RICM 2 – 2007-08 – CALCULS MODULO UN ENTIER – D. Duval

TD 1 — Addition et multiplication modulo N

1. Trouver trois nombres distincts congrus à 7 modulo 5, dont un négatif.

2. Trouver toutes les solutions de la congruence $x \equiv 7 \pmod{11}$.

3. Appliquer l'algorithme de division euclidienne aux entiers 213 et 43, en écrivant les valeurs successives de q et r. Même question avec -213 et 43.

4. En faisant le moins de calculs possible, trouver le représentant canonique de la classe de 213 modulo 43, puis le représentant canonique de la classe de -213 modulo 43, puis celui de $2 \times 213^2 - 20$.

5. Pour tout $a \in \mathbb{N}$, on note $s(a)$ la somme des chiffres de a quand on l'écrit en base 10.
Calculer $s(987654321)$, puis $s(s(987654321))$, etc.
Montrer que tout entier $a \in \mathbb{N}$ est congru à $s(a)$ modulo 9.
Application : quel est le reste de la division euclidienne de 987654321 par 9 ?

6. Soit n un entier se terminant par 99, et k un entier naturel. Montrer que n^k se termine par 01 si k est pair, et par 99 si k est impair.

7. Trouver un nombre a tel que, dans $\mathbb{Z}/7\mathbb{Z}$, les classes de 1, a, a^2, ..., a^5 sont toutes distinctes. Montrer que $\overline{a}^n = \overline{1}$ si et seulement si n est divisible par 6. Quelles sont les solutions de l'équation $X^3 = \overline{1}$ dans $\mathbb{Z}/7\mathbb{Z}$?

RICM 2 – 2007-08 – CALCULS MODULO UN ENTIER – D. Duval

TD 2 — Division modulo N

1. En utilisant la table de multiplication dans $\mathbb{Z}/5\mathbb{Z}$, déterminer tous les éléments inversibles de $\mathbb{Z}/5\mathbb{Z}$ et leurs inverses. En déduire l'ensemble $(\mathbb{Z}/5\mathbb{Z})^*$.

2. En utilisant la table de multiplication dans $\mathbb{Z}/6\mathbb{Z}$, déterminer tous les éléments inversibles de $\mathbb{Z}/6\mathbb{Z}$ et leurs inverses. En déduire l'ensemble $(\mathbb{Z}/6\mathbb{Z})^*$.

3. Déterminer tous les éléments inversibles de $\mathbb{Z}/15\mathbb{Z}$ et leurs inverses. En déduire l'ensemble $(\mathbb{Z}/15\mathbb{Z})^*$.

4. Appliquer l'algorithme d'Euclide pour calculer le pgcd de 390 et 216.

5. Une machine emballe des pièces de monnaie dans des sacs. Toutes les pièces sont identiques, et tous les sacs aussi. Quand on lui donne 7912 pièces, la machine ne peut pas remplir le dernier sac, il ne contient que 37 pièces. Quand on lui donne 59167 pièces, la machine ne peut pas remplir le dernier sac, il ne contient que 42 pièces. Combien chaque sac plein contient-il de pièces ?

6. Trouver au moins deux couples (u, v) tels que $12\,u + 30\,v = pgcd(12, 30)$.

7. Appliquer l'algorithme d'Euclide étendu pour calculer une identité de Bézout entre 390 et 216.

8. Trouver le représentant canonique de l'inverse de la classe $\overline{213}$ dans $\mathbb{Z}/43\mathbb{Z}$, s'il existe.
Quels sont les $c \in \mathbb{Z}/43\,\mathbb{Z}$ tels que $\overline{213}\,c = \overline{15}$ dans $\mathbb{Z}/43\mathbb{Z}$?
Résoudre la congruence $213\,X \equiv 15 \pmod{43}$.

RICM 2 – 2007-08 – CALCULS MODULO UN ENTIER – D. Duval

TD 3 — Exponentiation modulo N

1. Calculer $2^6 - 1$, puis le diviser par 7. Quel est le reste ? Peut-on obtenir le même résultat sans faire de calcul ?

2. Calculer à la main $2^{44497} \pmod 3$.

3. Calculer à la main $2^{44497} \pmod{11}$.

4. Calculer à la main $(15^3 + (13 \times 36)^2 - 79)^{254}$ modulo 13.

5. Dans $\mathbb{Z}/7\mathbb{Z}$, calculer l'inverse de $\overline{3}$ en utilisant le théorème de Fermat.

6. Calculer $\varphi(m)$ pour m de 2 à 25, et dessiner la partie correspondante du graphe de la fonction φ.

7. Calculer à la main $2^{44497} \pmod 9$.

8. En utilisant le crible d'Erathostène, tester si le nombre 91 est un nombre premier, et sinon le décomposer en facteurs premiers. Puis répondre aux mêmes questions pour le nombre 97.

9.

a. Calculer 3^{11} modulo 23 de la façon suivante : calculer (toujours modulo 23) $3^2 = 3 \times 3$, puis $3^3 = 3^2 \times 3$, et ainsi de suite jusqu'à $3^{11} = 3^{10} \times 3$.

b. Remarquer que le nombre 11 s'écrit 1011 en binaire, cela revient à écrire $11 = 1 + 2 + 8$. Donc $3^{11} = 3^1 \times 3^2 \times 3^8$. En utilisant $3^4 = (3^2)^2$ et $3^8 = (3^4)^2$, calculer 3^{11} modulo 23, sans utiliser la question précédente.

c. Calculer 3^{473} modulo 23 en utilisant le résultat des questions précédentes.

RICM 2 – 2007-08 – CALCULS MODULO UN ENTIER – D. Duval

TD 4 — Le théorème chinois des restes

1. Soit $N = 15 = 3 \times 5$.
Construire la table de la fonction du théorème chinois :

$$F_{15,3,5} \ : \ \mathbb{Z}/15\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \ : \ \overline{a}^{(15)} \mapsto (\overline{a}^{(3)}, \overline{a}^{(5)}) \ .$$

Déterminer u et v tels que $3u + 5v = 1$, puis construire la table de l'autre fonction du théorème chinois :

$$G_{15,3,5} \ : \ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/15\mathbb{Z} \ : \ (\overline{b}^{(3)}, \overline{c}^{(5)}) \mapsto \overline{3uc + 5vb}^{(15)} \ .$$

Vérifier que $F_{15,3,5}$ et $G_{15,3,5}$ sont bien des fonctions réciproques l'une de l'autre.

2. Calculer 257 modulo 3 et modulo 5. En déduire la valeur de 257 modulo 15.

3. Calculer 83 modulo 3 et modulo 5. En déduire la valeur de 83 modulo 15.

4. Soit $a = (15^3 + (13 \times 36)^2 - 79)^{254}$. Rappeler la valeur de a modulo 7 et modulo 11. En déduire la valeur de a modulo 77.

5. Une boîte contient 160 allumettes. Après en avoir utilisées quelques-unes, on range les allumettes par paquets de 11, et on constate qu'il en reste 3. Puis on les range par paquets de 13, et on constate qu'il en reste 5. Combien reste-t-il d'allumettes dans le paquet ?

6.
Construire la table de l'élévation au carré dans $\mathbb{Z}/3\mathbb{Z}$, et en déduire toutes les solutions de l'équation $X^2 = 1$ dans $\mathbb{Z}/3\mathbb{Z}$.
Construire la table de l'élévation au carré dans $\mathbb{Z}/5\mathbb{Z}$, et en déduire toutes les solutions de l'équation $X^2 = 1$ dans $\mathbb{Z}/5\mathbb{Z}$.
Déterminer toutes les solutions de l'équation $X^2 = 1$ dans $\mathbb{Z}/15\mathbb{Z}$.