UNIVERSITÉ DE RENNES 1

UFR DE MATHÉMATIQUES

Licence – portail MIPE

NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES, PERMUTATIONS (*A2*)

Examen du 4 janvier 2006 (2 heures)

Documents, notes de cours ou de TD, téléphones portables, calculatrices sont interdits.
Justifiez toutes vos réponses

EXERCICE 1

1 Trouver les entiers relatifs x tels que $22x \equiv 143 \pmod{253}$.
2 Combien y a-t-il de solutions entre -40 et 130 ?

EXERCICE 2

1 Montrez par récurrence sur n que pour tout entier p tel que $0 \leqslant p < n$, on a

$$C_n^{p+1} = C_p^p + C_{p+1}^p + \cdots + C_{n-1}^p.$$

2 Montrer que pour tout entier $n \geqslant 0$, on a

$$C_n^0 + C_n^1 + \cdots + C_n^n = 2^n.$$

3 Donner une interprétation combinatoire de la formule précédente.

EXERCICE 3

1 Soit a un entier qui n'est pas un multiple de 59. Montrer que les valeurs possibles de l'ordre multiplicatif de a modulo 59 sont 1, 2, 29 ou 58.
2 Quel est l'ordre multiplicatif de 61 modulo 59.
3 Quel est l'ordre multiplicatif de 4 modulo 59 ?
4 Quel est l'ordre multiplicatif de -4 modulo 59 ?

Tournez la page S.V.P.

EXERCICE 4

1 Écrire 103 en base 2.

2 Décomposer 143 en facteurs premiers.

3 Calculer le pgcd d de 103 et 120 et déterminer des entiers u et v tels que $120u + 103v = d$.

4 Soit a et n des entiers relatifs. À quelle condition existe-t-il un entier x tel que $ax \equiv 1 \pmod{n}$?

5 Déterminer tous les entiers x compris entre 0 et 119 tels que $103x \equiv 1 \pmod{120}$.

6 Rappeler l'énoncé du « petit théorème de Fermat ».

7 Trouver $a \in \{0, 1, \ldots, 12\}$ tel que $27^{103} \equiv a \pmod{13}$.

8 Trouver $b \in \{0, 1, \ldots, 10\}$ tel que $27^{103} \equiv b \pmod{11}$.

9 Calculer le reste de la division euclidienne de 27^{103} par 143.

10 Juliette et Roméo ont lu dans la revue *Pour la Science* un article sur le principe de cryptographie RSA. Ils décident de le tester sur un exemple simple pour vérifier qu'ils ont compris. Pour cela, Juliette choisit la clef publique $(n = 143, c = 7)$; Roméo choisit alors un entier, compris entre 0 et 142, puis le code avant de transmettre à Juliette le résultat : 27.
Pouvez-vous aider Juliette à retrouver l'entier choisi par Roméo ? Justifiez soigneusement votre réponse ; en particulier, rappelez le principe du codage et du décodage et calculez la clef secrète qui permet le décodage.
Vous pourrez bien sûr utiliser les questions précédentes.

Licence – portail MIPE

NOMBRES ENTIERS ET RATIONNELS,
CONGRUENCES, PERMUTATIONS (*A2*)
Corrigé de l'examen du 4 janvier 2006 (2 heures)
Sujet proposé (et corrigé) par A. Chambert-Loir

SOLUTION DE L'EXERCICE 1.

1 On commence par remarquer que 22, 143 et 253 sont tous divisibles par 11. L'équation $22x \equiv 143 \pmod{253}$ équivaut alors à $2x \equiv 13 \pmod{23}$. Alors, 2 et 23 sont premiers entre eux, et la relation $2 \times 12 = 24 \equiv 1 \pmod{23}$ montre que 12 est un inverse de 2 modulo 23. Par suite, l'équation $2x \equiv 13 \pmod{23}$ équivaut à l'équation $x \equiv 12 \times 13 \equiv 156 \pmod{23}$, d'où $x \equiv 18 \pmod{23}$, puisque $156 = 23 \times 6 + 18$.
Les entiers relatifs x tels que $22x \equiv 143 \pmod{253}$ sont donc les entiers x tels que $x \equiv 18 \pmod{23}$, c'est-à-dire ceux de la forme $18 + 23n$ avec $n \in \mathbf{Z}$.

2 Cherchons les entiers $n \in \mathbf{Z}$ tels que $18 + 23n$ appartienne à l'intervalle $[-40; 130]$. Cela s'écrit $-40 \leqslant 18 + 23n \leqslant 130$, soit $-58 \leqslant 23n \leqslant 112$. Puisque $-3 \times 23 < -58 < -2 \times 23$ et $4 \times 23 < 112 < 5 \times 23$, on obtient l'inégalité $-2 \leqslant n \leqslant 4$. Les entiers cherchés sont donc les entiers -28, -5, 18, 41, 64, 97, 120.

SOLUTION DE L'EXERCICE 2.

1 Pour $n = 0$, il n'y a rien à démontrer car il n'y a pas d'entier p tel que $0 \leqslant p < 0$. Pour $n = 1$, le seul entier p tel que $0 \leqslant p < 1$ est $p = 0$ et il faut démontrer que $C_1^1 = C_0^0$, assertion vraie car les deux membres valent 1.
Supposons donc que l'on ait

$$C_n^{p+1} = C_p^p + C_{p+1}^p + \cdots + C_{n-1}^p$$

pour tout entier p tel que $0 \leqslant p < n$ et montrons que pour tout entier p tel que $0 \leqslant p < n+1$, on a

$$C_{n+1}^{p+1} = C_p^p + C_{p+1}^p + \cdots + C_n^p.$$

Pour cela, on utilise la relation du triangle de Pascal :

$$C_{n+1}^{p+1} = C_n^p + C_n^{p+1},$$

valable pour tout couple (n, p) d'entiers naturels (avec la convention $C_n^p = 0$ si $p > n$). Alors, pour tout entier p tel que $0 \leqslant p < n$,

$$\begin{aligned} C_{n+1}^{p+1} &= C_n^p + C_n^{p+1} \\ &= C_n^p + \left(C_p^p + C_{p+1}^p + \cdots + C_{n-1}^p\right) && \text{par l'hypothèse de récurrence} \\ &= C_p^p + C_{p+1}^p + \cdots + C_n^p. \end{aligned}$$

Si $p = n$, on a aussi $C_{n+1}^{p+1} = 1 = C_n^n$. Cela démontre l'assertion au rang $n + 1$.
Par récurrence, elle est donc vraie pour tout entier n.

2 Appliquons la formule du binôme, pour $n \geqslant 0$ et $x \in \mathbf{R}$,

$$(1+x)^n = \sum_{p=0}^{n} \mathrm{C}_n^p x^p$$

à l'entier $x = 1$. On trouve

$$2^n = \sum_{p=0}^{n} \mathrm{C}_n^p,$$

comme il fallait démontrer.

3 Si $n \geqslant 0$, 2^n est le nombre de parties d'un ensemble E_n à n éléments. Pour $0 \leqslant p \leqslant n$, C_n^p est le nombre de parties de E_n possédant exactement p éléments. La formule traduit donc le fait que le cardinal d'une partie de E_n est un entier compris entre 0 et n.

SOLUTION DE L'EXERCICE 3.

1 Comme 2 n'est pas multiple de 59, on a $2^{58} \equiv 1 \pmod{59}$ et les entiers n tels que $2^n \equiv 1 \pmod{59}$ sont des diviseurs de 58. On a $58 = 2 \times 29$ et 29 est premier. Les diviseurs de 58 sont donc 1, 2, 29 et 58. L'ordre multiplicatif de 2 modulo 59 est donc l'un de ces entiers.

2 On a $2^1 \equiv 2 \not\equiv 1 \pmod{59}$. De même, $2^2 \equiv 4 \not\equiv 1 \pmod{59}$. Donc $d \neq 1$ et $d \neq 2$. Calculons $2^2 9 \pmod{59}$. On a $2^6 = 64 \equiv 5 \pmod{59}$, donc $2^{12} \equiv 25 \pmod{59}$ et $2^{24} \equiv 625 = 590 + 35 \equiv 35 \pmod{59}$. Ensuite,

$$2^{29} = 2^5 \times 2^{24} \equiv 2^4 \times 70 \equiv 2^4 \times 11 \equiv 2 \times 88 \equiv 2 \times 29 \equiv 58 \pmod{59}.$$

On a donc $2^{29} \not\equiv 1 \pmod{59}$ et $d \neq 29$.
La seule valeur possible qui reste est $d = 58$.

SOLUTION DE L'EXERCICE 4.

1 Divisons successivement par 2 : $143 = 2 \times 71 + 1$, $71 = 2 \times 35 + 1$, $35 = 2 \times 17 + 1$, $17 = 2 \times 8 + 1$, $8 = 2^3$, d'où, remettant les restes dans l'autre sens, $143 = \overline{10001111}^{(2)}$.

2 On a $143 = 11 \times 13$. En outre, 11 et 13 sont premiers car ils ne sont divisibles ni par 2, ni par 3, ni par 5 et $5^2 = 25 > 13$.

3 Appliquons l'algorithme d'Euclide étendu à 103 et 120. On écrit donc

120	1	0	
103	0	1	$q = 1$
17	1	-1	$q = 6$
1	-6	7	$q = 17$
0			

si bien que 103 et 120 sont premiers entre eux, et que $-6 \times 120 + 7 \times 103 = 1$. (Vérification : le premier terme vaut 720, le second 721.) On a donc $d = 1$ et on peut donc prendre $u = -6$ et $v = 7$.

4 Il existe $x \in \mathbf{Z}$ tel que $ax \equiv 1 \pmod{n}$, c'est-à-dire a est inversible modulo n, si et seulement si a et n sont premiers entre eux.

5 103 et 120 sont premiers entre eux et 7 est un inverse de 103 modulo 120 (puisque $7 \times 103 \equiv 1 \pmod{120}$). En multipliant par 7 la relation $103x \equiv 1 \pmod{120}$, on obtient une relation équivalente, soit $x \equiv 7 \pmod{120}$. Le seul entier compris entre 0 et 119 qui vérifie cette congruence est $x = 7$.

6 Le petit théorème de Fermat affirme que si n est un entier relatif et p un nombre premier, $n^p \equiv n \pmod{p}$; si de plus n n'est pas multiple de p, $n^{p-1} \equiv 1 \pmod{p}$.

7 On a $27 \equiv 1 \pmod{13}$, donc $27^{103} \equiv 1^{103} \equiv 1 \pmod{13}$. On a ainsi $a = 1$.

8 On a $27 \equiv 5 \pmod{11}$ et $5^10 \equiv 1 \pmod{11}$. Par suite,

$$5^{103} \equiv 5^3 \times (5^{10})^{10} \equiv 25 \times 5 \equiv 3 \times 5 \equiv 15 \equiv 4 \pmod{11}.$$

Donc $b = 4$.

9 Soit r le reste de la division euclidienne de 27^{103} par 143. Il vérifie $0 \leqslant r \leqslant 142$ et $27^{103} \equiv r \pmod{143}$. En particulier, $r \equiv 1 \pmod{13}$ et $r \equiv 4 \pmod{11}$, car $143 = 11 \times 13$. On écrit alors $r = 1 + 13k$, avec $0 \leqslant k \leqslant 10$ (décomposition en base mixte $(11, 13)$). D'où $1 + 13k \equiv 4 \pmod{11}$, soit $2k \equiv 3 \pmod{11}$. Multipliant cette relation par 6, on obtient $12k \equiv k \equiv 18 \equiv 7 \pmod{11}$. Par suite, $k = 7$ et $r = 1 + 13 \times 7 = 92$. Le reste de la division euclidienne de 27^{103} par 143 est donc égal à 92.

10 Soit s l'entier choisi par Roméo ; on le suppose premier à $n = 143$. Par définition de l'algorithme RSA, l'entier crypté transmis à Juliette est le reste t de la division euclidienne de $s^c = s^7$ par n. Pour décoder le message, Juliette doit calculer le reste de la division euclidienne de t^d modulo 143, où la « clef de décodage » d est un entier tel que $cd \equiv 1 \pmod{\varphi(143)}$. Comme $143 = 11 \times 13$, $\varphi(143) = 10 \times 12 = 120$; on a donc $cd \equiv 1 \pmod{1)20}$. En effet, on a alors $t^d \equiv (s^c)^d \equiv s^{cd} \equiv s \pmod{143}$ car $s^{\varphi(n)} \equiv 1 \pmod{n}$ pour s et n premiers entre eux. Autrement dit, s est bien égal au reste de la division euclidienne de t^d par 143.

Comme $7 \times 103 \equiv 1 \pmod{120}$, on peut prendre $d = 103$. Ainsi, s est le reste de la division euclidienne de 27^{103} par 143, soit $s = 92$ en vertu des questions précédentes.