



Unité L1MT03

Structures mathématiques

Corrigé de l'examen du 30 juin 2005

durée: 2h

1. Question de cours: voir cours.
2. Trouver tous les couples (a, b) tels que le nombre qui s'écrit 111 en base a s'écrit 11 en base b et tels que a et b ne dépassent pas 50 (cinquante). $\overline{111}^a = a^2 + a + 1$ et $\overline{11}^b = b + 1$, donc $\overline{111}^a = \overline{11}^b$ est équivalent à $a^2 + a + 1 = b + 1$, soit $b = a(a + 1)$. On a donc les solutions: $(2, 6), (3, 12), (4, 20), (5, 30), (6, 42)$. Il n'y en a pas d'autre car pour $a \geq 7$, $a(a + 1) \geq 56 > 50$.
3. Les nombres premiers strictement compris entre 1 et 11 sont 2, 3, 5, 7. Posons $N = 2 \cdot 3 \cdot 5 \cdot 7 = 210 < 400$. Tout entier i entre 1 et 11 a un diviseur premier p entre 1 et 11: ce nombre premier est 2, 3, 5 ou 7: il divise donc N , donc p divise i et N , qui ne sont donc pas premiers entre eux.
4. (a) i. Si $d(n) \equiv 1 \pmod{2}$, alors pour tout p premier tel que $\nu_p(n) > 0$, $1 + \nu_p(n)$ est impair. En effet, il suffirait qu'un des termes soit pair pour que le produit soit pair. Ainsi, pour tout p premier tel que $\nu_p(n) > 0$, $\nu_p(n)$ est pair: il existe donc n_p entier naturel avec $\nu_p(n) = 2n_p$. Posons $a = \prod_{p \in \mathcal{P}; \nu_p(n) > 0} p^{n_p}$: on a $a^2 = \prod_{p \in \mathcal{P}; \nu_p(n) > 0} p^{2n_p} = \prod_{p \in \mathcal{P}; \nu_p(n) > 0} p^{\nu_p(n)} = n$.
- ii. Réciproquement, si n peut s'écrire $n = a^2$. Alors comme

$$a = \prod_{p \in \mathcal{P}; \nu_p(a) > 0} p^{\nu_p(a)},$$

on a

$$n = a^2 = \prod_{p \in \mathcal{P}; \nu_p(a) > 0} p^{2\nu_p(a)},$$

Soit pour tout p $\nu_p(n) = 2\nu_p(a)$. Cela implique que $1 + \nu_p(n) \equiv 1 \pmod{2}$, d'où en faisant le produit $d(n) \equiv 1 \pmod{2}$.

(b) si n peut s'écrire $n = a^3$. Alors comme

$$a = \prod_{p \in \mathcal{P}; \nu_p(a) > 0} p^{\nu_p(a)},$$

on a

$$n = a^3 = \prod_{p \in \mathcal{P}; \nu_p(a) > 0} p^{3\nu_p(a)},$$

Soit pour tout p $\nu_p(n) = 3\nu_p(a)$. Cela implique que $1 + \nu_p(n) \equiv 1 \pmod{3}$, d'où en faisant le produit $d(n) \equiv 1 \pmod{3}$.

(c) Non, car $d(6) = d(2^1 \cdot 3^1) = (1+1)(1+1) = 4$ qui est bien congru à 1 modulo 3, mais 6 n'est pas un cube.

5. (a) Il suffit de montrer que dans $\mathbb{Z}/7\mathbb{Z}$, on a $\overset{\circ}{a}^b = \overset{\circ}{a}^{\overset{\circ}{b}'}$. Comme a et a' sont congrus modulo 7, 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 6, il existe un entier n tel que $b' - b = 6n$. Ainsi

$$\overset{\circ}{a}^{\overset{\circ}{b}'} = \overset{\circ}{a}^b \cdot \overset{\circ}{a}^{6n} = \overset{\circ}{a}^b \cdot (\overset{\circ}{a}^6)^n.$$

Si $\overset{\circ}{a} = 0$, alors $\overset{\circ}{a}^b = 0 = \overset{\circ}{a}^{\overset{\circ}{b}'}$. Sinon $a \in \{1, 2, 3, 4, 5, 6\}$ et donc a est premier avec 7: d'après le théorème d'Euler, on a donc dans $\mathbb{Z}/7\mathbb{Z}$: $\overset{\circ}{a}^6 = \overset{\circ}{a}^{\phi(7)} = \overset{\circ}{1}$, d'où

$$\overset{\circ}{a}^{\overset{\circ}{b}'} = \overset{\circ}{a}^b \cdot (\overset{\circ}{a}^6)^n = \overset{\circ}{a}^b \cdot \overset{\circ}{1}^n = \overset{\circ}{a}^b.$$

(b)

ab	0	1	2	3	4	5
1	$\overset{\circ}{1}$	$\overset{\circ}{1}$	$\overset{\circ}{1}$	$\overset{\circ}{1}$	$\overset{\circ}{1}$	$\overset{\circ}{1}$
2	$\overset{\circ}{1}$	$\overset{\circ}{2}$	$\overset{\circ}{4}$	$\overset{\circ}{1}$	$\overset{\circ}{2}$	$\overset{\circ}{4}$
3	$\overset{\circ}{1}$	$\overset{\circ}{3}$	$\overset{\circ}{2}$	$\overset{\circ}{6}$	$\overset{\circ}{4}$	$\overset{\circ}{5}$
4	$\overset{\circ}{1}$	$\overset{\circ}{4}$	$\overset{\circ}{2}$	$\overset{\circ}{1}$	$\overset{\circ}{4}$	$\overset{\circ}{2}$
5	$\overset{\circ}{1}$	$\overset{\circ}{5}$	$\overset{\circ}{4}$	$\overset{\circ}{6}$	$\overset{\circ}{2}$	$\overset{\circ}{3}$
6	$\overset{\circ}{1}$	$\overset{\circ}{6}$	$\overset{\circ}{1}$	$\overset{\circ}{6}$	$\overset{\circ}{1}$	$\overset{\circ}{6}$

(c) Soit n tel que 7 divise $n^n + 2$: il est clair que n ne peut être divisible par 7, car sinon 7 diviserait n^n et $n^n + 2$, et donc 2, ce qui est faux. Ainsi, il existe $a \in \{1, 2, 3, 4\}$ tel que $n \equiv a \pmod{7}$. Soit $b \in \{0, 1, 2, 3\}$ tel que $n \equiv a \pmod{6}$. D'après la première question $n^n \equiv a^b \pmod{7}$: comme 7 divise $n^n + 2$, on a $n^n \equiv 5 \pmod{7}$, soit dans $\mathbb{Z}/7\mathbb{Z}$: $\overset{\circ}{a}^b = \overset{\circ}{5}$: d'après le tableau ci-dessus, on a donc $(a, b) \in \{(3, 5), (5, 1)\}$. Ce qui donne finalement

- soit $n \equiv 3 \pmod{7}$ et $n \equiv 5 \pmod{6}$

-
- soit $n \equiv 5 [7]$ et $n \equiv 1 [6]$
- Réciproquement, on voit sans difficulté que si un des deux systèmes est vérifié, alors $n^n \equiv 5 [7]$, c'est à dire 7 divise $n^n + 2$.
- (d) Comme 7 et 6 sont premiers entre eux, le théorème chinois nous enseigne que chacun des deux systèmes peut se réduire à $n \equiv u [42]$ pour un certain u à déterminer.
- Cherchons n qui s'écrive $7u + 3$ et $6v + 5$: si $n = 7u + 3 = 6v + 5$, alors $7u - 6v = 2$. Il est clair que $v = 2, u = 2$ forme une solution, ce qui correspond à la solution particulière $n_0 = 17$. Ainsi $n \equiv 2 [7]$ et $n \equiv 1 [6]$ est équivalent à dire que $n \equiv 17 [7]$ et $n \equiv 17 [6]$, autrement dit que $n - 17$ est divisible par 7 et 6. Mais comme 7 et 6 sont premiers entre eux, c'est équivalent à dire que $n - 17$ est divisible par 42. Soit $n \equiv 17 [42]$.
 - Cherchons n qui s'écrive $7u + 5$ et $6v + 1$: si $n = 7u + 5 = 6v + 1$, alors $7u - 6v = -4$. Il est clair que $v = -4, u = -4$ forme une solution, ce qui correspond à la solution particulière $n_0 = -23$. On peut aussi considérer la solution $42 - 23 = 19$. Ainsi $n \equiv 5 [7]$ et $n \equiv 1 [6]$ est équivalent à dire que $n \equiv 19 [42]$.
- (e) D'après ce qui précède les nombres entiers n tels que 7 divise $n^n + 2$ sont de la forme $42k + 17$ ou $42k + 19$: il y a donc entre 1 et 100: 17, 19, 59, 61.

FIN