A02 : Correction de quelques exercices...

1 Quelques équations polynomiales.

1.1 Résoudre l'équation $2x^2 + 3x + 1 \equiv 0\ (27)$.

On résout successivement l'équation modulo 3, 9 et enfin 27. Modulo 3, les solutions sont 1 et 2.

modulo 9 : On commence par chercher les solutions modulo 9 qui sont congrues à 1 modulo 3. Ceci revient à poser $x = 3y + 1$ et l'équation $2x^2 + 3x + 1 \equiv 0\ (9)$ devient

$$2(3y + 1)^2 + 3(3y + 1) + 1 \equiv 0\ (9)$$

c'est-à-dire

$$12y + 6 \equiv 0 \quad (9)$$

ou encore $3y+6 \equiv 0\ (9)$. On peut simplifier cette équation par 3, on obtient ainsi $y+2 \equiv 0\ (3)$ d'où $y \equiv 1\ (3)$. En injectant ce résultat dans la relation $x = 3y + 1$ on en déduit $x \equiv 4\ (9)$.

On cherche maintenant les solutions modulo 9 qui sont congrues à 2 modulo 3. De même on pose $x = 3y + 2$. L'équation en y devient $6y + 6 \equiv 0\ (9)$. On peut simplifier par 3 ce qui donne $2y + 2 \equiv 0\ (3)$ donc $y \equiv 2\ (3)$ d'où $x \equiv 8\ (9)$. Donc les solutions modulo 9 sont 4 et 8.

Résolution de l'équation modulo 27 : On commence par chercher les solutions qui sont congrues à 4 modulo 9. On pose donc $x = 9y+4$ et on remplace dans l'équation $2x^2+3x+1 \equiv 0\ (27)$. On obtient une équation dont tous les coefficients sont multiples de 9. On peut donc simplifier par 9 et on trouve (après calcul) $y \equiv 1\ (3)$ soit $x \equiv 13\ (27)$.

On cherche ensuite les solutions qui sont congrues à 8 modulo 9. On pose donc $x = 9y + 8$ (ou $x = 9y - 1$ si l'on veut simplifier un peu les calculs) et on remplace dans l'équation $2x^2 + 3x + 1 \equiv 0\ (27)$. On obtient une équation dont tous les coefficients sont multiples de 9. On peut donc simplifier par 9 et on trouve (après calcul) $y \equiv 2\ (3)$ (ou bien $y \equiv 0\ (3)$ si l'on a posé $x = 9y - 1$) soit dans tous les cas $x \equiv 26\ (27)$.

Conclusion : Les solutions de l'équation initiale sont les entiers x qui sont congrus à 13 ou 26 modulo 27.

1.2 Résoudre l'équation $5x^2 + 3x + 1 \equiv 0\ (100)$.

La méthode générale consiste à décomposer 100 en facteurs premiers, $100 = 2^2 \times 5^2$, puis à résoudre séparément les équations polynomiales modulo 2^2 et modulo 5^2, et enfin à utiliser le théorème chinois pour en déduire les solutions de l'équation modulo 100.

modulo 2^2 : De même que dans l'équation précédente, on résout (avec un t !!) d'abord l'équation modulo 2, puis modulo 4. Modulo 2, l'équation devient

$$x^2 + x + 1 \equiv 0 \quad (2)$$

Cette équation n'a pas de solution. On peut donc s'arrêter là et conclure : l'équation $5x^2 + 3x + 1 \equiv 0\ (100)$ n'a pas de solutions (en effet s'il existait un entier x tel que $5x^2 + 3x + 1$ soit congru à 0 modulo 100, alors cet entier vérifierait aussi $x^2 + x + 1 \equiv 0\ (2)$).

1.3 Résoudre l'équation $x^2 + x + 1 \equiv 0\ (30)$.

Cette équation n'a déjà pas de solution modulo 2 donc elle ne peut en avoir modulo 30.

1.4 Une dernière pour s'entraîner...

Résoudre l'équation $x^2 + x \equiv 0\ (30)$. (Faites-le vraiment, sans regarder la réponse ! La solution se trouve à la fin de cette feuille...)

2 Correction du devoir maison.

2.1 Exercice 8 du paragraphe 3 de la feuille 4 (sur les triplets pythagoriciens).

1. Soit $d = \text{pgcd}\,(x, y)$. Alors d divise x et y donc d^2 divise x^2 et y^2, donc il divise aussi leur somme z^2. Si p est un nombre premier, on rappelle que l'on note $v_p(n)$ la valuation p-adique d'un entier n. Ici vu que d^2 divise z^2 on a pour tout nombre premier p :

$$v_p(d^2) \leq v_p(z^2)$$

ou encore

$$2v_p(d) \leq 2v_p(z)$$

donc $v_p(d) \leq v_p(z)$ pour tout p ce qui prouve que d divise z.

Vu que d divise aussi x et y, il divise $\text{pgcd}\,(x, y, z)$ (qui vaut 1) donc $d = 1$. On a montré que x et y sont premiers entre eux. En procédant de la même manière on montre que $\text{pgcd}\,(x, z) = 1$ et $\text{pgcd}\,(y, z) = 1$, si bien que x, y et z sont deux à deux premiers entre eux.

2. Comme x et y sont premiers entre eux, ils ne peuvent être tous les deux pairs. Par ailleurs, s'ils étaient tous les deux impairs on aurait $x^2 \equiv 1\ (4)$ et $y^2 \equiv 1\ (4)$ donc $z^2 \equiv 2\ (4)$, ce qui est impossible car le carré d'un entier est toujours congru à 0 ou 1 modulo 4.

On suppose dans la suite que x est pair et y impair.

3. Soit $d' = \text{pgcd}\,(z - y, z + y)$. Comme x est pair, z est nécessairement impair (car x et z sont premiers entre eux). Donc $z - y$ et $z + y$ sont tous les deux pairs. On en déduit que 2 divise d'. D'autre part, en regardant la somme et la différence de $z - y$ et $z + y$, on voit que d' divise $2z$ et $2y$, donc d' divise $\text{pgcd}\,(2y, 2z)$. Or ce pgcd est égal à $2.\text{pgcd}\,(y, z)$ c'est-à-dire à 2. On a montré que 2 divise d' et que d' divise 2, donc $\text{pgcd}\,(z - y, z + y) = 2$.

Montrons maintenant qu'il existe des entiers u et v vérifiant les propriétés annoncées. On pose $a = \frac{z+y}{2}$ et $b = \frac{z-y}{2}$. Les entiers a et b sont premiers entre eux. De plus on a

$$ab = \frac{(z + y)(z - y)}{4} = \left(\frac{x}{2}\right)^2$$

(n'oublions pas que x est pair !). Le produit ab est donc un carré. Nous allons montrer que a et b sont eux-mêmes des carrés. Digressons quelques instants et essayons de trouver une condition facile à vérifier permettant de déterminer si un entier positif n est un carré ou non. Si n est un carré, il existe par définition un entier α tel que n soit égal à α^2. Alors pour tout nombre premier p, on a

$$v_p(n) = v_p(\alpha^2) = 2v_p(\alpha)$$

donc la valuation p-adique de n est paire. En fait la réciproque est vraie. Supposons que pour tout p premier la valuation p-adique de n soit paire et montrons que n est un carré. On peut écrire

$$n = \prod_{p \in \mathcal{P}} p^{v_p(n)} = \prod_{p \in \mathcal{P}} (p^{\frac{v_p(n)}{2}})^2 = \left(\prod_{p \in \mathcal{P}} p^{\frac{v_p(n)}{2}}\right)^2$$

si bien que n est un carré (bien sûr, ce calcul ne marche pas si l'on ne suppose pas que la valuation p-adique de n est paire pour tout p car alors rien ne garantirait que $\frac{v_p(n)}{2}$ soit un nombre entier) !

Revenons à nos moutons. Pour montrer que a et b sont des carrés il suffit donc de montrer qu'ils sont positifs (ce qui est vrai car z est supérieur à y vu l'équation qu'ils vérifient) et surtout que pour tout nombre premier p les entiers $v_p(a)$ et $v_p(b)$ sont pairs. Soit p un nombre premier. On sait que le produit ab est un carré donc $v_p(ab) = v_p(a)+v_p(b)$ est pair. Supposons que l'un des deux soit non nul par exemple supposons $v_p(a) > 0$ (si $v_p(a)$ et $v_p(b)$ sont nuls il est évident qu'ils sont pairs). Alors $v_p(b) = 0$ car a et b sont premiers entre eux (si $v_p(b)$ était non nul alors p diviserait le pgcd de a et b). Or on a vu que $v_p(a) + v_p(b)$ est pair donc $v_p(a)$ est pair (et $v_p(b)$ est pair aussi puisqu'il est nul).

Nous avons montré que a et b sont des carrés. Il existe donc des entiers u et v positifs tels que $a = u^2$ et $b = v^2$. On a alors $z + y = 2u^2$, $z - y = 2v^2$ et $u^2v^2 = ab = (\frac{x}{2})^2$ d'où $x = 2uv$.

Remarque : On en déduit que le triplet (x, y, z) est égal à $(2uv, u^2 - v^2, u^2 + v^2)$. De plus u et v sont premiers entre eux puisque leur pgcd divise celui de u^2 et v^2 qui est égal à 1. Enfin l'un au moins de u et v est pair. En effet si u et v étaient tous les deux impairs alors $y = u^2 - v^2$ serait pair.

4. Réciproquement, supposons que u et v sont deux entiers premiers entre eux, dont l'un au moins est pair et avec $u > v > 0$ (ces hypothèses sont nécessaires, il y a une erreur dans l'énoncé). Montrons que le triplet (x, y, z) donné par $x = 2uv$, $y = u^2 - v^2$ et $z = u^2 + v^2$ est un triplet pythagoricien. Ce sont trois entiers strictement positifs, et un calcul facile montre qu'ils vérifient la relation

$$x^2 + y^2 = z^2.$$

Il reste juste à montrer qu'ils sont premiers entre eux dans leur ensemble. Raisonnons par l'absurde et supposons que $\text{pgcd}\,(x, y, z)$ est différent de 1. Soit p un facteur premier de ce pgcd. Il divise $u^2 - v^2$ qui est impair (car u et v sont de parités différentes) donc $p \neq 2$. Il divise $u^2 - v^2$ et $u^2 + v^2$ donc en faisant la somme il divise $2u^2$. Comme $p \neq 2$, on en déduit que p divise u^2, puis que p divise u. De même en prenant la différence au lieu de la somme on voit que p divise v. Ceci contredit le fait que u et v sont premiers entre eux.

Conclusion : Nous avons réussi à *paramétrer* l'ensemble des triplets pythagoriciens. En effet les triplets pythagoriciens sont exactement les triplets $(2uv, u^2 - v^2, u^2 + v^2)$ où u et v sont deux entiers premiers entre eux, dont l'un au moins est pair et vérifiant $u > v > 0$. Par exemple le triplet $(x, y, z) = (4, 3, 5)$ correspond au couple $(u, v) = (2, 1)$. En prenant $(u, v) = (3, 2)$ nous obtenons le triplet $(12, 5, 13)$. Avec $(u, v) = (4, 1)$ on trouve le triplet $(8, 15, 17)$, etc... En énumérant la liste des couples (u, v) possibles on trouve la liste de *tous* les triplets pythagoriciens.

2.2 Exercice supplémentaire sur les relations d'équivalence.

On note S l'ensemble des entiers relatifs u tels que 3 ne divise pas u.

$$S = \{u \in \mathbb{Z} \mid v_3(u) = 0\}$$

On définit sur $\mathbb{Z} \times S$ une relation $\mathcal{R}$ de la manière suivante. Pour tous couples (a, b) et (c, d) appartenant à $\mathbb{Z} \times S$ on dit que (a, b) est en relation avec (c, d) et on note $(a, b)\mathcal{R}(c, d)$ si et seulement s'il existe un entier u appartenant à S tel que $u(ad - bc)$ soit congru à 0 modulo 24. En langage mathématique, ceci peut s'écrire :

$$(a, b)\mathcal{R}(c, d) \iff \exists u \in S \text{ tel que } u(ad - bc) \equiv 0 \quad (24)$$

Nous allons montrer que $\mathcal{R}$ est une relation d'équivalence. Il ne faut pas paniquer : c'est juste un exercice de « recopiage » des définitions (bien sûr, il faut tout de même connaître la définition d'une relation d'équivalence). Une relation d'équivalence est une relation qui est réflexive, symétrique et transitive.

Réflexivité : Il s'agit de montrer que pour tout couple (a, b) appartenant à $\mathbb{Z} \times S$ on a $(a, b)\mathcal{R}(a, b)$. Pour l'instant il n'y a pas à réfléchir, on se rappelle que pour montrer une assertion qui commence par « Pour tout truc appartenant à machin... », on commence par écrire « Soit Bidule un truc appartenant à machin... ». La première phrase de notre démonstration sera donc la suivante :

> « Soit (a, b) appartenant à $\mathbb{Z} \times S$. »

Mais au fait, que voulait-on montrer au sujet de ce couple (a, b) ? Ah oui ! On veut montrer que $(a, b)\mathcal{R}(a, b)$. Éventuellement on peut l'écrire, pour être sûr de bien savoir ce que l'on fait (ou pour que le correcteur soit sûr que vous savez bien ce que vous faites). Donc notre seconde phrase sera :

> « Montrons que $(a, b)\mathcal{R}(a, b)$. »

Mais qu'est-ce que ça veut dire, $(a, b)\mathcal{R}(a, b)$? Là on recopie la définition (en remplaçant c par a et d par b)...

> « Ceci revient à dire qu'il existe u appartenant à S tel que $u(ab - ba)$ soit congru à 0 modulo 24. »

On s'aperçoit alors que $ab - ba$ est nul, si bien que la condition « tel que $u(ab - ba)$ soit congru à 0 modulo 24 » est toujours vérifiée. A-t-on terminé pour autant ? Pas tout à fait ! Reprenons la phrase ci-dessus et regardons-la de plus près. On peut supprimer le morceau de phrase « tel que $u(ab - ba)$ soit congru à 0 modulo 24 » puisque nous venons de dire que cette condition est toujours vérifiée. Il nous reste donc à montrer qu'il existe u appartenant à S. Autrement dit que S est non vide ! ! Nous avons progressé dans le raisonnement donc nous l'écrivons (toujours pour être sûr que le correcteur nous suit).

> « Vu que $ab - ba$ est nul, ceci revient à dire qu'il existe u appartenant à S. Autrement dit il faut montrer que S est non vide. »

Maintenant on réfléchit un tout petit peu... S est-il non vide ? Bien sûr ! Par exemple 1 appartient à S puisque 3 ne divise pas 1. Nous l'écrivons, et en mettant les phrases bout à bout nous obtenons la démonstration suivante :

> « Soit (a, b) appartenant à $\mathbb{Z} \times S$. Montrons que $(a, b)\mathcal{R}(a, b)$. Ceci revient à dire qu'il existe u appartenant à S tel que $u(ab - ba)$ soit congru à 0 modulo 24. Vu que $ab - ba$ est nul, ceci revient à dire qu'il existe u appartenant à S. Autrement dit il faut montrer que S est non vide. Or 3 ne divise pas 1 donc 1 est un élément de S, ce qui prouve que S est non vide. »

Vous remarquerez que les seuls étapes qui n'étaient pas purement formelles, c'est-à-dire les seules étapes où il a fallu réfléchir un peu, étaient le constat $ab - ba = 0$ et la recherche d'un entier qui n'était pas multiple de 3.

Symétrie : Reprenons notre jeu de recopiage. On commence par écrire (par exemple sur un brouillon ou sur notre copie) la définition de la symétrie, ou plus exactement ce que cela signifie pour $\mathcal{R}$. Dire que $\mathcal{R}$ est symétrique, c'est dire que pour tous couples (a, b) et (c, d) appartenant à $\mathbb{Z} \times S$, $(a, b)\mathcal{R}(c, d)$ implique $(c, d)\mathcal{R}(a, b)$. Là, le début de cette phrase (« pour tout... ») déclenche un réflexe pavlovien et nous écrivons sans réfléchir davantage :

> « Soient (a, b) et (c, d) des éléments de $\mathbb{Z} \times S$. Montrons que $(a, b)\mathcal{R}(c, d)$ implique $(c, d)\mathcal{R}(a, b)$. »

Ici encore, vous devez avoir ce réflexe : pour montrer une assertion de la forme « truc implique bidule » on commence par « On suppose truc, montrons bidule. »

> « On suppose $(a, b)\mathcal{R}(c, d)$. Montrons que $(c, d)\mathcal{R}(a, b)$. »

Continuons et traduisons dans un langage intelligible ce que nous venons d'écrire. D'abord avec les hypothèses...

> « On sait par hypothèse qu'il existe un entier u appartenant à S tel que $u(ad-bc)$ soit congru à 0 modulo 24. »

... puis avec la conclusion que l'on veut obtenir. Mais attention aux notations !! Maintenant nous avons fixé un entier u appartenant à S et la notation u est réservée. On ne peut plus utiliser la lettre u pour désigner autre chose. Traduisons la phrase « Montrons que $(c,d)\mathcal{R}(a,b)$. » en respectant cette consigne.

> « On veut montrer qu'il existe un entier u' appartenant à S tel que $u'(cb-da)$ soit congru à 0 modulo 24. »

On constate alors que $cb-da=-(ad-bc)$ ce qui nous invite aussitôt à penser que le choix $u'=-u$ pourrait répondre à nos attentes. A-t-on fini pour autant ? Presque... Si l'on regarde avec attention ce que l'on veut montrer, on s'aperçoit qu'il nous faut tout de même vérifier que $-u$ est bien un élément de S. Nous pouvons dès lors achever la rédaction de notre démonstration.

> « On pose $u'=-u$. Comme 3 ne divise pas u, il ne divise pas non plus u' donc u' est un élément de S. De plus la relation $u(ad-bc)\equiv 0$ (24) entraîne $u'(cb-da)\equiv 0$ (24), ce qu'il fallait démontrer. »

En mettant les morceaux bout à bout on obtient la démonstration suivante.

> « Soient (a,b) et (c,d) des éléments de $\mathbb{Z}\times S$. Montrons que $(a,b)\mathcal{R}(c,d)$ implique $(c,d)\mathcal{R}(a,b)$. On suppose $(a,b)\mathcal{R}(c,d)$. Montrons que $(c,d)\mathcal{R}(a,b)$. On sait par hypothèse qu'il existe un entier u appartenant à S tel que $u(ad-bc)$ soit congru à 0 modulo 24. On veut montrer qu'il existe un entier u' appartenant à S tel que $u'(cb-da)$ soit congru à 0 modulo 24. On pose $u'=-u$. Comme 3 ne divise pas u, il ne divise pas non plus u' donc u' est un élément de S. De plus la relation $u(ad-bc)\equiv 0$ (24) entraîne $u'(cb-da)\equiv 0$ (24), ce qu'il fallait démontrer. »

Transitivité : En contemplant la définition de la transitivité, on voit que dire que $\mathcal{R}$ est transitive signifie la chose suivante. « Pour tous couples (a,b), (c,d) et (e,f) appartenant à $\mathbb{Z}\times S$, si $(a,b)\mathcal{R}(c,d)$ et $(c,d)\mathcal{R}(e,f)$ alors $(a,b)\mathcal{R}(e,f)$. Le jeu de recopiage qui commence à devenir familier nous permet d'écrire sans réfléchir le début d'une démonstration.

> « Soient (a,b), (c,d) et (e,f) appartenant à $\mathbb{Z}\times S$ tels que $(a,b)\mathcal{R}(c,d)$ et $(c,d)\mathcal{R}(e,f)$. Montrons que $(a,b)\mathcal{R}(e,f)$. On sait par hypothèse qu'il existe u_1 et u_2 appartenant à S tels que $u_1(ad-bc)\equiv 0$ (24) et $u_2(cf-de)\equiv 0$ (24). On veut montrer qu'il existe un entier u_3 appartenant à S tel que $u_3(af-be)\equiv 0$ (24). »

Vous remarquerez ici encore l'importance cruciale de la consigne : « ne pas réutiliser un symbole qui est déjà en cours d'utilisation ». Ici l'erreur à ne pas faire aurait été de désigner les éléments u_1, u_2 et u_3 par la même lettre u. Comment aurait-on pu les distinguer ensuite ? ?

Maintenant, je le reconnais, il faut réfléchir un tout petit peu, mais seulement maintenant. Tout ce qui précède n'est, je le répète, qu'un exercice bête et méchant de formalisme qui deviendra automatique avec un peu d'habitude. On peut achever la démonstration ainsi.

> « On multiplie l'équation $u_1(ad-bc)\equiv 0$ (24) par u_2f et l'équation $u_2(cf-de)\equiv 0$ (24) par u_1b, puis on additionne les deux équations obtenues. Les termes u_1u_2bcf disparaissent et nous obtenons l'équation $u_1u_2(adf-bde)\equiv 0$ (24), ou encore :
>
> $$u_1u_2d(af-be)\equiv 0 \quad (24).$$
>
> Comme u_1, u_2 et d sont des éléments de S, aucun d'eux n'est multiple de 3. Donc 3 ne divise pas non plus leur produit puisque c'est un nombre premier. On peut donc poser $u_3=u_1u_2d$, c'est un élément de S car il n'est pas multiple de 3, et le calcul ci-dessus montre que $u_3(af-be)\equiv 0$ (24). »

3 Résolution de l'équation $x^2 + x \equiv 0 \quad (30)$.

On décompose 30 en facteurs premiers : $30 = 2 \times 3 \times 5$. La première étape consiste à résoudre cette équation modulo 2, 3 et 5.
Modulo 2 : Les solutions sont 0 et 1.
Modulo 3 : Les solutions sont 0 et 2.
Modulo 5 : Les solutions sont 0 et 4.

Il y a donc huit possibilités pour le triplet ($x \bmod 2, x \bmod 3, x \bmod 5$), à savoir $(0,0,0)$, $(0,0,4)$, $(0,2,0)$, $(0,2,4)$, $(1,0,0)$, $(1,0,4)$, $(1,2,0)$ et $(1,2,4)$. À chacun de ces triplets correspond une unique solution modulo 30. Par exemple pour le triplet $(0,2,4)$ il faut résoudre le système

$$\begin{cases} x & \equiv & 0 & (2) \\ x & \equiv & 2 & (3) \\ x & \equiv & 4 & (5) \end{cases}$$

Notez que chacun de ces systèmes peut être résolu de tête assez rapidement comme suit. L'entier x que l'on cherche est compris entre 0 et 29. On commence par résoudre le système correspondant aux équations modulo 2 et modulo 5, ce qui nous donne le reste de x modulo 10. Par exemple pour $(0,2,4)$ on commence par résoudre le système

$$\begin{cases} x & \equiv & 0 & (2) \\ x & \equiv & 4 & (5) \end{cases}$$

dont la solution est $x \equiv 4$ (10) (la seconde ligne donne $x \equiv 4$ ou $x \equiv 9$, la première permet de trancher). Le dernier chiffre de x est donc 4. La congruence modulo 3 nous dit par ailleurs que la somme des chiffres de x doit être congrue à 2 modulo 3. On en déduit que le premier chiffre est 1, d'où $x = 14$. Les résultats des huit systèmes sont rassemblés dans le tableau ci-dessous.

$x \bmod 2$	0	0	0	0	1	1	1	1
$x \bmod 3$	0	0	2	2	0	0	2	2
$x \bmod 5$	0	4	0	4	0	4	0	4
$x \bmod 10$	0	4	0	4	5	9	5	9
$x \bmod 30$	0	24	20	14	15	9	5	29

Finalement notre équation a huit solutions modulo 30, à savoir 0, 5, 9, 14, 15, 20, 24 et 29.