Corrigé du partiel de maths discrètes du 30/10/2007

Exercice 1.
a) 31 n'est pas divisible par 2 (ce n'est pas un nombre pair), ni par 3 (la somme de ses chiffres est 4, ce n'est pas divisible par 3), ni par 5 (31 ne se termine ni par 0 ni par 5). De plus, $7^2 = 49 > 31$, autrement dit $7 > \sqrt{31}$, donc 31 n'est divisible par aucun nombre premier $p \leq \sqrt{31}$. Or on sait qu'un entier n non premier premier est divisible par un nombre premier $p \leq \sqrt{n}$. Conclusion : 31 est un nombre premier.

b) Par a), 31 est un nombre premier, donc par le théorème de Fermat, $2^{30} \equiv 1$ (31) (2 n'est pas divisible par 31 puisque $0 < 2 < 31$). Division euclidienne de 94 par 30 : $94 = 3 \times 30 + 4$. Donc

$$2^{94} \equiv (2^{30})^3 \cdot 2^4 \equiv 1^3 \cdot 16 \equiv 16 \ (31).$$

Conclusion : comme $0 \leq 16 < 31$, 16 est le reste de la division euclidienne de 2^{94} par 31.

Exercice 2 Si a, b, c conviennent, a est divisible par $\text{pgcd}(a, b) = 10 = 2 \times 5$ et par $\text{pgcd}(a, c) = 15 = 3 \times 5$, donc a est divisible par $2 \times 3 \times 5$ en raison de la décomposition en nombres premiers (2, 3 et 5 sont premiers). De même, b est divisible par $\text{pgcd}(a, b) = 10 = 2 \times 5$ et par $\text{pgcd}(b, c) = 3$, donc b est divisible par $2 \times 3 \times 5$. Ceci implique que $\text{pgcd}(a, b) \geq 2 \times 3 \times 5$, ce qui est une contradiction. Conclusion : on ne peut pas trouver des entiers a, b, c vérifiant les conditions demandées.

Exercice 3.
a) Appliquons l'algorithme d'Euclide à 7 et 10 pour trouver leur pgcd et une relation de Bézout :
$10 = 1 \times 7 + 3$
$7 = 2 \times 3 + 1$
$3 = 3 \times 1 + 0$.
Donc $\text{pgcd}(7, 10) = 1$ et l'équation $7x - 10y = c$ a des solutions pour tout $c \in \mathbb{Z}$. De plus,

$$1 = 7 - 2 \times 3 = 7 - 2(10 - 7) = 3 \times 7 - 2 \times 10,$$

donc $3 \times 7 - 2 \times 10 = 1$ est une relation de Bézout entre 7 et 10.
On en déduit que $x_0 = 3c, y_0 = 2c$ est une solution particulière de $7x - 10y = c$, et un théorème du cours dit que l'ensemble des solutions de $7x - 10y = c$ est l'ensemble des couples d'entiers relatifs (x, y) avec $x = x_0 + 10k = 3c + 10k$ et $y = y_0 + 7k = 2c + 7k$, pour tout $k \in \mathbb{Z}$.

b) Soit x le nombre de tours de manège que fait Ariane et y le nombre de tours à poney que fait Sophie. Le temps que passe Ariane à faire du manège est égal à $7x$, le temps que passe Sophie à faire du poney est $10y$. On veut qu'elles finissent en même temps, et Sophie a commencé 4 minutes après, donc il faut que $7x = 4 + 10y$, autrement dit $7x - 10y = 4$. C'est la question a) avec $c = 4$.
L'ensemble des (x, y) solutions de $7x - 10y = 4$ est donné par $x = 12 + 10k$ et $y = 8 + 7k$. x, y sont des entiers naturels (ce sont des nombres de tours), donc il faut
$\begin{cases} 12 + 10k \geq 0 \iff k \geq -1 \ (k \text{ est un entier}) \\ 8 + 7k \geq 0 \iff k \geq -1 \end{cases}$
On cherche la plus petite solution parmi les couples d'entiers naturels. Vu la forme des solutions, il faut que k soit le plus petit possible, c'est-à-dire $k = -1$. La solution cherchée est $x = 12 - 10 = 2$ et $y = 8 - 7 = 1$. Conclusion : Ariane et Sophie finiront en même temps pour la première fois quand Ariane aura fait 2 tours de manège et Sophie 1 tour à poney.

Exercice 4. Appliquons l'algorithme d'Euclide à 5 et 12 :
$12 = 2 \times 5 + 2$
$5 = 2 \times 2 + 1$
$2 = 2 \times 1 + 0$
Donc 5 et 12 sont premiers entre eux. Par le théorème des restes chinois, le système

$$(S) \qquad \begin{cases} x \equiv 1 \ (5) \\ x \equiv 2 \ (12) \end{cases}$$

a des solutions et, si x_0 est une solution particulière, alors x est solution de (S) si et seulement si $x \equiv x_0$ (60) ($5 \times 12 = 60$).
On considère les systèmes élémentaires :

$$(S1) \quad \begin{cases} x \equiv 1 \ (5) \\ x \equiv 0 \ (12) \end{cases} \qquad (S2) \quad \begin{cases} x \equiv 0 \ (5) \\ x \equiv 1 \ (12) \end{cases}$$

L'algorithme d'Euclide ci-dessus donne la relation de Bézout suivante entre 5 et 12 : $1 = 5 \times 5 - 2 \times 12$. On en déduit que $y_1 = -2 \times 12 = -24$ est une solution de (S1) et $y_2 = 5 \times 5 = 25$ est une solution de (S2). Alors $x_0 = y_1 + 2y_2 = 26$ est une solution particulière de (S), et l'ensemble des entiers relatifs solutions de (S) est $\{x \in \mathbb{Z} \mid x \equiv 26 \ (60)\} = \{26 + 60k \mid k \in \mathbb{Z}\}$.

Remarque : on peut aussi résoudre (S) en cherchant $a, b \in \mathbb{Z}$ tels que $x = 1 + 5a = 2 + 12b$, autrement dit $5a - 12b = 1$.

Exercice 5. $3 \times 3 - 8 = 9 - 8 = 1$, donc, par le théorème de Bézout, 3 et 8 sont premiers entre eux, et $3 \times 3 - 8 = 1$ est une relation de Bézout entre 3 et 8. On a donc $3 \times 3 \equiv 1$ (8). Un théorème du cours sur les congruences dit que dans ce cas $3x \equiv 2$ (8) $\iff x \equiv 3 \times 2$ (8), autrement dit $x \equiv 6$ (8). Conclusion : l'ensemble des entiers relatifs x tels que $3x \equiv 2$ (8) est $\{x \in \mathbb{Z} \mid x \equiv 6 \ (8)\} = \{6 + 8k \mid k \in \mathbb{Z}\}$.

Exercice 6. a) Tout entier n est congru modulo 7 à un des entiers suivants : $0, 1, 2, 3, -1, -2, -3$.
Liste des carrés modulo 7 :

n (7)	n^2 (7)
0	0
$1, -1$	1
$2, -2$	4
$3, -3$	$9 \equiv 2$

Parmi les entiers $0, 1, \ldots, 6$, ceux qui sont congrus à un carré modulo 7 sont $0, 1, 2$ et 4.

b) Soit x, y des entiers tels que $x^2 + y^2 \equiv 0$ (7), autrement dit $y^2 \equiv -x^2$ (7). Par la question a), x^2 et y^2 sont congrus modulo 7 à un des entiers $0, 1, 2$ ou 4.
– Si $x^2 \equiv 0$ (7), alors $y^2 \equiv 0$ (7) ; vu le tableau de la question a), on a nécessairement $x \equiv y \equiv 0$ (7).
– Si $x^2 \equiv 1$ (7), alors $y^2 \equiv -1 \equiv 6$ (7) : impossible.
– Si $x^2 \equiv 2$ (7), alors $y^2 \equiv -2 \equiv 5$ (7) : impossible.
– Si $x^2 \equiv 4$ (7), alors $y^2 \equiv -4 \equiv 3$ (7) : impossible.
Réciproquement, si $x \equiv 0$ (7) et $y \equiv 0$ (7) alors $x^2 + y^2 \equiv 0$ (7). Conclusion : $x^2 + y^2 \equiv 0$ (7) si et seulement si $x \equiv 0$ (7) et $y \equiv 0$ (7).

c) Soit (a, b, c) des entiers tels que $a^2 + b^2 = 7c^2$. Modulo 7, cette égalité devient : $a^2 + b^2 \equiv 0$ (7). La question b) implique que $a \equiv 0$ (7) et $b \equiv 0$ (7), autrement dit a et b sont divisibles par 7.
Notons a', b' les entiers tels que $a = 7a'$ et $b = 7b'$. L'équation (E) devient : $7^2a'^2 + 7^2b'^2 = 7c^2$. On simplifie par 7 (qui est non nul) : $7(a'^2 + b'^2) = c^2$. On voit donc que c^2 est divisible par 7. On sait que si un nombre premier divise un produit d'entiers, il divise un des facteurs. Comme 7 est un nombre premier divisant $c^2 = c \times c$, on en déduit que 7 divise c.

d) On a supposé que $a^2 + b^2 = 7c^2$ et que $a = 7^r a'$, $b = 7^r b'$, $c = 7^r c'$. L'équation (E) devient : $7^{2r}a'^2 + 7^{2r}b'^2 = 7 \cdot 7^{2r}c'^2$. On simplifie par 7^{2r} (qui est non nul) : $a'^2 + b'^2 = 7c'^2$. Conclusion : (a', b', c') est aussi une solution de (E).

e) Supposons que (a, b, c) est une solution de (E) différente de $(0, 0, 0)$. On considère l'ensemble D des entiers naturels n tels que 7^n divise à la fois a, b et c. Cet ensemble est non vide car il contient 0 ($7^0 = 1$ divise a, b, c). De plus, au moins un des entiers a, b ou c est non nul ; si k est l'exposant de 7 dans cet entier, alors tout $n \in D$ vérifie $n \leq k$ (théorème de divisibilité lié à la décomposition en nombres premiers). L'ensemble D est donc borné et non vide ; comme c'est un ensemble d'entiers, il a un plus grand élément $r = \max D$.
Par définition de r, 7^r divise a, b et c. Notons a', b', c' les entiers tels que $a = 7^r a'$, $b = 7^r b'$, $c = 7^r c'$. Par la question d), (a', b', c') est aussi une solution de (E). Par la question c), 7 divise a', b' et c' ; notons a'', b'', c'' les entiers tels que $a' = 7a'', b' = 7b'', c' = 7c''$. Alors $a = 7r + 1a'', b = 7^{r+1}b'', c = 7^{r+2}c''$, donc 7^{r+1} divise a, b et c, et donc $r + 1 \in D$. Ceci contredit le fait que r est l'élément maximal de D.
Conclusion : il n'existe pas de solution de (E) différente de $(0, 0, 0)$. Comme $(0, 0, 0)$ est clairement une solution, on en déduit que c'est l'unique solution entière de (E).