



**Structures mathématiques**

Corrigé de l'examen du 27 mai 2005

1. Question de cours: voir le cours.
2. (a) Pour  $x, y$  réels,  $xy - x - y + 2$  est bien un réel, donc  $\star$  est bien une loi de composition interne. Il est facile de voir que pour tous  $x, y$  réels,  $x \star y = y \star x$ . Posons  $F(x, y, z) = (x \star y) \star z$ : on a

$$\begin{aligned} F(x, y, z) &= (xy - x - y + 2)z - (xy - x - y + 2) - z + 2 \\ &= xyz - xz - yz + 2z - xy + x + y - z \\ &= xyz - (xz + xy + yz) + (x + y + z) \end{aligned}$$

Comme  $\star$  est commutative,  $x \star (y \star z) = (y \star z) \star x = F(y, z, x)$ . D'après le calcul fait ci-dessus,  $F(x, y, z) = F(y, z, x)$ , ce qui montre que  $\star$  est associative.

- (b) Il est facile de voir que  $u = 2$  est la seule solution.
  - (c) Reste à vérifier que 2 est bien l'élément neutre. Pour tout  $x$  dans  $\mathbb{R}$ , on a  $2 \star x = x \star 2 = 2x - x - 2 + 2 = x$ .
3. (a) Montrons que pour tout entier naturel  $k$ ,  $2^k \geq 1 + k$ . Pour  $k = 0$   $2^0 = 1 \geq 1 + 0$ . Maintenant, pour  $k \geq 0$ , la propriété est héréditaire:  $2^{k+1} = 2 \cdot 2^k \geq 2(k + 1) = 2k + 2 \geq k + 2 = (k + 1) + 1$ .
  - (b) Soit  $n$  un entier naturel non nul tel que  $n$  divise  $2^n$ . Soit  $p$  un diviseur premier de  $n$ . Comme  $p$  divise  $n$  et  $n$  divise  $2^n$ ,  $p$  divise  $2^n$ . Mais le seul diviseur premier de  $2^n$  est 2, donc  $p = 2$ . Ainsi 2 est le seul diviseur premier de  $n$ , ce qui entraîne l'existence d'un entier  $k$  non nul tel que  $n = 2^k$ .  
Réciproquement, si  $n = 2^k$  pour un certain entier  $k$  non nul, on a  $2^n / n = 2^{2^k} / 2^k = 2^{2^k - k} \in \mathbb{N}$  car  $2^k - k > 0$ .
4. Soient  $a$  et  $b$  deux tels entiers: comme 7 divise  $a$  et  $b$ , il existe des entiers  $a'$  et  $b'$  avec  $a = 7a'$  et  $b = 7b'$ . On a  $(a \wedge b) = 7(a' \wedge b')$  et  $(a \vee b) = 7(a' \vee b')$ , d'où  $a' \wedge b' = 1$  et  $a' \vee b' = 10$ . Réciproquement, si  $a' \wedge b' = 1$  et  $a' \vee b' = 10$ , on a bien  $a \wedge b = 7$  et  $a \vee b = 70$ . On s'est donc ramené à un problème équivalent: résoudre  $a' \wedge b' = 1$  et  $a' \vee b' =$

10 Mais comme on a toujours  $a'b' = (a' \wedge b')(a' \vee b')$ , ce système est équivalent à On a alors  $a'b' = 10$  et  $a' \wedge b' = 1$ . Mais 10 se décompose en produit de facteurs premiers en  $10 = 5 \times 2$ , donc les solutions pour le couple  $(a', b')$  sont exactement:  $(1, 10), (2, 5), (5, 2), (10, 1)$ , soit pour  $(a, b)$ :  $(7, 70), (14, 35), (35, 14), (7, 70)$ .

5. (a) Il suffit de montrer que dans  $\mathbb{Z}/5\mathbb{Z}$ , on a  $\overset{\circ}{a}^b = \overset{\circ}{a}^{\overset{\circ}{b}'}$ . Comme  $a$  et  $a'$  sont congrus modulo 5, on a déjà  $\overset{\circ}{a} = \overset{\circ}{a}'$ . Comme  $\overset{\circ}{a}^b = \overset{\circ}{a}^b$  et  $\overset{\circ}{a}^{\overset{\circ}{b}'} = \overset{\circ}{a}^{\overset{\circ}{b}'}$ , il suffit alors de montrer que  $\overset{\circ}{a}^b = \overset{\circ}{a}^{\overset{\circ}{b}'}$ . Quitte à échanger les rôles, on peut supposer que  $b' \geq b$ : on a alors  $\overset{\circ}{a}^{\overset{\circ}{b}'} = \overset{\circ}{a}^b \cdot \overset{\circ}{a}^{b'-b}$ . Comme  $b$  et  $b'$  sont congrus modulo 4, il existe un entier  $n$  tel que  $b' - b = 4n$ . Ainsi

$$\overset{\circ}{a}^{\overset{\circ}{b}'} = \overset{\circ}{a}^b \cdot \overset{\circ}{a}^{4n} = \overset{\circ}{a}^b \cdot (\overset{\circ}{a}^4)^n.$$

Si  $\overset{\circ}{a} = 0$ , alors  $\overset{\circ}{a}^b = 0 = \overset{\circ}{a}^{\overset{\circ}{b}'}$ . Sinon  $a \in \{1, 2, 3, 4\}$  et donc  $a$  est premier avec 5: d'après le théorème d'Euler, on a donc dans  $\mathbb{Z}/5\mathbb{Z}$ :  $\overset{\circ}{a}^4 = \overset{\circ}{a}^{\phi(5)} = \overset{\circ}{1}$ , d'où

$$\overset{\circ}{a}^{\overset{\circ}{b}'} = \overset{\circ}{a}^b \cdot (\overset{\circ}{a}^4)^n = \overset{\circ}{a}^b \cdot \overset{\circ}{1}^n = \overset{\circ}{a}^b.$$

(b)

$ab$	0	1	2	3
1	$\overset{\circ}{1}$	$\overset{\circ}{1}$	$\overset{\circ}{1}$	$\overset{\circ}{1}$
2	$\overset{\circ}{1}$	$\overset{\circ}{2}$	$\overset{\circ}{4}$	$\overset{\circ}{3}$
3	$\overset{\circ}{1}$	$\overset{\circ}{3}$	$\overset{\circ}{4}$	$\overset{\circ}{2}$
4	$\overset{\circ}{1}$	$\overset{\circ}{4}$	$\overset{\circ}{1}$	$\overset{\circ}{4}$

- (c) Soit  $n$  tel que 5 divise  $n^n + 3$ : il est clair que  $n$  ne peut être divisible par 5, car sinon 5 diviserait  $n^n$  et  $n^n + 3$ , et donc 3, ce qui est faux. Ainsi, il existe  $a \in \{1, 2, 3, 4\}$  tel que  $n \equiv a \pmod{5}$ . Soit  $b \in \{0, 1, 2, 3\}$  tel que  $n \equiv a \pmod{4}$ . D'après la première question  $n^n \equiv a^b \pmod{5}$ : comme 5 divise  $n^n + 3$ , on a  $n^n \equiv 2 \pmod{5}$ , soit dans  $\mathbb{Z}/5\mathbb{Z}$ :  $\overset{\circ}{a}^b = \overset{\circ}{2}$ : d'après le tableau ci-dessus, on a donc  $(a, b) \in \{(2, 1), (3, 3)\}$ . Ce qui donne finalement

- soit  $n \equiv 2 \pmod{5}$  et  $n \equiv 1 \pmod{4}$
- soit  $n \equiv 3 \pmod{5}$  et  $n \equiv 3 \pmod{4}$

Réciproquement, on voit sans difficulté que si un des deux systèmes est vérifié, alors  $n^n \equiv 2 \pmod{5}$ , c'est à dire 5 divise  $n^n + 3$ .

- (d) Comme 5 et 4 sont premiers entre eux, le théorème chinois nous enseigne que chacun des deux systèmes peut se réduire à  $n \equiv u \pmod{20}$  pour un certain  $u$  à déterminer. Cherchons  $n$  qui s'écrive  $5u + 2$  et  $4v + 1$ : si  $n = 5u + 2 = 4v + 1$ , alors  $4v - 5u = 1$ . Il est clair que  $v = -1, u = -1$  forme une solution, ce qui correspond à la solution particulière  $n_0 = -3$ . Ainsi  $n \equiv 2 \pmod{5}$  et  $n \equiv 1 \pmod{4}$  est équivalent

---

à dire que  $n \equiv -3 \pmod{5}$  et  $n \equiv -3 \pmod{4}$ , autrement dit que  $n + 3$  est divisible par 5 et 4. Mais comme 5 et 4 sont premiers entre eux, c'est équivalent à dire que  $n + 3$  est divisible par 20. Soit  $n \equiv -3 \pmod{20}$  ou encore  $n \equiv 17 \pmod{20}$ . De la même manière,  $n \equiv 3 \pmod{5}$  et  $n \equiv 3 \pmod{4}$  est équivalent à  $n \equiv 3 \pmod{20}$ .

- (e) 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 39, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 91, 97
- (f) D'après ce qui précède les nombres entiers  $n$  tels que 5 divise  $n^n + 3$  sont de la forme  $20k + 3$  ou  $20k - 3$ : il y a donc entre 1 et 100: 17, 23, 37, 43, 57, 63, 77, 83, 97, parmi lesquels sont premiers: 17, 23, 37, 43, 83, 97.

**FIN**