Corrigé Examen Arithmétique et algèbre commutative vendredi 3 mai 2013
9h00–12h00

1. Dans cette partie on cherche à trouver tous les nombres naturels n à trois chiffres décimaux (où on admet la possibilité d'avoir le chiffre '0' comme premier chiffre) tel que les trois derniers chiffres de n^2 sont ceux du nombre n lui-même (dans l'ordre).

a. Justifier que les solutions de ce problème correspondent aux solutions de l'équation $x^2 = x$ pour x dans l'anneau $\mathbf{Z}/1000\mathbf{Z}$.

√ *Le nombre formé des trois derniers chiffres d'un entier positif n représente la classe x de n dans $\mathbf{Z}/1000\mathbf{Z}$; dire que les trois derniers chiffres de n sont ceux de n lui-même revient donc à dire que $x^2 = x$ dans $\mathbf{Z}/1000\mathbf{Z}$, et pour chaque tel x il existe un unique représentant n avec $0 \leq n < 1000$.*

b. Comment le théorème chinois permet-il de trouver ces solutions si l'on suppose connues les solutions de la même équation $x^2 = x$ mais avec x pris dans l'anneau $\mathbf{Z}/8\mathbf{Z}$ et également celles pour l'équation avec x pris dans l'anneau $\mathbf{Z}/125\mathbf{Z}$, ? Si ces deux problèmes possèdent respectivement k et l solutions, combien de solutions aura le problème avec $x \in \mathbf{Z}/1000\mathbf{Z}$?

√ *Le théorème chinois affirme pour ce cas que $\mathbf{Z}/1000\mathbf{Z} \cong \mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/125\mathbf{Z}$ (car 8 et 125 sont premiers entre eux et leur produit est 1000) donc $x \in \mathbf{Z}/1000\mathbf{Z}$ vérifie $x^2 = x$ si et seulement si ses deux projections dans $x_8 \in \mathbf{Z}/8\mathbf{Z}$ et $x_{125} \in \mathbf{Z}/125\mathbf{Z}$ vérifient chacune cette équation, car par définition $(x_8, x_{125})^2 = (x_8^2, x_{125}^2)$ dans $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}/125\mathbf{Z}$. Pour chaque paire d'une solution modulo 8 et une solution modulo 125 on trouve donc une solution modulo 1000, et avec k, l comme dans la question le nombre de telles solutions est kl.*

c. Trouver des coefficients de Bezout s, t tels que $\text{pgcd}(8, 125) = 1 = 8s + 125t$.

√ *On a $5 = 1 \times 125 - 15 \times 8$, puis $3 = 8 - 5 = 16 \times 8 - 1 \times 125$, $2 = 5 - 3 = 2 \times 125 - 31 \times 8$, et finalement $1 = 3 - 2 = 47 \times 8 - 3 \times 125$. On trouve donc $s = 47$ et $t = -3$.*

d. Trouver les solutions de $x^2 = x$ avec $x \in \mathbf{Z}/8\mathbf{Z}$.

√ *En essayant toutes le classes modulo 8, on trouve que les classes de 0 et de 1 sont les seules solutions.*

e. Argumenter que pour que la classe $x = m_{125} \in \mathbf{Z}/125\mathbf{Z}$ d'un entier m modulo 125 soit une solution de $x^2 = x$, il est nécessaire que la classe $x' = m_{25} \in \mathbf{Z}/25\mathbf{Z}$ du même nombre modulo 25 soit une solution de $(x')^2 = x'$, et que pour cela il est nécessaire que la classe $x'' = m_5 \in \mathbf{Z}/5\mathbf{Z}$ de m modulo 5 soit une solution de $(x'')^2 = x''$.

√ *Si d est un diviseur de n, les multiples de n sont en particulier des multiples de d, donc $n\mathbf{Z}$ est contenu dans le noyau $d\mathbf{Z}$ de la projection canonique $\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$, et ce morphisme passe au quotient pour donner un morphisme d'anneaux $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$. Cela veut dire que si nue classe modulo n vérifie une équation polynomiale, son image modulo d vérifiera l'équation correspondante (mais la réciproque n'est pas garantie). Cela s'applique en particulier pour l'équation $x^2 = x$, et les paires $(n, d) = (125, 25)$ et $(n, d) = (25, 5)$.*

f. Utiliser cela pour trouver successivement toutes les solutions de $x^2 = x$ pour $x \in \mathbf{Z}/5\mathbf{Z}$, ensuite celles pour $x \in \mathbf{Z}/25\mathbf{Z}$, et finalement celles pour $x \in \mathbf{Z}/125\mathbf{Z}$.

√ *Les solutions de $x^2 = x$ dans $\mathbf{Z}/5\mathbf{Z}$ sont les classes de $0, 1$. Si $s = \{0, 1\}$ représente une telle solution, alors les classes modulo 25 correspondant à s sont $s + 5k$ pour $k \in \{0, 1, 2, 3, 4\}$, et les solutions potentielles des $x^2 = x$ modulo 25 sont à chercher uniquement parmi ces valeurs. Or $(s + 5k)^2 = s^2 + 20s + 25k^2 \equiv s^2 + 10k \pmod{25}$, et compte tenu du fait que nos représentants s vérifient tous deux $s^2 = s$ dans l'anneau $\mathbf{Z}$, on voit que $(s + 5k)^2 \equiv s + 5k \pmod{25}$ revient à $5k \equiv 0 \pmod{25}$ ou encore $k \equiv 0 \pmod{5}$, donc $k = 0$ est la seule solution, à la fois pour $s = 0$ que pour $s = 1$; les solutions de $x^2 - x$ sont les classes modulo 25 de 0 et de 1. Le passage de $\mathbf{Z}/25\mathbf{Z}$ à $\mathbf{Z}/125\mathbf{Z}$ est similaire, l'équation $(s + 25k)^2 \equiv s + 25k \pmod{125}$ donne $25k \equiv 0 \pmod{125}$ et donc $k \equiv 0 \pmod{5}$; les solutions de $x^2 - x$ sont les classes modulo 125 de 0 et de 1 (encore).*

g. Conclure en donnant tous les nombres n vérifiant la condition de l'introduction de cette partie.

√ *Les 2 solutions modulo 8 est les deux solutions modulo 125 donnent par combinaison 4 solutions modulo 1000. Combiner les paires de solutions $(0, 0)$ et $(1, 1)$ est facile, et donne les classes de 0 et de 1 modulo 1000. Combiner les paires de solutions $(0, 1)$ et $(1, 0)$ est un peu plus difficile, mais se fait directement à l'aide de la relation de Bezout $47 \times 8 - 3 \times 125 = 1$, car on voit que $47 \times 8 \equiv 0 \pmod{8}$ et $47 \times 8 \equiv 1 \pmod{125}$, d'où la classe de $47 \times 8 = 376$ correspond aux classes de $0, 1$ respectivement modulo 8 et modulo 125, pendant que $-3 \times 125 \equiv 1 \pmod{8}$ et $-3 \times 125 \equiv 0 \pmod{125}$ montrent que la classe de $-3 \times 125 = -375$ correspond aux classes de*

$1, 0$ *respectivement modulo* 8 *et modulo* 125. *Pour trouver les solutions du problème donné il suffit maintenant de choisir des représentants* $0 \leq n < 1000$, *ce qui nécessite juste de remplacer* -375 *par son représentant* 625 *; les solutions sont* $n \in \{0, 1, 376, 625\}$.

2. Soit R un anneau commutatif, et $a \in R$.

a. Montrer que si a est nilpotent (c'est-à-dire $a^n = 0$ pour un certain $n \in \mathbf{N}$) et $\mathfrak{p} \subseteq R$ est un idéal premier, alors $a \in \mathfrak{p}$.

√ *L'image* $\bar{a}$ *de* a *dans le quotient* $A/\mathfrak{p}$, *qui est un anneau intègre car* $\mathfrak{p}$ *est un idéal premier, vérifie* $\bar{a}^n = 0$, *ce qui entraîne* $\bar{a} = 0$ *(l'un au moins des* n *facteur* $\bar{a}$ *dans le produit doit être nul, et dans ce cas tous le sont). Cela veut dire que* $a \in \mathfrak{p}$.

b. On rappelle que l'anneau des séries formelles $R[[X]]$ contient des expressions formelles $\sum_{i=0}^{\infty} c_i X^i$ sans condition sur suite des coefficients $c_i \in R$, avec les opérations définies comme dans $R[X]$. Vérifier que pour $a \in R$ quelconque, la série formelle $1 - aX$ (dont les coefficients de X^i pour $i > 1$ sont tous nuls) possède dans $R[[X]]$ un inverse, à savoir la série géométrique $\sum_{i=0}^{\infty} a^i X^i$.

√ *Il suffit de montrer que dans* $R[[X]]$ *(qui est un anneau commutatif) on a* $(1-aX)(\sum_{i=0}^{\infty} a^i X^i) = 1$. *Le coefficient constant de ce produit est* $1 \times a^0 = 1$, *et les contributions au terme de degré* $i > 0$ *du produit sont les produits* $1 \times a^i X^i$ *et* $-aX \times a^{-1} X^{-1}$, *dont la somme est nulle. Le produit est donc égal à son terme constant qui vaut* 1.

c. On suppose maintenant que $a \in R$ n'est pas nilpotent. Montrer que $1 - aX$ n'est pas inversible dans $R[X]$ (bien qu'il soit inversible dans $R[[X]]$). [Utiliser que l'inverse d'un élément est unique.]

√ *L'inverse* $\sum_{i=0}^{\infty} a^i X^i$ *de* $1 - aX$ *dans* $R[[X]]$ *se trouver dans le sous-anneau* $R[X]$ *des polynômes si et seulement si les coefficients* a^i *sont ultimement nuls, c'est-à-dire si* a *est nilpotent. Si ce n'est pas le cas, cet inverse n'est pas un polynôme. Mais comme* $1 - aX$ *ne peut pas avoir d'autres inverses dan* $R[[X]]$ *cela veut dire que* $1 - aX$ *n'a aucun inverse dans* $R[X]$.

d. Dans cette situation, indiquer un idéal propre $I \subseteq R[X]$ tel que $1 - aX \in I$.

√ *L'idéal principal* $I = (1 - aX) = (1 - aX)R[X]$ *de* $R[X]$ *est un idéal propre parce que* $1 - aX$ *n'est pas inversible ; il contient bien évidemment l'élément* $1 - aX$ *qui est son générateur.*

On admet qu'il existe dans $R[X]$ un idéal maximal qui contient cet idéal I (le théorème de Krull affirme cela pour tout idéal propre); on désigne par $\mathfrak{m}$ un tel idéal maximal de $R[X]$.

e. Expliquer que $a \notin \mathfrak{m}$ pour le polynôme constant $a \in R \subseteq R[X]$.

√ *On a en tout case* $1 - aX \in I \subseteq \mathfrak{m}$, *et si on avait aussi* $a \in \mathfrak{m}$, *alors aussi* $(1 - aX) + X \times a = 1 \in \mathfrak{m}$, *mais cela voudrait dire* $\mathfrak{m} = R$, *contredisant que* $\mathfrak{m}$ *est un idéal maximal (donc propre). Donc* $a \notin \mathfrak{m}$.

f. En déduire (toujours sous l'hypothèse que $a \in R$ n'est pas nilpotent) que l'anneau R contient un idéal premier $\mathfrak{p}$ avec $a \notin \mathfrak{p}$. (Attention qu'ici on *ne parle plus* de l'anneau $R[X]$.)

√ *L'idéal* $\mathfrak{m} \subseteq R[X]$ *est maximal, donc* $R[X]/\mathfrak{m}$ *est un corps. L'image du morphisme composé* $f : R \to R[X] \to R[X]/\mathfrak{m}$ *est un sous-anneau de ce corps, donc un anneau intègre. Le noyau de* f *est* $\mathfrak{p} = R \cap \mathfrak{m}$, *qui est donc un idéal premier, et il ne contient pas* a *(car* $\mathfrak{m}$ *ne le contient pas). On pourra aussi évoquer le résultat général que tout idéal premier coupe un sous-anneau dans un idéal premier du dernier (dont ce qu'on vient de dire fournit une preuve).*

3. Soit p un nombre premier avec $p \neq 2$. On pose $K = \mathbf{Z}/p\mathbf{Z}$, un corps fini à p éléments.

a. Pour $a \in K^\times$, montrer que a est racine du polynôme $X^2 + 1 \in K[X]$ si et seulement si l'ordre multiplicatif de a est 4 (c'est-à-dire $a^4 = 1$ pendant que $a^m \neq 1$ pour $0 < m < 4$).

b. Combien d'éléments possède l'anneau $R = K[X]/(X^2 + 1)$?

√ *Tout élément de* R *a un unique représentant de degré* < 1, *donc leur nombre est* $(\#K)^2 = p^2$.

c. Soit $A = \mathbf{Z}[i] \cong \mathbf{Z}[X]/(X^2 + 1)$ l'anneau des entiers de Gauss. Montrer que $R \cong A/pA$.

√ *Soit* $f : \mathbf{Z}[X] \to K[X]$ *le morphisme d'anneaux défini par la réduction modulo* p *des coefficients des polynômes, et* $g : K[X] \to K[X]/(X^2 + 1) = R$ *la projection canonique. Alors le noyau de* $g \circ f : \mathbf{Z}[X] \to R$ *contient l'idéal* $(X^2 + 1) \subseteq \mathbf{Z}[X]$, *donc* $g \circ f$ *passe au quotient, donnant un morphisme d'anneaux* $h : A \cong \mathbf{Z}[X]/(X^2 + 1) \to R$ *qui envoie* $a + b\mathbf{i} \mapsto g(f(a + bX))) = g(a_{[p]} + b_{[p]}X)$ *où les indices indiquent réduction modulo* p. *Ce morphisme* h *est surjectif, car* g *est surjectif et si pour* $P \in K[X]$ *son reste pour la division par* $X^2 + 1$ *est* r, *alors* $g(P) = g(r)$ *et* $\deg r < 2$ *implique que* r *est de la forme* $r = a_{[p]} + b_{[p]}X$. *Or* $\ker(h) = \{\, a + b\mathbf{i} \in A \mid a_{[p]} = b_{[p]} = 0 \,\} = pA$, *donc d'après le théorème d'isomorphisme* $R = \mathrm{im}(h) \cong A/\ker(h) = a/pA$.

d. Montrer que si $p \equiv 3 \pmod 4$, alors $X^2+1 \in K[X]$ est un polynôme irréductible.

$\surd$ *Si X^2+1 était réductible, c'est qu'il est produit de facteurs de degré 1, et donc qu'il possède des racines ; or d'après la question a ces racines, évidemment non nuls, seraient des éléments d'ordre 4 dans le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$, mais l'ordre $p-1$ de ce groupe n'est pas divisible par 4 donc cela n'est pas possible. N'étant pas non plus nul ou inversible, X^2+1 est irréductible.*

e. Montrer que si $p \equiv 1 \pmod 4$, alors il existe $u \in K$ tel que $X^2+1 = (X-u)(X+u)$ dans $K[X]$.

$\surd$ *Dans ce cas, le groupe $(\mathbf{Z}/p\mathbf{Z})^\times$ est d'ordre $p-1$ divisible par 4, et comme il est cyclique (théorème 1.5.10), il possède deux éléments d'ordre 4. Si $u \in K$ est un tel élément il vérifie $u^2+1=0$ (question a), et donc $(X-u)(X+u) = X^2+1$.*

f. Montrer que R est un corps si et seulement si $p \equiv 3 \pmod 4$.

$\surd$ *Comme $K[X]$ est un anneau principal, un quotient $K[X]/(P)$ avec $P \neq 0$ est un corps si et seulement si P est réductible (proposition 2.3.9). On a vient de voir que c'est le cas si et seulement si $p \equiv 3 \pmod 4$.*

g. Dans le cas de la question *e*, c'est-à-dire $p \equiv 1 \pmod 4$, appliquer le théorème chinois (théorème 2.1.8 du cours, mais avec $K[X]$ à la place de $\mathbf{Z}$) pour déduire que R est isomorphe à $K \times K$.

$\surd$ *On a $X^2+1 = (X-u)(X+u)$, où $X-u$ et $X+u$ sont distincts (car $u \neq 0$, ce qui en caractéristique impaire entraîne $u \neq -u$), donc (étant de degré 1 dans $K[X]$) premiers entre eux. D'après le théorèmes chinois on a alors $P \in K[X]/(X^2+1) \cong K[X]/(X-u) \times K[X]/(X+u)$. Or les deux facteurs du produit direct sont chacun isomorphe à K, l'image $\overline{P}$ d'un polynôme $P \in K$ étant sa valeur $P[X := u]$ en u (reste dans la division par $X-u$) dans le premier cas, et sa valeur en $-u$ dans le second cas.*

h. Ce qui précède montre que dans le cas $p \equiv 1 \pmod 4$ il existe un isomorphisme $A/pA \xrightarrow{\sim} K \times K$. Décrire explicitement cet isomorphisme (en termes de $u \in \mathbf{Z}/p\mathbf{Z}$ de la question *e*).

$\surd$ *Un élément de A/pA représenté par $a+b\mathbf{i} \in A$ correspond à $g(a_{[p]}+b_{[p]}X) \in R$, élément représenté par le polynôme $P = a_{[p]}+b_{[p]}X \in K[X]$, et ce polynôme correspond à la paire de valeurs $(P[X := u], P[X := -u]) = (a_{[p]}+b_{[p]}u, a_{[p]}-b_{[p]}u) \in K \times K$.*

Fin.