UNIVERSITÉ DE RENNES 1

UFR DE MATHÉMATIQUES

Licence STS — mention mathématiques *Année 2007/2008*

A2. NOMBRES ENTIERS ET RATIONNELS, CONGRUENCES. PERMUTATIONS

Feuille de travaux dirigés n° 6 : *Congruences - Partie 2*

EXERCICE 1

Pour chaque valeur de l'entier n, $2 \leqslant n \leqslant 20$, calculer $\varphi(n)$ en dénombrant les entiers de $\{1,\dots,n\}$ qui sont premiers avec n.

EXERCICE 2

1 Calculer $\varphi(n)$ si n est une puissance d'un nombre premier p.

2 En utilisant le théorème chinois, démontrer que $\varphi(mn) = \varphi(m)\varphi(n)$ si m et n sont des entiers premiers entre eux.

3 En déduire $\varphi(n)$ en fonction de la décomposition en facteurs premiers de n.

EXERCICE 3

Soit n un entier qui est le produit de deux nombres premiers distincts. Montrer que pour tout $x \in \mathbf{Z}$, on a $x^{\varphi(n)+1} \equiv x \pmod{n}$.

EXERCICE 4

Montrer que si n est un entier impair alors $\varphi(2n) = \varphi(n)$ et si n est un entier pair alors $\varphi(2n) = 2\varphi(n)$.

EXERCICE 5

Trouver l'ordre multiplicatif de 2 modulo n et vérifier qu'il divise $\varphi(n)$ pour

- $n = 63$
- $n = 105$

EXERCICE 6

Trouver les trois derniers chiffres de 7^{9999}.

EXERCICE 7

Déterminer le chiffre des unités et celui des dizaines de 123456^{789}.

EXERCICE 8

1) Calculer la valeur $\varphi(91)$ de l'indicatrice d'Euler.
2) Quels sont les valeurs possibles de l'ordre multiplicatif modulo 91 d'un entier ?
3) A l'aide du théorème d'Euler, déterminer un entier n tel que $17^n = 1\,[91]$.
4) Déterminer l'ordre multiplicatif de 17 modulo 7, modulo 13 et modulo 91.
5) Déterminer l'ordre multiplicatif de 4 puis de 16 modulo 7, modulo 13 et modulo 91.

EXERCICE 9

(extrait du contrôle du 24/11/2004)

Juliette et Roméo ont lu dans la revue Pour la Science un article sur le principe de cryptographie RSA. Ils décident de tester sur un exemple simple pour vérifier qu'ils ont compris. Pour cela Juliette choisit la clef publique ($n = 143$, $e = 7$). Roméo choisit alors un entier compris entre 0 et 142 puis le chiffre 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 chiffrement et du déchiffrement et calculez la clef secrète qui permet le déchiffrement.

EXERCICE 10

On précise que $5 \times 317 = 1 + 4 \times 396$ et que $15^4 = 115 \times 437 + 370$. Alice veut transmettre un message codé à Bertrand. Bertrand choisit deux nombres premiers 19 et 23 et obtient une clé publique $(e = 317, n = 437)$ qu'il envoie à Alice.

1) Alice veut transmettre le message M. Comment fait-elle pour chiffrer le message ?

2) Bertrand recoit le message chiffré 15. Retrouver l'information transmise par Alice ?

EXERCICE 11

7 est-il un carré modulo 13 ?

EXERCICE 12

Trouver les racines modulo 7 de

- $2x^2 - 3x - 2$
- $x^3 + x^2 + 4x + 1$
- $x^3 + 4x^2 + 3x + 6$

EXERCICE 13

Trouver les racines modulo 8 de $x^2 + x + 4$.

EXERCICE 14

Ecrire le développement décimal de 22/7.

Calculer l'ordre multiplicatif de 10 modulo 7.

Ecrire sous forme de fraction irréductible le nombre rationnel dont le développement décimal est $3,14\overline{159}$.

EXERCICE 15

(extrait de l'examen de janvier 2007) Dans tout l'exercice n désignera l'entier 187.

a) Factoriser n et calculer $\varphi(n)$.

b) Quel est l'inverse de 7 modulo 160 ?

c) Montrer que l'ordre multiplicatif modulo n de 21 est égal à 4.

d) Lucas souhaite transmettre un message m à Antoine en utilisant le cryptosystème RSA. Il chiffre le message m en un message $M = 21$ puis envoie M à Antoine. Sachant que la clé publique d'Antoine est $(n, e) = (187, 7)$, retrouver le message initial m.

EXERCICE 16

(extrait de l'examen de janvier 2007)

a) Calculer $\varphi(100)$.

b) En déduire 53^{799} modulo 100.

c) En déduire les deux derniers chiffres de 999953^{799}.

EXERCICE 17

Soit n un entier $\geqslant 2$; si $0 \leqslant k \leqslant n-1$, on note $c_k = \exp(2ik\pi/n)$.

1 Montrer que $\{c_0, \ldots, c_n\}$ est l'ensemble des racines complexes du polynôme $X^n - 1$.

2 Soit $c \in \mathbf{C}^*$; on suppose que $c^n = 1$. Soit d le plus petit entier > 0 tel que $c^d = 1$. (On dit que c est d'ordre d.) Montrer que n est multiple de d.

3 On suppose que n est le plus petit entier > 0 tel que $c^n = 1$. Montrer qu'il existe un unique entier $k \in \{0, \ldots, n\}$ tel que $\text{pgcd}(k, n) = 1$ et tel que que $c = c_k$. Combien y a-t-il de tels nombres complexes c ?

4 Plus généralement, si d divise n, combien y a-t-il d'éléments $c \in \mathbf{C}^*$ qui sont d'ordre d ?

5 Montrer que $\sum_{d|n} \varphi(d) = n$, où la somme est prise sur l'ensemble des diviseurs > 0 de n.