Université Paris 7-Denis Diderot — MT-282

D.E.U.G.- S.M. — Année 1998-99

EXAMEN PARTIEL du 12 décembre 1998

Durée : 3 h

Exercice 1

Pour $x \in \mathbf{Q}$, on note $[x]$ la partie entière de x, c'est-à-dire le plus grand entier $\leq x$.

1. Soient p un nombre premier et q un nombre rationnel non nul. Démontrer qu'il existe un unique $e \in \mathbf{Z}$ tel que $q = \frac{u}{v}p^e$ avec u et v entiers premiers à p. On pose alors $v_p(q) = e$.

2. Démontrer que $A_p = \{p^n / n \in \mathbf{Z}\}$ muni de la multiplication est un groupe.

3. Démontrer que v_p est un homomorphisme de groupes entre $\mathbf{Q}^*$ muni de la multiplication et $\mathbf{Z}$ muni de l'addition. En déduire un isomorphisme de groupes $A_p \to \mathbf{Z}$. Établir l'inégalité, pour $(x, y) \in \mathbf{Q}^{*2}$,

$$v_p(x+y) \geq \min(v_p(x), v_p(y)).$$

4. Démontrer qu'un nombre rationnel x non nul est entier si et seulement si on a $v_p(x) \geq 0$ pour tout nombre premier p.

5. Soit n un entier > 0. Considérons l'écriture $[a_k a_{k-1} ... a_0]_p$ de n en base p. Démontrer qu'on a, pour tout i tel que $0 \leq i \leq k$

$$[n/p^i] = a_k p^{k-i} + a_{k-1} p^{k-i-1} + ... + a_i.$$

6. Démontrer qu'on a

$$v_p(n\,!) = [n/p] + [n/p^2] + ... + [n/p^k].$$

Posons $s_p(n) = a_0 + a_1 + ... + a_k$. En déduire l'identité

$$v_p(n\,!) = \frac{n - s_p(n)}{p-1}.$$

7. Soient n et m deux entiers >0. Établir la formule

$$v_p(C_{n+m}^n) = \frac{s_p(n) + s_p(m) - s_p(n+m)}{p-1}.$$

(On rappelle que le coefficient binomial est donné par la formule $C_{n+m}^n = \frac{(m+n)\,!}{m\,!n\,!}$.) En déduire que tout coefficient binomial est entier.
8. Calculer $v_2(C_{22}^7)$.

Exercice 2

Soit p un nombre premier impair. On rappelle que $(\mathbf{Z}/p^2\mathbf{Z})^*$ est un groupe cyclique.
1. Démontrer que tout nombre entier x est congru modulo p à un unique entier de valeur absolue $< p/2$. Démontrer ensuite que tout entier x est congru modulo p^2 à un unique entier de la forme $ap+b$ avec a et b entiers de valeurs absolues $< p/2$. Dans ce qui suit lorsqu'on demande de calculer x modulo p^2, cela signifie déterminer a et b.

Désormais on suppose qu'on a $p = 1093$ (qui est un nombre premier). On s'efforcera de conserver la notation littérale p dans les calculs.

2. Décomposer $p-1 = 1092$ en produit de facteurs premiers. À quoi est égal 2^{1092} modulo p ?
3. Vérifier que les calculs de 3^7 et 2^{14} donnent respectivement $2p+1$ et $15p-11$ modulo p^2. En déduire le calcul de $3^2 2^{28}$ puis de $3^2 2^{26}$ modulo p^2 (on pourra utiliser que $-2970p+1089$ est congru à $-1876p-4$ modulo p^2). À l'aide de la remarque $182 = 26\times 7$ et de la formule du binôme en déduire le calcul de $3^{14}2^{182}$ modulo p^2. Comparer ce résultat au calcul de 3^{14} modulo p^2.
4. Calculer à l'aide de ce qui précède 2^{182} modulo p^2. En déduire le calcul de 2^{1092} modulo p^2.
5. L'équation $x^p = 2$ a-t-elle des solutions dans $(\mathbf{Z}/p^2\mathbf{Z})^*$?
6. S'il existe une solution de l'équation $x^p = 2$ dans $(\mathbf{Z}/p^2\mathbf{Z})^*$, retrouver directement le calcul de 2^{1092} modulo p^2 ?