UNIVERSITÉ DE RENNES 1

Algèbre et Arithmétique 1

Feuille n°5 : Congruences, indicatrice d'Euler, RSA

1 Exercices à savoir faire

Exercice 1

1 Trouver tous les couples $(x, y) \in \mathbf{Z}^2$ tels que $3x + 7y = 5$.
2 Résoudre dans $\mathbf{Z}$ l'équation $3x \equiv 5 \pmod 7$.

Exercice 2

1 L'entier 6 a t-il un inverse modulo 77 ? Si oui, en déterminer un.
2 Résoudre l'équation $6x \equiv 5 \pmod{77}$.

Exercice 3

1 Utiliser l'algorithme d'Euclide pour déterminer un inverse de 56 modulo 75.
2 Utiliser le petit théorème de Fermat pour déterminer un inverse de 10 modulo 13.
3 Déterminer un inverse de 75 modulo 13.

Exercice 4

Résoudre dans $\mathbf{Z}$ les systèmes de congruence suivants.

$$(1)\begin{cases} x \equiv 3 \pmod{12} \\ x \equiv 3 \pmod{21} \end{cases} \qquad (2)\begin{cases} x \equiv 5 \pmod{15} \\ x \equiv 4 \pmod{14} \end{cases}$$

$$(3)\begin{cases} 2x \equiv 1 \pmod{25} \\ x \equiv 5 \pmod{13} \end{cases} \qquad (4)\begin{cases} x \equiv 1 \pmod{10} \\ x \equiv 5 \pmod{15} \end{cases}$$

$$(5)\begin{cases} x \equiv 17 \pmod{21} \\ x \equiv 2 \pmod{6} \end{cases} \qquad (6)\begin{cases} 9x \equiv 2 \pmod{15} \\ x \equiv 6 \pmod{17} \end{cases}$$

Exercice 5

Résoudre dans $\mathbf{Z}$ le système $\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$

Exercice 6

Résoudre dans $\mathbf{Z}$ le système $\begin{cases} x & \equiv & 3 \pmod{12} \\ x & \equiv & 4 \pmod{17} \\ x & \equiv & 5 \pmod{25} \end{cases}$

Exercice 7

Quel est le plus petit entier plus grand que 10 000 qui divisé par 5, 12 et 17 ait pour reste 3 ?

Exercice 8

Trouver tous les entiers compris entre 100 et 1000 qui divisés par 21 aient pour reste 8 et par 17 pour reste 5.

Exercice 9

Donner (sans consulter le cours) la définition de l'indicateur d'Euler $\phi(n)$ d'un entier $n \in \mathbf{N} \setminus \{0\}$. Que vaut $\phi(p)$, si p est un nombre premier ?

Exercice 10

Énoncer (sans consulter le cours) le théorème d'Euler.

Exercice 11

1 Soient $n \in \mathbf{N}$ avec $n \geq 2$ et $a, b \in \mathbf{Z}$. Donner (sans consulter le cours) la définition de « b est un inverse de a modulo n ».
2 Montrer (sans consulter le cours) que si a et n sont deux entiers premiers entre eux alors a est inversible modulo n.

Exercice 12

1 À quelle condition nécessaire et suffisante sur a et n l'entier a est-il inversible modulo l'entier n ? (Répondre sans consulter le cours).
2 Montrer que si a' et a'' sont deux inverses de a modulo n alors $a' \equiv a'' \pmod{n}$.

Exercice 13

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

Exercice 14

Montrer en utilisant la définition de ϕ que si n est un entier impair alors $\phi(2n) = \phi(n)$ et si n est un entier pair alors $\phi(2n) = 2\phi(n)$.

Exercice 15

1 Calculer $\phi(n)$ si n est une puissance d'un nombre premier p.
2 En utilisant le théorème chinois, démontrer que $\phi(mn) = \phi(m)\phi(n)$ si m et n sont des entiers premiers entre eux.
3 En déduire $\phi(n)$ en fonction de la décomposition en facteurs premiers de n.

Exercice 16

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

Exercice 17

Juliette et Roméo ont lu dans la revue *Pour la Science* un article sur le système de chiffrement 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 18

On précise que $5 \times 317 = 1 + 4 \times 396$ et que $154 = 115 \times 437 + 370$. 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 19

1 Calculer $\phi(100)$.
2 En déduire 53^{799} modulo 100.
3 En déduire les deux derniers chiffres de 999953^{799}.

Exercice 20

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

Exercice 21

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

2 Exercices à chercher

Exercice 22

Le code ISBN a été inventé dans les années 60 pour faciliter le travail de catalogage des livres dans les bibliothèques. Il se compose de 10 chiffres décimaux séparés par des espaces ou des tirets, dont le dernier peut aussi être le symbole X représentant la valeur 10. Le premier représente la langue (0 pour l'anglais, 2 pour le français, 3 pour l'allemand...), le bloc suivant l'éditeur (Springer-Verlag en Allemagne : 540, aux États-Unis : 387, Cassini : 84225, Dargaux : 205, etc.), le suivant le numéro du livre chez l'éditeur — il reste d'autant peu de place que l'éditeur a un gros numéro — et le dernier est un code permettant de s'assurer (au moins partiellement) de l'intégrité du code. Si les 10 chiffres sont $a_1, \ldots, a_{10}$, la condition qu'ils doivent vérifier s'écrit

$$\sum_{i=1}^{10} i a_i \equiv 0 \pmod{11}.$$

1 Vérifier que 2-205-00694-0 (*Astérix en Corse*) et 0-387-54894-7 (*Introduction to Coding Theory* de J. H. van Lint) sont des codes ISBN valides.
2 Vérifier que 2-84225-007-1 n'est pas un ISBN valide. Peut-on le corriger ?
3 Montrer que l'on peut détecter un chiffre inexact, ou l'interversion de deux chiffres dans un ISBN (en supposant qu'il n'y ait qu'une seule erreur de ce type).

Exercice 23

Le code de sécurité sociale est formé de 13 chiffres décimaux suivi d'une clef de deux chiffres. Si N est l'entier de 13 chiffres et c la clef, la contrainte de vérification est la relation

$$N + c \equiv 0 \pmod{97}.$$

1 Quelle est la clef d'un individu dont le numéro de sécurité sociale serait 1-71-04-78-646-378 ?
2 Un numéro de sécurité sociale est 2-xx-07-35-231-584, clé 19, mais les caractères xx sont illisibles. Pouvez-vous retrouver l'année de naissance de la personne en question ? (Solution : 1943)
3 Montrer que la clef de contrôle détecte une erreur sur un chiffre, ainsi que l'interversion de deux chiffres consécutifs.
4 Montrer que 97 est un nombre premier et que $n = 96$ est le plus petit entier strictement positif tel que $10^n \equiv 1 \pmod{97}$.

5 Montrer plus généralement que la clef de contrôle détecte l'interversion de deux chiffres quelconques.

Exercice 24

1 Montrer que pour tout entier n, $n(n^4-1)$ est divisible par 15.
2 Montrer que pour tout entier n, $n^2(n^4-1)$ est divisible par 60. Peut-on faire mieux ?
3 Montrer que pour tout entier n, $n(n^6-1)$ est divisible par 42. Peut-on faire mieux ?

Exercice 25

Une vieille fermière s'en allant marché voit ses œufs écrasés par un cheval. Le cavalier voulant la rembourser lui demande combien d'œufs elle avait. Tout ce dont elle se souvient est qu'en les rangeant par 2, il en restait un, et de même en les rangeant par 3, 4, 5 ou 6 ; toutefois, en les rangeant par 7, il n'en restait pas. Combien d'œufs, au moins, avait-elle ? (D'après Lauritzen, repris de Ore)

Exercice 26

Sur une île déserte, cinq hommes et un singe ramassent des noix de coco. La nuit tombée, il s'endorment. Le premier homme se réveille et prend sa part du butin : il divise le tas de noix en cinq parts égales et donne au singe la noix de coco restante, prend sa part et va se recoucher. Le second se réveille, prend un cinquième du tas restant et donne au singe une noix qui restait à part. Et ainsi de suite des cinq hommes. Combien de noix de coco, au moins, avaient été ramassées ? (D'après Lauritzen)

Exercice 27

« Une dame ayant rencontré des pauvres, a eu la pensée charitable de leur donner ce qu'elle avait. Pour donner à chacun 9 sous, il lui en manquait 32 ; alors elle leur a donné 7 sous, et il lui en est resté 24. Combien avait-elle et quel est le nombre des pauvres ? » (J. Vinot, *Récréations mathématiques*, années 30).

Exercice 28

L'armée de César comptait plus de 1000 hommes, mais moins de 3000. Lorsqu'il voulut la dénombrer par groupes de 11, il n'en resta pas ; par groupes de 9, il en resta 5 ; par groupes de 13, il en resta 8. Combient y avait-il de soldats dans cette armée ? (D'après J. Vinot)

Exercice 29

Dix-sept pirates s'emparent d'un lot de pièces d'or toutes identiques. Leur loi exige

un partage à égalité : chacun doit recevoir le même nombre de pièces d'or et, s'il y a un reste, celui-ci est attribué au cuisinier de bord. Dans le cas présent, la part du cuisinier serait de trois pièces, mais les pirates se querellent et six d'entre eux sont tués, ce qui porte la part du cuisinier à quatre pièces. Au cours d'une terrible tempête, le bateau fait naufrage et ne survivent que six pirates et le cuisinier. Par bonheur, le butin est sauvé. La part du cuisinier est maintenant de cinq pièces. Que peut espérer gagner le cuisinier lorsqu'il décide d'empoisonner le reste de l'équipage, sachant que c'est la plus petite des solutions possibles ?

Exercice 30

7 est-il un carré modulo 13 ?

Exercice 31

Résoudre l'équation suivante : $3x^2 + 13x + 14 \equiv 0 \pmod{31}$.

Exercice 32

1 Écrire le développement décimal de $22/7$.
2 Calculer l'ordre multiplicatif de 10 modulo 7.
3 Ecrire sous forme de fraction irréductible le nombre rationnel dont le développement décimal est $3,14159$.

3 Exercices pour aller plus loin

Exercice 33

Sachant que le 1er janvier 1901 était un mardi, combien de vendredi 13 y a-t-il eu au XXe siècle ? Dans le calendrier grégorien, calculer les fréquences des lundi 13, mardi 13, etc.

Exercice 34

Soit ϕ l'application de $\{0, \ldots, 9\}$ dans lui-même définie par $\phi(x) = 2x$ si $x \leq 4$ et $\phi(x) = 1 + 2(x - 5)$ si $x \geq 5$. Un numéro de carte bancaire est un nombre décimal de la forme $a_n a_{n-1} \ldots a_1 a_0$, où les chiffres décimaux satisfont à la règle (dite de Luhn) :

$$a_0 + \phi(a_1) + a_2 + \phi(a_3) + \cdots \equiv 0 \pmod{10}.$$

1 Montrer que cela permet de détecter la présence d'un chiffre décimal erroné.
2 Montrer que cela permet de détecter une permutation de deux chiffres consécutifs, à l'exception de la permutation $09 \to 90$.

Avant l'introduction de l'Euro, les billets de banque allemands utilisaient paraît-il un code obtenu par l'adjonction d'un chiffre décimal à un nombre décimal de 9 chiffres qui détectait une erreur ou l'interversion de deux chiffres consécutifs.

Exercice 35

Trouver les racines modulo 7 de

1 $2x^2 - 3x - 2$

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

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

Exercice 36

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

Exercice 37

1 Calculer la valeur $\phi(91)$ 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 $17^n \equiv 1\,[91]$.

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 38

Soit n un entier supérieur ou égal à 2 et soit a un entier premier avec n.

1 Donner la définition de l'ordre multiplicatif de a modulo n.

2 Quel est l'ordre multiplicatif de 3 modulo 22 ?

Exercice 39

1 Calculer l'ordre multiplicatif de 3 modulo 13.

2 Calculer 133^{1961} modulo 13.

Exercice 40

1 Calculer l'ordre multiplicatif de 5 modulo 31.

2 Calculer 67^{1973} modulo 31.

Exercice 41

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

1 $n = 63$

2 $n = 105$

Exercice 42

Dans tout l'exercice n désignera l'entier 187.

1 Factoriser n et calculer $\phi(n)$.

2 Quel est l'inverse de 7 modulo 160 ?

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

4 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 43

Soit n un entier supérieur à 2 ; si $0 \leq k \leq n-1$, 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 strictement positif tel que $c^d = 1$ (on dit que d est l'ordre de c). Montrer que n est multiple de d .

3 On suppose que n est le plus petit entier strictement positif tel que $c^n = 1$. Montrer qu'il existe un unique entier $k \in \{0, \ldots, n\}$ tel que $pgcd(k, n) = 1$ et tel que que $c = c^k$. Combien y a-t-il de tels nombres complexes c ? Plus généralement, si d divise n, combien y a-t-il d'éléments $c \in \mathbf{C}^*$ dont l'ordre est d ?

4 Montrer la relation $\sum_{d|n} \phi(d) = n$, où la somme est prise sur l'ensemble des diviseurs positifs de n.