**Corrigé Examen 6L23 : Arithmétique dans les anneaux** jeudi 16 juin 2011
9h00–12h00

**1.** Dans cet exercice $K$ désigne d'abord un corps commutatif quelconque, qui sera spécialisé ensuite par $K = \mathbf{Q}$ ou par $K = \mathbf{R}$. On considérera d'abord une matrice carrée quelconque $A \in \mathcal{M}_n(K)$, qui sera spécialisée ensuite par une matrice spécifique dans $\mathcal{M}_2(K)$.

*a.* On considère ici $\mathcal{M}_n(K)$ comme une espace vectoriel sur $K$ (structure définie par l'addition et multiplication scalaire des matrices uniquement), espace dans lequel les puissances $A^i$ de $A$ pour $i \in \mathbf{N}$ sont des vecteurs. Pourquoi la famille infinie $A^0 = \mathrm{id}, A^1 = A, A^2, A^3, \ldots$ de vecteurs ne peut-elle pas être libre ?

√ *Comme $\mathcal{M}_n(K)$ est de dimension finie, aucune famille infinie de vecteurs ne peut être libre. En fait $\dim_K \mathcal{M}_n(K) = n^2$, et toute famille de plus de $n^2$ vecteurs est forcément liée.*

*b.* D'après la question précédente il existe $d \in \mathbf{N}$ telle que la famille $A^0, A^1, \ldots, A^d$ soit liée ; on prend $d$ minimal, de sorte que la famille $A^0, A^1, \ldots, A^{d-1}$ soit libre. Montrer qu'il existe un $d$-uplet unique de coefficients $c_0, \ldots, c_{d-1} \in K$ tels que $c_0A^0 + \cdots + c_{d-1}A^{d-1} = A^d$.

√ *D'après les hypothèses il existe une relation linéaire non triviale $\mu_0A^0 + \cdots + \mu_dA^d = 0$ mais aucune telle relation qui ne concerne pas $A^d$ ; par conséquent $\mu_d \neq 0$ et un peut poser $c_i = \frac{\mu_i}{\mu_d}$ pour $i = 0, \ldots, d-1$, pour obtenir l'expression cherchée $c_0A^0 + \cdots + c_{d-1}A^{d-1} = A^d$. Cette expression est unique parce que la famille formée de $A^0, A^1, \ldots, A^{d-1}$ est libre.*

*c.* On sait que l'application $f : K[X] \to \mathcal{M}_n(K)$ vérifiant $f(\sum_{i=0}^k a_iX^i) = \sum_{i=0}^k a_iA^i$ (substitution de $A$ pour $X$, notée $f(P) = P(A)$) est un morphisme d'anneaux. Décrire $\mathrm{Ker}(f)$ et $\mathrm{Im}(f)$.

√ *Par construction le polynôme $P = X^d - c_{d-1}X^{d-1} - \cdots - c_0X^0$ vérifie $P(A) = 0$, donc $P \in \mathrm{Ker}(f)$, et aucun polynôme non nul de degré inférieur à $d$ appartient à $\mathrm{Ker}(f)$. Comme $\mathrm{Ker}(f)$ est un idéal de l'anneau $K[X]$ ces conditions assurent que $\mathrm{Ker}(f)$ est l'ideál principal engendré par $P$. Les puissances $A^i$ pour $i \in \mathbf{N}$ engendrent $\mathrm{Im}(f)$ en tant que $K$-espace, mais $A^d$ est linéairement dépendant des puissances inférieurs, et en multipliant matriciellement cette relation par $A^i$, on voit qu'il en est de même pour $A^{d+i}$ avec $i \in \mathbf{N}$, ce qui montre $\mathrm{Im}(f) = \mathrm{Vect}(A_0, \ldots, A_{d-1})$. (On pourrait également arriver à cette conclusion en montrant $\dim(\mathrm{Im}(f)) = \dim(K[X]/(P)) = d$.)*

*d.* Quelle est la relation entre le polynôme minimal de $A$ et les réponses aux questions *b*,*c* ?

√ *Le polynôme $P$ est le polynôme minimal de $A$ ; il détermine donc la relation de dépendance de la question b, et engendre $\mathrm{Ker}(f)$.*

*e.* Sous quelle condition le sous-anneau commutatif $K[A] = \mathrm{Im}(f)$ de $\mathcal{M}_n(K)$ est-il un corps ?

√ *On a $K[A] = K[X]/(P)$, et en tant que quotient d'un anneau principal, cet anneau est un corps si et seulement si $P$ est irréductible.*

*f.* On spécialise maintenant $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right) \in \mathcal{M}_2(K)$. Déterminer $d$ et $c_0, \ldots, c_{d-1}$ de la question *b*.

√ *On a $A^2 = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right) = A^0 + A^1$ donc $d = 2$ et $c_0 = c_1 = 1$.*

*g.* On suppose que $K = \mathbf{Q}$ ou $K = \mathbf{R}$ (les deux cas se traitent simultanément), montrer qu'un morphisme d'anneaux $g : K[A] \to \mathbf{R}$, avec $g(\lambda\,\mathrm{id}) = \lambda$ pour tout $\lambda \in K$, est déterminé par $g(A) \in \mathbf{R}$. Déduire de la relation $c_0A^0 + \cdots + c_{d-1}A^{d-1} = A^d$, qui est explicitée dans la question précédente, que seulement deux valeurs pour $g(A)$ sont possibles, qu'on spécifiera.

√ *Un morphisme d'anneaux $R[X] \to S$ est déterminé par sa restriction à $R$, qui est un morphisme $R \to S$, et par l'image de $X$. Tout morphisme $g$ comme spécifié détermine par composition un morphisme $g \circ f : K[X] \to \mathbf{R}$, dont la restriction à $K$ est l'inclusion $K \hookrightarrow \mathbf{R}$ (car $f(\lambda) = \lambda\,\mathrm{id}$ pour $\lambda \in K$). Donc $g \circ f$ est déterminé par $g \circ f(X) = g(A)$, et comme $f$ est surjectif, $g \circ f$ détermine $g$ (par "passage au quotient par $\mathrm{Ker}(f) = (P)$"). Ainsi $g$ est déterminé par $g(A)$ (on aurait aussi plus simplement pu constater que $K[A] = \mathrm{Vect}(A^0, A^1)$ et que $g(\lambda A^0 + \mu A^1) = \lambda + \mu g(A)$). En plus la substitution de $r \in \mathbf{R}$ pour $X$ passe au quotient si et seulement si son noyau contient $\mathrm{Ker}(f) = (P)$, c'est-à-dire si $P(r) = 0$. Or $P = X^2 - X - 1$ a deux racines $\frac{\phi_\pm = 1 \pm \sqrt{5}}{2}$ dans $\mathbf{R}$, et $g(A)$ doit être l'une d'elles.*

*h.* Montrer que $K[A]$ est un corps si $K = \mathbf{Q}$. Indiquer un sous-corps de $\mathbf{R}$ auquel il est isomorphe.

√ *D'après la question e il s'agit de montrer que $X^2 - X - 1$ est irréductible dans $\mathbf{Q}[X]$, ce qui est clair car s'il se factorisait cette factorisation serait aussi une factorisation dans $\mathbf{R}[X]$, mais dans ce dernier anneau on a une factorisation $P = (X - \phi_+)(X - \phi_-)$ (unique si l'on prend les facteurs unitaires), dont les coefficients des facteurs ne sont pas dans $\mathbf{Q}$ (autre façon de le dire : $P$ étant de degré 2 et sans racines rationnelles, est irréductible dans $\mathbf{Q}[X]$). Chacun des deux morphismes $g$ est un isomorphe vers le sous-corps $\mathbf{Q}[\sqrt{5}]$ de $\mathbf{R}$.*

*i.* Maintenant on spécialise $K = \mathbf{R}$. Montrer que dans ce cas $K[A]$ n'est pas un anneau intègre.

√ *On a vu que $P$ se factorise $P = P_+P_-$ dans $\mathbf{R}[X]$ avec $P_\pm = X - \phi_\pm$. L'anneau $\mathbf{R}[A] \cong \mathbf{R}[X]/(P_+P_-)$ n'est donc pas un corps et pas intègre non plus (en fait $f(P_+)f(P_-) = f(P_+P_-) = f(P) = P(A) = 0$ mais $f(P_+) = P_+(A) = A - \phi_+ \,\mathrm{id}$ et $f(P_-) = P_-(A) = A - \phi_- \,\mathrm{id}$ ne sont pas nuls dans $\mathbf{R}[A]$).*

*j.* Soient $g_+, g_-$ les deux morphismes d'anneaux $\mathbf{R}[A] \to \mathbf{R}$ qui sont possibles d'après la question *f*. Montrer que $g_\pm : \mathbf{R}[A] \to \mathbf{R} \times \mathbf{R}$ donné par $g_\pm(x) = (g_+(x), g_-(x))$ est un isomorphisme d'anneaux, et décrire son morphisme inverse.

√ *On prend $g_+(A) = \phi_+ = \frac{1+\sqrt{5}}{2}$ et $g_-(A) = \phi_- = \frac{1-\sqrt{5}}{2}$. En tout cas $g_\pm$ est un morphisme d'anneau, et en tant qu'application $\mathbf{R}$-linéaire $\mathbf{R}[A] \to \mathbf{R}^2$ sa matrice dans la base $(A^0, A^1)$ est $\left(\begin{smallmatrix} 1 & \phi_+ \\ 1 & \phi_- \end{smallmatrix}\right)$ qui est inversible (son déterminant est $-\sqrt{5}$). Le morphisme réciproque se décrit par la matrice inverse $\frac{1}{\sqrt{5}}\left(\begin{smallmatrix} -\phi_- & \phi_+ \\ 1 & -1 \end{smallmatrix}\right)$ ce qui peut être explicité, sur la base$(A^0, A^1)$ à l'arrivée, par*

$$(x, y) \mapsto \begin{pmatrix} \frac{x+y}{2} - \frac{x-y}{2\sqrt{5}} & \frac{x-y}{\sqrt{5}} \\ \frac{x-y}{\sqrt{5}} & \frac{x+y}{2} + \frac{x-y}{2\sqrt{5}} \end{pmatrix} \in \mathbf{R}[A].$$

**2.** Dans cet exercice $K$ est un corps commutatif qui sera spécialisé à la question *d*.

*a.* On suppose que deux polynômes $P, Q \in K[X]$ sont premiers entre eux. Montrer que l'idéal de $K[X]$ engendré par $P$ et $Q$ est égal à $K[X]$ tout entier.

√ *Comme $K[X]$ est un anneau principal, l'idéal en question est engendré par un seul élément, qui doit diviser à la fois $P$ et $Q$. Comme ces polynômes sont premiers entre eux leurs seul diviseurs communs sont inversibles dans $K[X]$ (des constantes non nulles), et un tel élément engendre$K[X]$ tout entier en tant que idéal.*

*b.* La question précédente implique par le lemme chinois pour les idéaux (vu en TD) que le morphisme d'anneaux $f : K[X] \to K[X]/(P) \times K[X]/(Q)$, qui associe à un polynôme la paire de sa classe modulo $P$ et celle modulo $Q$, est surjectif. Conclure qu'on a un isomorphisme $K[X]/\operatorname{Ker}(f) \to K[X]/(P) \times K[X]/(Q)$, et donner explicitement ce noyau $\operatorname{Ker}(f)$.

√ *L'existence de l'isomorphisme vers $\operatorname{Im}(f) = K[X]/(P) \times K[X]/(Q)$ est affirmé par un théorème d'isomorphisme (1.3.4). Le noyau $\operatorname{Ker}(f)$ contient précisément les multiples communs de $P$ et $Q$, et est donc engendré par $\operatorname{ppcm}(P, Q) = PQ$. Ceux qui ont écrit $\operatorname{Ker}(f) = (P)(Q)$ n'ont pas strictement parlant tort (on peut définir le produit de deux idéaux, et dans le cas des idéaux principaux c'est l'idéal engendré par le produit des générateurs), mais il n'y a aucune raison d'invoquer le produit dans cet exercice (pour $f_1 \times f_2 : R \to S_1 \times S_2$ alors $\operatorname{Ker}(f_1 \times f_2) = \operatorname{Ker}(f_1) \cap \operatorname{Ker}(f_2)$ n'est pas en général $\operatorname{Ker}(f_1)\operatorname{Ker}(f_2)$) si n'est pour témoigner de ne pas savoir quoi faire.*

*c.* Soit $p > 2$ un nombre premier. Montrer que $a \in \mathbf{Z}/p\mathbf{Z}$ est un carré dans $\mathbf{Z}/p\mathbf{Z}$ (et donc la classe d'un carré $k^2$ avec $k \in \mathbf{Z}$) si et seulement si $a^{\frac{p-1}{2}} \in \{\overline{0}, \overline{1}\} \subseteq \mathbf{Z}/p\mathbf{Z}$. Combien de solutions $a$ possède l'équation $a^{\frac{p-1}{2}} = \overline{0}$ ? Et $a^{\frac{p-1}{2}} = \overline{1}$ ? *(Utiliser la structure connue du groupe $(\mathbf{Z}/p\mathbf{Z})^\times$.)*

√ *On sait que $(\mathbf{Z}/p\mathbf{Z})^\times$ est cyclique d'ordre $p - 1$ (théorème 1.5.10). Alors l'image de $x \mapsto x^2$ dans $(\mathbf{Z}/p\mathbf{Z})^\times$ est son unique sous-groupe d'indice 2 (et donc d'ordre $\frac{p-1}{2}$) qui est aussi le noyau de $x \mapsto x^{\frac{p-1}{2}}$, l'ensemble des solutions de $a^{\frac{p-1}{2}} = \overline{1}$. (On peut aussi raisonner : tout $x \in (\mathbf{Z}/p\mathbf{Z})^\times$ vérifie $x^{p-1} = \overline{1}$, donc $x^2 \in \{\, a \in \mathbf{Z}/p\mathbf{Z})^\times \mid a^{\frac{p-1}{2}} = \overline{1} \,\}$, ensemble qui d'un côté ne peut pas avoir plus de $\frac{p-1}{2}$ éléments (racines d'un polynôme de ce degré) et d'autre côté, chaque équation $x^2 = a$ ne pouvant avoir plus de 2 solutions, possède au moins $\frac{1}{2}\#(\mathbf{Z}/p\mathbf{Z})^\times = \frac{p-1}{2}$ éléments.) Le seul élément laissé à côté est $x = \overline{0}$, qui vérifie évidemment $x^{\frac{p-1}{2}} = \overline{0}$, et est le seul à le faire.*

*d.* Soit maintenant $K = \mathbf{Z}/p\mathbf{Z}$, $Q = X^2 + bX + c \in K[X]$ un polynôme quadratique unitaire, et $\Delta = b^2 - 4c \in K$ son discriminant. Montrer que (1) si $\Delta = 0$ alors $Q$ est le carré d'un polynôme de degré 1 ; (2) si $\Delta^{\frac{p-1}{2}} = \overline{1}$ alors $Q$ est le produit de deux polynômes distincts de degré 1 ; (3) sinon on a l'égalité $\Delta^{\frac{p-1}{2}} = \overline{p-1} \in K$, et $Q$ est irréductible dans $K[X]$.

√ *Comme pour les polynômes quadratiques réels, $Q$ possède des racines si et seulement si $\Delta$ est un carré, et elles sont donnés par $\frac{-b\pm\delta}{2}$ où $\delta$ désigne l'une des racines carrées de $\Delta$. En effet $4Q = (2X+b)^2 - \Delta$ a les mêmes racines que $Q$, et elles ne peuvent exister que si $\Delta$ est un carré disons $\Delta = \delta^2$, auquel cas $4Q = (2X+b+\delta)(2X+b-\delta)$ dont les racines sont celles indiquées. Si $\Delta = 0$ alors $\delta = 0$ et $Q = (X + \frac{b}{2})^2$ ; si $\Delta^{\frac{p-1}{2}} = \overline{1}$ alors un $\delta \neq 0$ existe, et $Q = (X + \frac{b+\delta}{2})(X + \frac{b-\delta}{2})$ est un factorisation en deux facteurs distincts. Dans le cas restant $Q$ n'a pas de racines et (étant de degré 2) est donc irréductible dans $K[X]$ ; la valeur de $\Delta^{\frac{p-1}{2}}$, dont le carré est $\overline{1}$, est forcément $\overline{-1} = \overline{p-1}$.*

*e.* Montrer que l'anneau $A = K[X]/(Q)$ a $p^2$ éléments, et que selon les trois cas décrits on a: (1) $A$ contient au moins un élément nilpotent non nul ; (2) $A$ contient des diviseurs de zéro mais pas d'éléments nilpotents non nuls ; (3) $A$ est un corps commutatif.

√ *En tant que $K$-espace vectoriel, $A$ est de dimension 2 (avec base formée des classes de 1 et de $X$), et comme $\#K = p$ on a $\# = \#K^2 = p^2$. Dans le cas (1) on a $Q = Q_0^2$, et la classe de $Q_0 \in K[X]$ modulo $Q$ est un élément nilpotent (d'ordre 2) dans $A$. Dans le cas (2) on a $Q = Q_1Q_2$ et les classes de $Q_1$ et $Q_2$ modulo $Q$ ont produit 0 sans être elles-mêmes nulles. D'après le lemme chinois on a $K[X]/(Q) \cong K[X]/(Q_1) \times K[X]?(Q_2) \cong K[X] \times K[X]$, et cet anneau n'a pas d'éléments nilpotents non nuls (car les deux composantes d'un élément nilpotent doivent être nilpotents dans $k$, donc nuls). Finalement dans le cas (3) $A$ est le quotient d'un anneau principal par l'idéal engendré par l'élément irréductible $Q$ et donc un corps commutatif.*

*f.* On considère un nombre $n \in \mathbf{Z}$ dont la classe modulo $p$ n'est pas un carré dans $\mathbf{Z}/p\mathbf{Z}$. Alors l'anneau commutatif $R = \mathbf{Z}[\sqrt{n}] \cong \mathbf{Z}[X]/(X^2 - n)$ est intègre et contient $\mathbf{Z}$ et donc le nombre $p$. Montrer $p$ est un élément irréductible et même premier de l'anneau $R$.

√ *Le quotient $R/pR$ est isomorphe à $\mathbf{Z}[X]/(X^2 - n, p) \cong K[X]/(X^2 - n)$, et par hypothèse sur $n$ le polynôme $X^2 - n \in K[X]$ n'a pas de racines. Il est donc irréductible d'après la question d, et $K[X]/(X^2 - n)$ est un corps ; comme c'est aussi le cas de $R/pR$, l'idéal $pR$ de $R$ est maximal, donc premier, et l'élément $p$ est premier, donc irréductible dans $R$.*

**3.** Cet exercice considère la résolution d'un système de relations de congruence dans $\mathbf{Z}$. L'outil principal est l'algorithme d'Euclide étendu, qui calcule pour deux entiers $a, b$ à la fois $d = \text{pgcd}(a, b)$ et des coefficients $s, t$ d'une relation de Bezout $d = sa+tb$. Cet algorithme assez élémentaire a été mentionné dans le cours (en haut de page 22), mais n'a pas été le sujet d'exercices de TD. On rappelle que l'idée de base est de déterminer pour toutes les valeurs intermédiaires (restes) dans l'algorithme d'Euclide aussi des coefficients qui les expriment en combinaison linéaire de $a$ et $b$. Si toutefois vous n'arrivez pas à déterminer correctement les coefficients de Bezout nécessaires, vous pouvez les nommer et exprimer les résultats suivants symboliquement en termes de ces coefficients.

On considère les deux congruences suivantes, pour $x \in \mathbf{Z}$ :

$$74x \equiv 22 \pmod{84} \tag{1}$$

$$x \equiv 67 \pmod{130} \tag{2}$$

*a.* Argumenter, après le calcul seulement d'un pgcd dans $\mathbf{Z}$, que la congruence (1) possède des solutions. Que peut-on dire (sans le calculer explicitement) de l'ensemble de ses solutions ?

√ *On a $\text{pgcd}(74, 84) = 2$ qui divise aussi 22, et la congruence se simplifie en divisant par 2 à $37x \equiv 11 \pmod{42}$ dans lequel le coefficient 37 est premier avec 42. Par conséquent le coefficient est inversible dans $\mathbf{Z}/42\mathbf{Z}$, et en multipliant 22 par un représentant de cet inverse modulo 42 on trouvera un solution. La multiplication correspondante dans $\mathbf{Z}/42\mathbf{Z}$ transformera la relation de congruence en une congruence simple modulo 42, qui détermine l'ensemble des solutions (une classe modulo 42).*

*b.* Déterminer l'inverse de (la classe de) 37 dans $\mathbf{Z}/42\mathbf{Z}$.

√ *On a*

$$\begin{array}{rrcl} & 42 & = & 1\times 42 \;+\; 0\times 37 \\ & 37 & = & 0\times 42 \;+\; 1\times 37 \\ 42-1\times 37= & 5 & = & 1\times 42 \;-\; 1\times 37 \\ 37-7\times 5= & 2 & = & -7\times 42 \;+\; 8\times 37 \\ 5-2\times 2= & 1 & = & 15\times 42 \;-\; 17\times 37 \end{array}$$

*ou plus simplement la suite des congruences modulo* 42*:* $42\equiv 0\times 37$*,* $37\equiv 1\times 37$*,* $5\equiv -1\times 37$*,* $2\equiv 8\times 37$*,* $1\equiv -17\times 37$*. En final, l'inverse cherché est la classe de* $-17$*, ou de* 25*, modulo* 42*.*

*c.* Trouver une solution particulière de la congruence (1), et décrire ensuite l'ensemble de toutes ses solutions.

√ *On a pour* $x=-17\times 11=-187$ *que* $37x=37\times -17\times 11\equiv 11 \pmod{42}$*. Cette solution est congruente modulo* 42 *à* 23*, donc la solution complète est donnée par* $x\equiv 23 \pmod{42}$*.*

*d.* On considère maintenant le système des deux congruences (1) et (2), dont la première a été simplifiée dans les questions précédentes pour donner un système de la forme

$$x\equiv a_1 \pmod{n_1} \tag{3}$$
$$x\equiv a_2 \pmod{n_2} \tag{4}$$

avec $a_1, a_2, n_1, n_2\in\mathbf{Z}$ (en fait $a_2=67$, $n_2=130$). Calculer $d=\operatorname{pgcd}(n_1,n_2)$ et déduire de chacune des congruences une congruence modulo $d$. Les deux congruences sont-elles compatibles ?

√ *En clair on a*

$$x\equiv 23 \pmod{42}, \tag{3}$$
$$x\equiv 67 \pmod{130}. \tag{4}$$

*On a* $d=\operatorname{pgcd}(42,130)=2$*, et en réduisant modulo* 2 *les deux équations donnent* $x\equiv 1 \pmod 2$*. Elles sont alors compatible (le cours décrit, et la suite de cet exercice montre, que qu'une réduction contradictoire modulo* $d=\operatorname{pgcd}(n_1,n_2)$ *est la seule obstruction possible à une solution).*

*e.* Si $r$ est le reste modulo $d$ que toute solution du système doit avoir (trouvé dans la question précédente), on peut introduire une nouvelle variable $x'=\frac{x-r}{d}$. Donner un système de congruences pour $x'$ de la forme

$$x'\equiv a'_1 \pmod{n'_1} \tag{5}$$
$$x'\equiv a'_2 \pmod{n'_2} \tag{6}$$

où en plus $n'_1$ et $n'_2$ sont premiers entre eux.

√ *En clair on a*

$$x'\equiv 11 \pmod{21} \tag{5}$$
$$x'\equiv 33 \pmod{65} \tag{6}$$

*où effectivement* $21=42/2$ *et* $65=130/2$ *sont premiers entre eux. Un système de cette forme a toujours comme solution une classe modulo* $n'_1n'_2$ *(proposition 2.1.7), dans ce cas modulo* 1365*.*

*f.* Montrer que si $y\in\mathbf{Z}$ vérifie $y\equiv 0 \pmod{n'_1}$ et $y\equiv 1 \pmod{n'_2}$, alors l'ensemble des solutions du système ((5),(6)) est formé des $x'$ vérifiant $x'\equiv a'_1+y(a'_2-a'_1) \pmod{n'_1n'_2}$.

√ *Modulo* $n'_1$ *on a* $a'_1+y(a'_2-a'_1)\equiv a'_1$ *et modulo* $n'_2$ *on a* $a'_1+y(a'_2-a'_1)\equiv a'_1+a'_2-a'_1=a'_2$*, donc* $x'=a'_1+y(a'_2-a'_1)$ *est une solution du système de congruences. La solution entière est donnée par sa classe modulo* $n'_1n'_2$*, c'est-à-dire par* $x'\equiv a'_1+y(a'_2-a'_1) \pmod{n'_1n'_2}$*.*

*g.* Trouver un tel $y$ à l'aide d'une relation de Bezout pour $n'_1, n'_2$.

√ *On trouve une relation de Bezout* $1=31\times 21-10\times 65$ *par la méthode de la question b. Alors* $y=31\times 21=651$ *convient.*

*h.* Terminer en donnant les solutions du système ((1),(2)) du départ.

√ *La solution de ((5),(6)) est* $x'\equiv 11+651(33-11)=14333 \pmod{1365}$ *ou de façon équivalente* $x'\equiv 863 \pmod{1365}$*. La solution de ((1),(2)) en découle par* $x=2x'+1$*, et forme une classe modulo* $\operatorname{ppcm}(42,130)=2\times 1365=2730$ *; en clair cette solution est donc*

$$x\equiv 2\times 683+1=1367 \pmod{2730}.$$



**Fin.**