UNIVERSITE DE RENNES 1

Algèbre et Arithmétique 1

Corrections de l'Examen du 16 Décembre 2008

Exercice 2

1) Pour tout entier relatif n on a n^2 est un entier positif. Il suit donc que l'assertion (a) est vraie, puisque il suffit de prendre $a = 0$.

L'assertion (b) est fausse car on prenant $(a, b, c) = (4, 2, 2) \in \mathbb{Z}^3$ on voit que a divise bc et que a ne divise ni b ni c.

2) La négation de (a) :

$$\forall a \in \mathbb{Z}, \exists n \in \mathbb{Z}, n^2 < a.$$

La négation de (b) :

$$\exists (a, b, c) \in \mathbb{Z}^3, (a|bc \text{ et } a \not| b \text{ et } a \not| c).$$

Exercice 3

1) Soit A, B deux parties finies d'un même ensemble. La formule d'inclusion-exclusion est

$$Card(A \cup B) = Card(A) + Card(B) - Card(A \cap B).$$

2) Dans l'échantillon de 100 foyers, il y a 15 foyers n'ayant pas de téléviseur et 25 n'ayant pas d'ordinateur. Donc, le cardinal de l'ensemble des foyers n'ayant pas de téléviseur ou n'ayant pas d'ordinateur ne peut excéder $15 + 25 = 40$. D'où, le nombre de foyers équipés d'un téléviseur et d'un ordinateur est au minimum 60.

3) De même, le nombre de foyers n'ayant pas de plante ou pas de téléviseur ou pas d'ordinateur ne peut excéder $5 + 15 + 25 = 45$. Donc, le nombre de foyers ayant un téléviseur, un ordinateur et une plante est au minimum 55.

Exercice 4

1) On a les divisions euclidiennes suivantes :

$$138 = 5 \times 27 + 3 \quad 27 = 5 \times 5 + 2$$

Donc, on a $138 = 5 \times (5 \times 5 + 2) + 3 = 5^3 + 2 \times 5 + 3 = \overline{1023}^{(5)}$.

2) On a $\overline{2342}^{(5)} = 2 + 4 \times 5 + 3 \times 5^2 + 2 \times 5^3 = 347$.

3) En faisant directement le calcul en base de 6, on obtient le résultat $\overline{431}^{(6)} \times \overline{35}^{(6)} = \overline{25205}^{(6)}$. Pendant ce calcul on effectue les opérations suivantes :

$$5 \times 3 = 15 = 6 \times 2 + 3 \quad 5 \times 4 = 20 = 6 \times 3 + 2 \quad 3 \times 3 = 9 = 6 \times 1 + 3 \quad 3 \times 4 = 12 = 6 \times 2 + 0.$$

4) Le reste de la division de $\overline{23510325}^{(6)}$:

- par 6 est 5 puisque $\overline{23510325}^{(6)} = 6 \times \overline{2351032}^{(6)} + 5$.
- par 3 est 2 puisque $\overline{23510325}^{(6)} = 3 \times 2 \times \overline{2351032}^{(6)} + 3 + 2$.
- par 54 est 17 puisque $\overline{23510325}^{(6)} = 6^3 \times \overline{2351}^{(6)} + 3 \times 6^2 + 2 \times 6 + 5$ et $54 = 6 \times 3 \times 3$.

Exercice 5

1_

On utilise l'algorithme d'Euclide étendu :

$$\begin{array}{ll} & 5715 = 5715\times 1 + 3915\times 0 \\ & 3915 = 5715\times 0 + 3915\times 1 \\ 5715 = 3915\times 1 + 1800 & 1800 = 5715\times 1 + 3915\times(-1) \\ 3915 = 1800\times 2 + 315 & 315 = 5715\times(-2) + 3915\times 3 \\ 1800 = 315\times 5 + 225 & 225 = 5715\times 11 + 3915\times(-16) \\ 315 = 225\times 1 + 90 & 90 = 5715\times(-13) + 3915\times 19 \\ 225 = 90\times 2 + 45 & 45 = 5715\times 37 + 3915\times(-54) \\ 90 = 45\times 2 + 0 & \end{array}$$

Le pgcd de 5715 et 3915 est donc 45, et l'on a $45 = 5715\times 37 + 3915\times(-54)$.

2_

En utilisant l'algorithme d'Euclide, on trouve :

$$\begin{aligned} \mathrm{pgcd}(4878565, 4878564) &= \mathrm{pgcd}(4878564, 1) & (4878565 = 4878564\times 1 + 1) \\ &= \mathrm{pgcd}(1, 0) & (4878564 = 4878564\times 1 + 1) \\ &= 1 \end{aligned}$$

donc les entiers 4878564 et 4878565 sont premiers entre eux.

3_

Posons $d = \mathrm{pgcd}(n, m)$. Comme d divise n et m, il existe des entiers n' et m' tels que $n = dn'$ et $m = dm'$.

Comme $nu + mv = d$, on a alors $n'u + m'v = 1$,

donc tout diviseur commun de u et v est un diviseur de 1,

donc u et v sont premiers entre eux.

Exercice 6

1_

D'après le petit théorème de Fermat, comme $31 \nmid (-5)$ et 31 est premier,

on a $(-5)^{30} \equiv 1 \pmod{31}$: l'entier $k = 30$ convient.

2_

Le plus petit $k_0 \in \mathbb{N}^*$ tel que $(-5)^{k_0} \equiv 1 \pmod{31}$ s'appelle l'ordre multiplicatif de -5 modulo 31.

Comme $(-5)^{30} \equiv 1 \pmod{31}$, c'est un diviseur de 30.

On a : $(-5)^2 \equiv 25 \equiv -6 \not\equiv 1 \pmod{31}$, donc $k_0 \nmid 2$

$(-5)^3 \equiv (-5)\times(-6) \equiv 30 \equiv -1 \not\equiv 1 \pmod{31}$, donc $k_0 \nmid 3$

$(-5)^6 \equiv (-1)^2 \equiv 1 \pmod{31}$, donc $k_0 \mid 6$,

donc k_0 est un diviseur de 6 autre que 1, 2 ou 3, donc $k_0 = 6$.

3_

On a : $57^{1529} \equiv (-5)^{1529} \pmod{31}$ car $57 \equiv -5 \pmod{31}$

$\equiv (-5)^5 \pmod{31}$ car $(-5)^6 \equiv 1 \pmod{31}$ et $1529 \equiv 5 \pmod 6$

4_

On a donc : $57^{1529} \equiv (-5)^5 \pmod{31}$ par 3.

$\equiv (-6)\times(-1) \pmod{31}$ car $\begin{cases}(-5)^2 \equiv -6 \pmod{31} \\ (-5)^3 \equiv -1 \pmod{31}\end{cases}$ (cf. réponse au 2_)

donc $57^{1529} \equiv 6 \pmod{31}$

Exercice 7

1.

On a $3 \times (-5) \equiv 1 \pmod{16}$, donc -5 est un inverse de 3 modulo 16,

donc $3x \equiv 7 \pmod{16} \iff x \equiv (-5) \times 7 \pmod{16}$

$\iff x \equiv -3 \pmod{16}$,

donc les solutions de la congruence $3x \equiv 7 \pmod{16}$ sont les entiers congrus à -3 modulo 16.

2.

Comme $\mathrm{pgcd}(5, 11) = 1$, d'après le théorème chinois le système de congruences

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{11} \end{cases}$$

équivaut à une congruence $x \equiv x_0 \pmod{55}$ (où $x_0 \in \mathbb{Z}$ est une solution particulière du système).

On a une relation de Bezout : $5 \times (-2) + 11 \times 1 = 1$,

alors $x_0 = 5 \times (-2) \times 4 + 11 \times 1 \times 2 = -18$ est une solution particulière du système.

Donc les solutions du système sont les entiers congrus à -18 modulo 55.

3.

On a $(-7) \times 7 + 2 \times 25 = 1$, donc -7 est un inverse de 7 modulo 25,

donc $7x \equiv 2 \pmod{25} \iff x \equiv (-7) \times 2 \pmod{25}$

$\iff x \equiv 11 \pmod{25}$.

D'autre part, on a : $18x \equiv 6 \pmod{24} \iff 3x \equiv 1 \pmod{4}$ (par division par 6)

$\iff x \equiv -1 \pmod{4}$,

donc $\begin{cases} 7x \equiv 2 \pmod{25} \\ 18x \equiv 6 \pmod{24} \end{cases} \iff \begin{cases} x \equiv 11 \pmod{25} \\ x \equiv -1 \pmod{4} \end{cases}$.

Comme $\mathrm{pgcd}(25, 4) = 1$, le théorème chinois s'applique directement, et donne l'équivalence de ce système avec une congruence modulo 100. Il reste à déterminer une solution particulière.

On a une relation de Bezout : $25 \times 1 + 4 \times (-6) = 1$,

donc $25 \times 1 \times (-1) + 4 \times (-6) \times 11 = -25 + 264 = 239 \equiv 39 \pmod{100}$ est une solution particulière du système,

donc $\begin{cases} x \equiv 11 \pmod{25} \\ x \equiv -1 \pmod{4} \end{cases} \iff x \equiv 39 \pmod{100}$.

Donc les solutions du système de congruences $\begin{cases} 7x \equiv 2 \pmod{25} \\ 18x \equiv 6 \pmod{24} \end{cases}$ sont les entiers congrus à 39 modulo 100.