Université de Rennes

ARIC - Arithmétique pour la Cybersécurité

Feuille n°1 : Congruences, indicatrice d'Euler, RSA

1. Sur les groupes

Exercice 1

La réunion de deux sous-groupes d'un groupe G est-elle un sous-groupe de G ? Et l'intersection ?

Exercice 2

Voici la table d'un groupe fini :

$*$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

Déterminer l'ordre de a.

Exercice 3

1 Soit H un sous-groupe de $(\mathbf{Z}, +)$ contenant $\{2, 7\}$. Montrer que 1 est dans H.
2 Montrer que 1 est dans le sous-groupe de $(\mathbf{Z}, +)$ engendré par $\{2, 7\}$.
3 Quel est le sous-groupe engendré par $\{2, 7\}$?

Exercice 4

Soit $< a, b >$ le sous-groupe de $(\mathbf{Z}, +)$ engendré par a et b, deux entiers non tous nuls.
1 Montrer que $a\mathbf{Z}$ est inclus dans $< a, b >$.
2 Montrer que $a\mathbf{Z} + b\mathbf{Z}$ est inclus dans $< a, b >$.
3 Montrer que $a\mathbf{Z} + b\mathbf{Z}$ est un sous-groupe de $(\mathbf{Z}, +)$ contenant $\{a, b\}$.
4 Montrer que $< a, b >= a\mathbf{Z} + b\mathbf{Z}$.
5 Montrer que $< a, b >= a\mathbf{Z} + b\mathbf{Z} = pgcd(a, b)\mathbf{Z}$.

Exercice 5

1 Déterminer $45\mathbf{Z} \cap 60\mathbf{Z}$.
2 Déterminer $56\mathbf{Z} + 63\mathbf{Z}$.
3 Trouver les sous-groupes de $\mathbf{Z}$ contenant $48\mathbf{Z}$ et donner les relations d'inclusion existant entre eux.

2. Congruences

Exercice 6

1 Pour tout x entier, calculer le reste de la division euclidienne de $3x$ par 7, suivant le reste de la division euclidienne de x par 7.
2 Résoudre dans $\mathbf{Z}$ l'équation $3x \equiv 5 \pmod 7$.

Exercice 7

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

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

2 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 8

1 L'équation $x^2 - x \equiv 1 \pmod 2$ a-t-elle des solutions dans $\mathbf{Z}$?
2 L'équation $x^2 - 3x - 1$ a-t-elle des solutions dans $\mathbf{Z}$?

3. Les anneaux $(\mathbf{Z}/n\mathbf{Z}, +, \times)$

Exercice 9

1 Dans l'anneau $\mathbf{Z}/3\mathbf{Z}$, calculer $(a+b)^3$ où a et b sont deux éléments.
2 Dans l'anneau $\mathbf{Z}/6\mathbf{Z}$, calculer $(a+b)^6$ où a et b sont deux éléments.
3 Dans l'anneau $\mathbf{Z}/7\mathbf{Z}$, calculer $(a+b)^7$ où a et b sont deux éléments.

Exercice 10

1 Ecrire les tables d'opération dans l'anneau $\mathbf{Z}/6\mathbf{Z}$.
2 L'application $f : \mathbf{Z}/10\mathbf{Z} \to \mathbf{Z}/3\mathbf{Z}$ construite de la manière suivante est-elle bien définie ? Pour un élément c de $\mathbf{Z}/10\mathbf{Z}$, on choisit un représentant x et on pose $f(c) := [x]_3$.

4. Inversibles de $\mathbf{Z}/n\mathbf{Z}$

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 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).
3 Montrer que si a' et a'' sont deux inverses de a modulo n alors $a' \equiv a'' \pmod n$.
4 Donner la liste des inversibles de $\mathbf{Z}/15\mathbf{Z}$.

Exercice 12

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

Exercice 13

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 14

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 15

1 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.
2 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 $\phi(2n) = 2\phi(n)$.
3 Soit n un entier qui est le produit de deux nombres premiers distincts p et q. Montrer que pour tout $x \in \mathbf{Z}$ premier avec p et q, on a $x^{(p-1)(q-1)} \equiv 1 \pmod{n}$.

Exercice 16

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

5. Sur l'algorithme RSA

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 m compris entre 0 et 142 puis le chiffre avant de transmettre à Juliette le résultat : $M = 27$.

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

Le but de cet exercice est de réussir à décrypter un message d'Isabelle envoyé à Gilles par le protocole du cryptosystème RSA.

1 Montrer que $523 = 4 \pmod{133}$.

2 Calculer $\phi(133)$.

3 Calculer l'inverse de 25 modulo 108.

4 Gilles crée sa clé publique dans le cryptosystème RSA et la publie dans l'annuaire : ($n = 133$, $e = 25$). Isabelle désire transmettre un message $m \in \{1, ...132\}$ (premier avec 133) à Gilles. Elle le chiffre à l'aide du protocole RSA en un message M et envoie M à Gilles. Exprimer M en fonction de m et de la clé publique de Gilles.

5 Véronique intercepte le message M destiné à Gilles : $M = 5$. Expliquer comment elle calcule m et donner le résultat.