U\cap V$ ∎

⑨ $\chi_{U-V}(x)=1$ ssi $x\in U-V \Leftrightarrow x\in U$ et $x\notin V \Leftrightarrow \chi_U(x)=1$ et

$\chi_V(x)=0 \Leftrightarrow \chi_U(x)-\chi_V(x)=1 \Leftrightarrow (\chi_U-\chi_V)(x)=1$.

remarque $(\chi_U-\chi_V)(x)\in\{-1,0,1\}$ donc $\sup(0,\chi_U-\chi_V)\in\{0,1\}$.

⑩ $x\in U\cup V$ ssi soit $x\in U$ et $x\notin V$ soit $x\in V$ et $x\notin U$ soit $x\in U$ et $x\in V$

dans les 3 cas $(\chi_U+\chi_V-\chi_U\cdot\chi_V)(x)=1$

si $x\notin U\cup V$ $\quad(\chi_U+\chi_V-\chi_U\cdot\chi_V)(x)=0$ ∎

11 d'après 8, 9, 10 $\quad \chi_{U\Delta V} = \sup(0, \chi_U + \chi_V - 2\chi_U\chi_V)$

12 en substituant A à U et B à V on obtient $\chi_{A\Delta B} = \sup(0, \chi_A + \chi_B - 2\chi_A\chi_B)$
" " B à U et A à V " " $\chi_{B\Delta A} = \sup(0, \chi_B + \chi_A - 2\chi_B\chi_A)$
par commutativité de + et . dans $\{0,1\}^E$ $\quad \chi_{A\Delta B} = \chi_{B\Delta A}$
*

13 en substituant $A\Delta B$ à U et C à V on obtient

$$\chi_{(A\Delta B)\Delta C} = \sup(0, \chi_{A\Delta B} + \chi_C - 2\chi_{A\Delta B}\chi_C)$$

par 12

$$= \sup\left(0, \chi_A + \chi_B - 2\chi_A\cdot\chi_B + \chi_C - 2(\chi_A + \chi_B - 2\chi_A\chi_B)\chi_C\right)$$

$$\overset{*}{=} \sup\left[0, \chi_A + \chi_B + \chi_C - 2(\chi_A\cdot\chi_B + \chi_A\chi_C + \chi_B\chi_C) + 4\chi_A\chi_B\chi_C\right]$$

en substituant A à U et $B\Delta C$ à V on obtient

$$\chi_{A\Delta(B\Delta C)} = \sup(0, \chi_A + \chi_{B\Delta C} - 2\chi_A\cdot\chi_{B\Delta C})$$

par 12

$$= \sup(0, \chi_A + \chi_B + \chi_C - 2\chi_B\cdot\chi_C - 2\chi_A(\chi_B + \chi_C - 2\chi_B\chi_C)$$

$$\overset{*}{=} \sup(0, \chi_A + \chi_B + \chi_C - 2(\chi_A\chi_B + \chi_A\chi_C + \chi_B\chi_C) + 4\chi_A\chi_B\chi_C]$$

d'où $\chi_{A\Delta(B\Delta C)} = \chi_{(A\Delta B)\Delta C}$

14 χ étant injective $\quad \chi_{A\Delta B} = \chi_{B\Delta A} \Leftrightarrow A\Delta B = B\Delta A$

$$\chi_{A\Delta(B\Delta C)} = \chi_{(A\Delta B)\Delta C} \Leftrightarrow A\Delta(B\Delta C) = (A\Delta B)\Delta C$$

Donc Δ est commutative et associative dans $\mathcal{P}(E)$
De plus $A\Delta\phi = A$ car $\chi_{A\Delta\phi} = \chi_A + \chi_\phi - 2\chi_A\chi_\phi$ avec $\chi_\phi = 0$
$= \chi_A$

donc $(\mathcal{P}(E), \Delta, \phi)$ est un monoïde commutatif.