CC2 2010. Corrigé

Questions 1 (Arithmétique) : 11 pts

(1) 2 pts

On sait par le cours que si $n = p_1^{a_1} \cdots p_l^{a_l}$ est la décomposition primaire de l'entier $n \in \mathrm{N}$ alors

$$Div_+(n) = \{p_1^{r_1} \cdots p_l^{r_l},\ \forall i \in [1,l], 0 \leq r_i \leq a_i\}$$

et il y a $(a_1+1)\cdots(a_l+1)$ diviseurs positifs.

Ici, $100 = 10 \cdot 10 = 2^2 \cdot 5^2$. D'où $n = 100^{100} = 2^{200} \cdot 5^{200}$. Dès lors n admet $201 \cdot 201 = 40401$ diviseurs positifs.

(2) 1 pt + 1 pt + 2 pts

Reste de 101^{101} par 3:

$101 = 3 \cdot 33 + 2$ i.e. $101 \equiv 2[3]$ d'où $101^{101} \equiv 2^{101}[3]$. Ensuite, $2^2 \equiv 1[3]$ donne $2^{101} = 2^{2\cdot 50+1} = (2^2)^{50} \cdot 2 \equiv 2[3]$.

Reste par 5:

$101 = 5 \cdot 20 + 1$ i.e. $101 \equiv 1[5]$ d'où $101^{101} \equiv 1[5]$.

Reste par 15:

L'entier $N = 101^{101}$ est solution du système de congruences:

$$X \equiv 2[3], \quad X \equiv 1[5]$$

dont les solutions sont

$$X = N + (3 \cdot 5)l = N + 15l, \quad l \in \mathrm{Z}.$$

Pour trouver le reste de N par 15 il suffit de trouver une solution de ce système. Par inspection, on peut observer que $X = 11$ convient et son reste par 15 vaut 11.

Si on ne voit pas cette solution, on cherche $u, v \in \mathrm{Z}$ tels que $X = 2 + 3u = 1 + 5v$ i.e. tels que

$$5v - 3u = 1.$$

Une solution est $u = -2$ et $v = -1$. Dès lors $X = 2 - 6 = -4$ convient et le reste de -4 par 15 vaut 11. C'est aussi le reste de N par 15.

(3) 3 pts

Notons N le nombre d'inscrits. Par hypothèse il existe $a, b, c \in \mathrm{N}$ tels que

$$N = 9 + 18a = 9 + 20b = 9 + 24c$$

C'est un système de 3 congruences modulo des entiers non 2 à 2 premiers. Les deux premières donnent $9a = 10b$; par Gauss, 10 divise a i.e. $a = 10u$. La condition $18a = 24c$ i.e. $3a = 4c$ devient $30u = 4c$ i.e. $15u = 2c$; par Gauss 2 divise u i.e. $u = 2v$. Conclusion $N = 9 + 18a = 9 + (18 \cdot 10 \cdot 2)v = 9 + 360v$, $v \in \mathrm{N}$. La condition $500 \leq N \leq 1000$ donne alors $N = 729$.

(4) 1 pt (pour Fermat) + 1 pt (pour si p divise ab alors p divise a ou b).

L'assertion est vraie: par Fermat, $a^{p-1} \equiv 1[p]$ i.e. p divise $(a^{p-1}-1) = (a^{\frac{p-1}{2}}-1)\cdot(a^{\frac{p-1}{2}}+1)$ dès lors p (étant premier) divise l'un des facteurs de ce produit.

Questions 2 (Applications) : 9 pts + bonus 3 pts

(1) 1.5 pt + 1.5 pt (injectif ou pas /surjectif ou pas)

Une manière de répondre est d'observer que $u^{-1} \circ v^{-1} \circ u^{-1}$ est la réciproque de $u \circ v \circ u$.

Une autre réponse est d'étudier séparément l'injectivité et la surjectivité:

C'est injectif: En utilisant successivement l'injectivité de u et de v on a

$$u(v(u(x))) = u(v(u(x'))) \Rightarrow v(u(x)) = v(u(x')) \Rightarrow u(x) = u(x') \Rightarrow x = x'.$$

C'est surjectif: en utilisant successivement la surjectivité de u et de v, $z \in \mathrm{Z}$ s'écrit $z = u(z')$, $z' \in \mathrm{N}$. z' s'écrit $z' = v(z'')$, $z'' \in \mathrm{Z}$. z'' s'écrit $z'' = u(x)$, $x \in \mathrm{N}$. Voici en un coup d'oeil:

$$\begin{array}{c} \mathrm{N} \to \mathrm{Z} \to \mathrm{N} \to \mathrm{Z} \\ x \mapsto z'' \mapsto z' \mapsto z \end{array}$$

Conclusion:

$$\forall z \in \mathrm{Z},\ \exists x \in \mathrm{N},\ z = u(v(u(x)).$$

(2) 1.5 pt + 1.5 pt

C'est injectif par unicité de la factorisation en premiers:

$$2^a 3^b 5^c = 2^{a'} 3^{b'} 5^{c'} \Rightarrow a = a', b = b', c = c'$$

Ce n'est pas surjectif car, par exemple, 7 n'a pas d'antécédent.

(3) 1.5 pt + 1.5 pt

Ce n'est pas surjectif car quel que soit $l \in \mathrm{Z}, \varphi(l) < n$ donc n n'a pas d'antécédent. Ce n'est pas injectif car pour un reste r, $\varphi(r) = \varphi(n+r)$.

$\star$ Question bonus $\star$

(4) 3 pts

On a

$$f^{-1}(u,v) = (U,V) \Leftrightarrow (u,v) = f(U,V) = (aU+bV+1, cU+dV-1).$$

Il faut donc résoudre le système

$$(1)\, aU+bV+1 = u, \quad (2)\, cU+dV-1 = v$$

pour U, V.

$d \times (1) - b \times (2)$ donne $adU + dbV + d - bcU - bdV + b = du - bv$ i.e. $(ad-bc)U + (b+d) = du - bv$ i.e. $U = du - bv - (b+d)$

$a \times (2) - c \times (1)$ donne $acU + adV - a - caU - cbV - c = av - cu$ i.e. $(ad-bc)V - (a+c) = av - cu$ i.e. $V = av - cu + (a+c)$.