UTM - Département de Mathématiques et d'Informatique **Année 2005-06**
L.1 - M.A.S.S - Algèbre S1 - session 2
Alain COUVREUR : couvreur@univ-tlse2.fr
Page Perso : http ://www.univ-tlse2.fr/grimm/couvreur

Corrigé du Devoir Maison

Exercice 1. Implications et équivalences

Solutions.

(i)	$pgcd(p_1,\dots,p_n)=1$	$\iff$	les entiers $p_1,\dots,p_n$ sont deux à deux premiers entre eux.
(ii)	$p\|a$ ou $p\|b$	$\implies$	$p\|ab$
(iii)	$p\|a$ ou $p\|b$	$\impliedby$	$p\|ab$ et p est un nombre premier.
(iv)	$a=8$	$\implies$	$a\equiv 3 \bmod 5$.
(v)	$c\|a$ et $c\|b$	$\iff$	$c\|\text{pgcd}(a,b)$.
(vi)	$a\nmid b$	$\implies$	$\exists p\in\mathbb{Z},\ b\neq ap$.
(vii)	$\exists(u,v)\in\mathbb{Z}^2,\ d=au+bv$	$\impliedby$	$d=a\wedge b$.

Justifications

(i). C'est la définition de "deux à deux premiers entre eux".

(ii). Supposons par exmple que $p|a$, alors il existe un entier s tel que $a=ps$, donc $ab=psb$, donc $p|ab$, la démonstration est exactement similaire si $p|b$. La réciproque est fausse car par exemple $6|12=4\times 3$ mais $6\nmid 3$ et $6\nmid 4$.

(iii). L'implication vers la gauche est vraie, c'est une conséquence directe de la décomposition d'un entier en facteurs premiers. La réciproque est évidemment fausse, en général, le fait que $p|a$ ou $p|b$ n'implque en aucun cas que p est premier.

(iv). L'implication est immédiate, il suffit de savoir réduire 8 modulo 5. La réciproque est fausse, engénéral on en peut pas déduire une égalité d'une congruence. Ici par exemple $13\equiv 3 \bmod 5$ mais $13\neq 8$.

(v). Si $c|a$ et $c|b$ alors c est un diviseur commun de a et de b il divise donc le $\text{pgcd}(a,b)$. Réciproquement, si $c|\text{pgcd}(a,b)$, il divise un entier qui divise a et b, par transitivité de la relation de divisibilité, $c|a$ et $c|b$.

(vi). L'implication vers la droite est vraie même si elle est quelque peu stupide : si je prends deux entiers a et b non nuls, je peux toujours trouver un troisième entier p tel que $a\neq b$ il n'est en fait pas nécessaire d'ajouter une quelconque condition. La réciproque est biensur fausse car si $a=2$ et $b=4$ il existe bien $p\in\mathbb{Z},\ b\neq ap$ (par exemple $p=3$) mais $a|b$. Remarquez par contre qu'il y a équivalence si on remplace le "$\exists$" de l'assertion de gauche par un "$\forall$" ! (pourquoi ?)

(vii). L'implication ves la gauche n'est autre que le théorème de Bezout. La réciproque est fausse si je prends $a=2$, $b=3$, $u=v=1$, on obtient $au+bv=2+3=5$ or $2\wedge 3=1$.

Exercice 2. Quelques problèmes de divisibilité.

1. $a(a^2-1)=a(a-1)(a+1)$, c'est un produit de trois entiers successifs, l'un d'entre eux est un multiple de 3 et au moins l'un d'entre eux est multiple de 2. Comme 2 et 3 sont premiers entre eux, d'après le lemme de Gauss, s'ils divsent tous deux $a(a^2-1)$, alors leur produit divise $a(a^2-1)$. On a bien $6|a(a^2-1)$

2. $a(a^{2n}-1)=a(a^n-1)(a^n+1)=a(a-1)(1+a+\cdots+a^{n-1})(a^n+1)$. Les deux premiers termes de ce produit sont deux entiers successifs, l'un d'entre eux est pair, donc $2|a(a^{2n}-1)$. Ensuite, il y a trois cas de figure :

1. Si $a\equiv 0$ [3], alors $3|a$, et immédiatement $3|a(a^{2n}-1)$.
2. Si $a\equiv 1$ [3], alors $a^{2n}-1\equiv 1^{2n}-1\equiv 0$ [3], donc $3|a(a^{2n}-1)$.
3. Si $a\equiv 1$ [3], alors $a^{2n}-1\equiv 2^{2n}-1\equiv 4^n-1\equiv 1^n-1$[3], donc $3|a(a^{2n}-1)$.

Ainsi quoi qu'il arrive $3|a(a^{2n}-1)$, donc par un raisonnement analogue à celui de la question précédente on démontre que $6|a(a^{2n}-1)$

3. $n(n+1)(n+2)(n+3)$, dans ce produit de 4 entiers successifs, l'un d'entre eux au moins est multiple de 3, ensuite parmi ces nombres il y a forcément un couple de deux nombres pairs successifs, leur produit est divisible par 8 (c.f. remarque de l'énoncé). Donc comme 3 et 8 sont premiers entre eux $24|n(n+1)(n+2)(n+3)$.

4. D'après la question précédente, on sait que $24|n(n+1)(n+2)(n+3)(n+4)$, de plus ce nombre est un produit de cinq entiers successifs, l'un d'entre eux est divisible par 5. Comme 5 et 24 sont premiers entre eux, leur produit divise $n(n+1)(n+2)(n+3)(n+4)$.

5. Soit$n \in \mathbb{N},\ n^3 - n = n(n^2-1)$, donc d'après la question 1. $\forall n \in \mathbb{N},\ 6|n^3 - 1$.

6. Soit $n \in \mathbb{N},\ n^5 - n = n(n^4-1) = n(n^2-1)(n^2+1) = n(n-1)(n+1)(n^2+1)$. Posons $p = n^5 - n$. D'après les questions précédentes on sait que $6|p$. Ensuite il y a cinq cas de figure :

1. Si $n \equiv 0\ [5]$, alors $5|n$, donc $5|p$.
2. Si $n \equiv 1\ [5]$, alors $5|n-1$ et donc $5|p$.
3. Si $n \equiv 2\ [5]$, alors $n^2+1 \equiv 5 \equiv 0\ [5]$ donc $5|n^2+1$ et $5|p$.
4. Si $n \equiv 3\ [5]$, alors $n^2+1 \equiv 10 \equiv 0\ [5]$ donc $5|n^2+1$ et $5|p$.
5. Si $n \equiv 4\ [5]$, alors $5|n+1$ et donc $5|p$.

Donc $5|p$, et comme 5 et 6 sont premiers entre eux $30|n^5 - n$

7. Soient $m \geq 1$ et $n \geq 2$ des entiers. $(n^m - 1) = (n-1)(1 + n + \cdots + n^{m-1})$. Donc $(n-1)|(n^m - 1)$.

8. n est un entier impair, donc il existe $k \in \mathbb{N},\ n = 2k+1$. Et :

$$\begin{aligned} 7^n + 1 &= 7^{2k+1} + 1 = 49^k.7 + 1 \\ &\equiv 1^k.7 + 1\ [8] \\ &\equiv 0\ [8] \end{aligned}$$

Donc $8|7^n + 1$.

9. n est un entier pair, donc il existe $k \in \mathbb{N}$ tel que $n = 2k$

$$\begin{aligned} 7^n + 1 &= 7^{2k} + 1 = 49^k.7 + 1 \\ &\equiv 1^k + 1\ [8] \\ &\equiv 1\ [8] \end{aligned}$$

Le reste de la division de $7^n + 1$ par 8 est égal à 1.

10. Décomposons a et b en facteurs premiers,

$$a = \prod_{p \in \mathcal{P}} p^{\alpha_p} \qquad b = \prod_{p \in \mathcal{P}} p^{\beta_p}$$

.

Où les α_p et les β_p sont tous nuls sauf un nombre fini d'entre eux. On en déduit ainsi les décompositions en facteurs premiers de a^2 et b^2 :

$$a^2 = \prod_{p \in \mathcal{P}} p^{2\alpha_p} \qquad b^2 = \prod_{p \in \mathcal{P}} p^{2\beta_p}$$

.

Dire que $a^2|b^2$ revient à dire que $\forall p \in \mathcal{P},\ 2\alpha_p \leq 2\beta_p$
Donc : $\forall p \in \mathcal{P},\ \alpha_p \leq \beta_p$. Donc $a|b$.

Exercice 3. Problèmes de congruences.

1. Soit n un entier dont le reste par la division par 15 est égal à 6, raisonnons par l'absurde, supposons que le reste de la division de n par 18 est égal à 5. En d'autres termes,

$$\begin{cases} n \equiv 6\ [15] \\ n \equiv 5\ [18] \end{cases}$$

Dire que $n \equiv 6\ [15]$ revient à dire qu'il existe un entier p tel que $n = 15p + 6$ ce qui signifie entre autre que $3|n$ (ou, ce qui revient au même que $n \equiv 0\ [3]$). Dire que $n \equiv 5\ [18]$ revient à dire qu'il existe un entier p tel que $n = 18p + 5$, donc que $n \equiv 5 \equiv 2\ [3]$. Ce qui contredit le fait que $3|n$. Le reste de la division de n par 18 ne peut être 5.

2. Soit n, un entier de la forme $n = 6k + 5$ où $k \in \mathbb{Z}$ (i.e. $n \equiv 5\ [6]$). Alors :

$$n \equiv 5 \equiv -1\ [3]$$

Donc il existe bien un entier k' tel que $n = 3k' - 1$.

3. Non. Prenez par exemple $n = 2$, on a bien $n \equiv -1\ [3]$, mais n n'est pas congru à -1 modulo 6.

4. Soit n, un entier de la forme $n = 5k + 1$ où $k \in \mathbb{Z}$. Alors :

$$n \equiv 1\ [5] \quad \text{et} \quad n^2 \equiv 1^2 \equiv 1\ [5]$$

Par conséquent il existe un entier k' tel que $n^2 = 5k' + 1$.

5. Soit n un entier, il y a quatre cas de figure possibles :

1. $n \equiv 0\ [4]$, dans ce cas $n^2 \equiv 0\ [4]$
2. $n \equiv 1\ [4]$, dans ce cas $n^2 \equiv 1^2 \equiv 1\ [4]$
3. $n \equiv 2\ [4]$, dans ce cas $n^2 \equiv 4 \equiv 0\ [4]$
4. $n \equiv 3\ [4]$, dans ce cas $n^2 \equiv 9 \equiv 1\ [4]$

Donc le carré d'un entier est bien toujours congru à 0 ou à 1 modulo 4.

6. Soit a un entier naturel qui est à la fois un carré et un cube, c'est à dire qu'il existe b et c tels que $a = b^2 = c^3$. Ecrivons les décompositions en facteurs premiers de b et c,

$$b = \prod_{p \in \mathcal{P}} p^{\beta_p} \qquad c = \prod_{p \in \mathcal{P}} p^{\gamma_p}$$

.

Où les β_p et les γ_p sont tous nuls sauf un nombre fini d'entre eux. Le fait que $b^2 = c^3$ signifie que pour tout $p \in \mathcal{P}$, $2\beta_p = 3\gamma_p$. Comme 2 et 3 sont premiers entre eux, d'après le lemme de Gauss :

$$\forall p \in \mathcal{P},\ 2|\gamma_p \text{ donc } \exists \gamma'_p,\ \gamma_p = 2\gamma'_p$$

.

Donc $a = c^3 = \prod p^{6\gamma'_p}$, c'est donc une puissance sixième. Ensuite un raisonnement similaire à celui de la question précédente (il faudra traiter sept cas cette fois ci !) permet de montrer qu'une puissance sixième d'un entier est toujours congrue à 0 ou 1 modulo 7.

Exercice 4. L'agorithme d'Euclide dans $\mathbb{Z}$.

1. $\text{pgcd}(28, 148) = 4$, et $16.28 - 3.148 = 4$
2. $\text{pgcd}(27, 237) = 3$, et $-35.27 + 4.237 = 3$
3. $\text{pgcd}(91, 911) = 1$, et $911 - 10.91 = 1$
4. $\text{pgcd}(126, 230) = 2$, et $42.126 - 23.230 = 2$
5. $\text{pgcd}(18480, 9828) = 84$, et $25.18480 - 47.9828 = 84$

Exercice 5. fractions rationnelles

Sur $\mathbb{R}$.

$F_1 = 1 - \frac{1}{X+2} - \frac{3}{X-1}$

$G_1 = X^2 - 3X + 7 + \frac{2}{X+1} - \frac{17}{X+2}$

$H_1 = \frac{1/2}{X-1} - \frac{4}{X-2} + \frac{9/2}{X-3}$

$F_2 = -\frac{1}{(X-1)^3} - \frac{2}{(X-1)^2} - \frac{2}{X-1} + \frac{2}{X-2}$

$G_2 = \frac{3/8}{(X-1)^3} - \frac{5/16}{(X-1)^2} + \frac{3/16}{X-1} + \frac{1/8}{(X+1)^3} - \frac{1/16}{(X+1)^2} - \frac{3/16}{X+1}$

$H_2 = X + 1 + \frac{1/3}{X+1} - \frac{X+1}{3(X^2-X+1)}$

$F_3 = -\frac{1}{X^2+1} + \frac{X+1}{X^2+X+1}$

$G_3 = \frac{X+4}{(X^2+X+1)^2} + \frac{X-1}{X^2+X+1}$

$H_3 = -\frac{1/3}{(X+1)^2} + \frac{2/3}{X+1} - \frac{2X-5}{3(X^2-X+1)}$

Sur $\mathbb{C}$, les décompositions de $F1, G1, H1, F2$ et $G2$ sont identiques.