Université de Paris 7 **2009-2010**
31UBMT42

Arithmétique IV

Exercice I:

1) a) Quels sont les ordres possibles d'un élément modulo 23? (au sens multiplicatif)

b) En déduire les ordres de 2, 3, 5 modulo 23 (en effectuant le moins de calculs possibles.)

2) a) Calculer $\left(\frac{38}{495}\right)$; 38 est il un carré modulo 495?

b) Calculer $\left(\frac{57}{495}\right)$; 57 est il un carré modulo 495?

c) Calculer $\left(\frac{-149}{495}\right)$; -149 est il un carré modulo 495?

d) Calculer $\left(\frac{-164}{495}\right)$; -164 est il un carré modulo tout diviseur premier de 495? Est il un carré modulo 495?

Exercice II:

1) a) Soit $N = 5(n!)^2 - 1$. Montrer qu'il existe un diviseur premier de N congru à -1 modulo 5.

b) En déduire qu'il existe une infinité de nombres premiers congrus à -1 modulo 5.

c) Montrer qu'il existe une infinité de nombres premiers dont l'écriture en base 10 se termine par 9

2) En considérant $2(n!)^2 - 1$, montrer qu'il existe une infinité de nombres premiers congrus à -1 modulo 8

Exercice III:

Déterminer les nombres premiers p tels que $X^2 + 15$ ait une racine dans $\mathbb{F}_p$

Exercice IV:

1) Montrer que si p est un nombre premier divisant $3^{\frac{p-1}{2}} + 1$, alors $p \equiv 5$ [12] ou $p \equiv 7$ [12]

2) On pose $F_n = 2^{2^n} + 1$

a) Montrer que si F_n est premier, alors F_n divise $3^{\frac{F_n-1}{2}} + 1$.

b) Montrer que si F_n divise $3^{\frac{F_n-1}{2}} + 1$, alors F_n est premier.

Exercice V:

Soit n un entier supérieur ou égal à 2. On pose $q = 3^n - 2$

1) Calculer $\left(\frac{2}{q}\right)$.

2) Calculer $\left(\frac{3}{q}\right)$.

Exercice VI:

1) Donner le nombre de classes pour $SL_2(\mathbb{Z})$ et pour $GL_2(\mathbb{Z})$ de formes quadratiques de discriminant -11

2) Trouver les p premiers tels que $p = x^2 + 3xy + 5y^2$ ait une solution entière.

Exercice VII:

1) Montrer qu'il existe une forme quadratique de discriminant -20 représentant 47.

2) Quel est le nombre de classes $h(-20)$?

3) Soit $\alpha \in \mathbb{Z}$, l'équation $47 = x^2 + 2\alpha xy + (\alpha^2 + 5)y^2$ a t'elle une solution dans $\mathbb{Z}$?

4) a) Montrer que s'il existe un entier n représenté par toute forme de discriminant -20, alors n est nul modulo 5.

b) Existe il $n \neq 0$ tel que n soit représenté par toute forme quadratique de discriminant -20?

Exercice VIII:

Donner une forme réduite de $10x^2 + 31xy + 25y^2$

Exercice IX:

1) a) Combien y a t il de $SL_2(\mathbb{Z})$-classes de formes quadratiques de discriminant -39? Donner un représentant de chaque classe.

b) Combien y a t il de $GL_2(\mathbb{Z})$-classes de formes quadratiques de discriminant -39?

2) a) Dans quelle classe est la forme $q(x,y) = 4x^2 + 11xy + 10y^2$?

b) On note $q_0(x,y) = ax^2 + bxy + cy^2$ le représentant de q tel que $0 \leq b \leq a \leq c$, et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ et $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Exprimer $q(x,y)$ en fonction de q_0, S et T.

3) On considère un nombre premier p de la forme $4.(12)^n + 11$ où $n \in \mathbb{N}^*$

a) Calculer $\left(\frac{13}{p}\right)$

b) Montrer qu'il existe une forme quadratique de discriminant -39 représentant p.

c) En vous aidant de $\left(\frac{p}{3}\right)$, montrer qu'il existe une unique $GL_2(\mathbb{Z})$-classe (que l'on explicitera) représentant p

Exercice X:

1) Montrer qu'il existe une forme quadratique de discriminant -204 représentant 167

2) On dispose du tableau suivant:

i	2	4	6	8	10	12	14	16	18	20	22
$51^i[167]$	96	31	137	126	72	65	61	11	54	7	4

a) En donner une explicitement (non nécessairement réduite)

b) En donner une réduite: q_0

c) Donner $(x,y) \in \mathbb{Z}^2$ tels que $q_0(x,y) = 167$

Exercice XI:

On considère une forme quadratique q sur $\mathbb{Z}^3$ telle que sa matrice dans la base canonique de $\mathbb{Z}^3$ soit à coefficients entiers et de déterminant 1. On suppose q définie positive.

1) On note $b_{1,1}$ le minimum de q sur $\mathbb{Z}^3 - \{0\}$, et u_1, u_2, u_3 des entiers tels que $q(u_1,u_2,u_3) = b_{1,1}$.

a) Montrer que u_1, u_2, u_3 sont premiers entre eux dans leur ensemble.

b) En déduire qu'il existe un élément de $SL_3(\mathbb{Z})$ dont la première colonne soit (u_1,u_2,u_3)

c) En déduire qu'il existe des entiers $b_{i,j}$, tels que $b_{i,j} = b_{j,i}$, et que q soit $SL_3(\mathbb{Z})$ équivalente à $\sum_{1\leq i,j\leq 3} b_{i,j}x_i.x_j$ (où $b_{1,1}$ est toujours l'entier défini précédemment).

2) On considère une matrice $Q \in SL_3(\mathbb{Z})$ de la forme $\begin{pmatrix} 1 & r & t \\ 0 & & \\ 0 & & P \end{pmatrix}$. On note $X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, et l'on pose $X' = Q.X$

a) Montrer que l'on peut choisir r,t tels que la matrice $A = {}^tQ.B.Q$ vérifie:

$$a_{1,1} = b_{1,1}, |2a_{1,2}| \leq a_{1,1}, |2a_{1,3}| \leq a_{1,1}.$$

b) Montrer qu'il existe $A' \in \mathcal{M}_2(\mathbb{Z})$ symétrique telle que:

$${}^tX.a_{1,1}A.X = (a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3)^2 + (x_2,x_3).A'.\begin{pmatrix} x_2 \\ x_3 \end{pmatrix}$$

c) Montrer que $b_{1,1}x'_1 + b_{1,2}x'_2 + b_{1,3}x'_3 = a_{1,1}x_1 + a_{1,2}x_2 + a_{1,3}x_3$.

d) Montrer que l'on peut choisir P pour que $|2a'_{1,2}| \leq a'_{1,1} \leq a'_{2,2}$

e) Calculer $a'_{1,1}$ et $\det(A')$.

f) En déduire que $a_{1,1} = 1$

g) En déduire que q est $SL_3(\mathbb{Z})$ équivalente à $x_1^2 + x_2^2 + x_3^2$.

Exercice XII:

Soit $n \in \mathbb{N}, n \geq 2$. On suppose qu'il existe $d \in \mathbb{N}^*$ tel que $-d$ soit un carré modulo $dn-1$

1) a) On pose $a_{2,2} = dn - 1$. Trouver des entiers $a_{1,1}$ et $a_{1,2}$ tels que $a_{1,1} \geq 1$ et que la matrice $A = \begin{pmatrix} a_{1,1} & a_{1,2} & 1 \\ a_{1,2} & a_{2,2} & 0 \\ 1 & 0 & n \end{pmatrix}$ ait pour déterminant 1.

b) Montrer que si $\det\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{1,2} & a_{2,2} \end{pmatrix} \geq 1$, la forme quadratique associée à A est définie positive.

2) Conclure que n est somme de 3 carrés.