

# TABLE DES MATIERES

## Chapitre 1 : Arithmétique Élémentaire

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| 1. Divisibilité .....                                                         | 6  |
| 1.1. Entiers Naturels .....                                                   | 6  |
| 1.2. Divisibilité des entiers .....                                           | 6  |
| 1.3. Division euclidienne .....                                               | 7  |
| 1.4. Système de numération .....                                              | 8  |
| 1.5. P.G.C.D. ....                                                            | 11 |
| 1.5.1. Algorithme d' <i>Euclide</i> .....                                     | 13 |
| 1.5.2. Relation de <i>Bézout</i> .....                                        | 15 |
| 1.5.3. Propriétés du P.g.c.d. ....                                            | 15 |
| 1.6. P.P.C.M. ....                                                            | 17 |
| 1.6.1. Relation entre le p.g.c.d. et le p.p.c.m. ....                         | 18 |
| 1.6.2. Propriétés du P.p.c.m. ....                                            | 18 |
| 2. Nombres premiers .....                                                     | 19 |
| 2.1. Infinité des nombres premiers .....                                      | 20 |
| 2.2. Une propriété des nombres premiers .....                                 | 21 |
| 2.3. Le crible d' <i>Erathostène</i> .....                                    | 22 |
| 2.4. Le théorème fondamental de l'Arithmétique .....                          | 23 |
| 2.4.1. Le théorème d' <i>Euclide</i> .....                                    | 23 |
| 2.4.2. Le théorème fondamental de l'Arithmétique .....                        | 25 |
| 2.4.3. Applications .....                                                     | 25 |
| 2.5. Le théorème des nombres premiers dans une progression arithmétique ..... | 27 |
| Exercices .....                                                               | 29 |

## Chapitre 2 : Fonctions Arithmétiques

|                                                               |    |
|---------------------------------------------------------------|----|
| 1. Introduction .....                                         | 37 |
| 2. Définitions et exemples .....                              | 38 |
| 3. Algèbre des fonctions arithmétiques .....                  | 40 |
| 3.1. fonctions arithmétiques additives .....                  | 40 |
| 3.2. fonctions arithmétiques multiplicatives .....            | 41 |
| 3.3. Convolution de <i>Dirichlet</i> .....                    | 43 |
| 3.4. Inverse d'une fonction arithmétique multiplicative ..... | 45 |
| 4. Etude de certaines fonctions arithmétiques .....           | 48 |

|                                                    |    |
|----------------------------------------------------|----|
| 4.1. La fonction $d$ diviseur                      | 48 |
| 4.2. La fonction $\sigma$ somme des diviseurs      | 49 |
| 4.3. La fonction $\sigma_r$                        | 51 |
| 4.4. La fonction $\varphi$ indicatrice d'Euler     | 52 |
| 5. Formule d'inversion de Möbius                   | 54 |
| 6. Nombres parfaits                                | 55 |
| 7. Nombres de Mersenne                             | 57 |
| 8. Nombres de Fermat                               | 59 |
| 9. Propriétés des nombres de Fermat et de Mersenne | 61 |
| Exercices                                          | 63 |

### Chapitre 3 : Congruences I

|                                                             |     |
|-------------------------------------------------------------|-----|
| Introduction                                                | 73  |
| 1. Définitions et Propriétés élémentaires                   | 74  |
| 1.1. L'anneau $\mathbb{Z}/n\mathbb{Z}$                      | 75  |
| 1.2. Générateurs du groupe additif $\mathbb{Z}/n\mathbb{Z}$ | 76  |
| 1.3. Inverse arithmétique                                   | 76  |
| 1.4. Le groupe $U(\mathbb{Z}/n\mathbb{Z})$                  | 77  |
| 2. Applications des congruences                             | 82  |
| 2.1. Critères de divisibilité                               | 82  |
| 2.2. Reste modulo un entier                                 | 84  |
| 2.3. Système complet de restes modulo $n$                   | 84  |
| 2.4. Système réduit de restes modulo $n$                    | 86  |
| 3. Congruences particulières                                | 88  |
| 3.1. Le "petit" théorème de Fermat                          | 88  |
| 3.2. Nombres pseudo-premiers                                | 91  |
| 3.3. Nombres de Carmichael                                  | 93  |
| 3.4. Le théorème d'Euler                                    | 95  |
| 3.5. L'indicateur de Carmichael                             | 97  |
| 3.6. Le théorème de Wilson-Ibn-Al-Haythem                   | 100 |
| 4. Quelques applications des congruences                    | 101 |
| 4.1. Carrés modulo $p$                                      | 101 |
| 4.2. Facteurs premiers des nombres de Mersenne              | 102 |
| 4.3. Facteurs premiers des nombres de Fermat                | 103 |
| 5. Racines primitives                                       | 105 |
| 5.1. Ordre d'un entier modulo $m$                           | 105 |
| 5.2. Racines primitives                                     | 106 |
| Exercices                                                   | 111 |

### Chapitre 4 : Congruences II

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| Introduction                                                        | 121 |
| 1. Congruences linéaires à une inconnue                             | 121 |
| 2. Congruences linéaires à deux inconnues                           | 124 |
| Application : Equation Diophantienne linéaire                       | 126 |
| 3. Congruences Simultanées                                          | 129 |
| 4. Congruences Quadratiques à une inconnue                          | 133 |
| 4.1. Symbole de Legendre                                            | 137 |
| 4.2. Propriétés du symbole de Legendre                              | 137 |
| 4.3. Loi de réciprocité quadratique                                 | 142 |
| 4.4. Applications                                                   | 145 |
| 4.4.1. Calcul de $\left(\frac{3}{p}\right)$                         | 145 |
| 4.4.2. Facteurs premiers des nombres de Fermat                      | 146 |
| 4.4.3. Facteurs premiers des nombres de Mersenne                    | 146 |
| 4.4.4. Equations Diophantiennes quadratiques de plusieurs variables | 147 |
| 4.4.5. Sommes de deux carrés                                        | 149 |
| 4.5. Symbole de Jacobi                                              | 154 |
| 4.5.1. Propriétés du symbole de Jacobi                              | 154 |
| 4.5.2. Applications                                                 | 160 |
| 4.6. Symbole de Kronecker                                           | 163 |
| 4.6.1. Définition du symbole de Kronecker                           | 163 |
| 4.6.2. Propriétés du symbole de Kronecker                           | 163 |
| Exercices                                                           | 165 |

### Chapitre 5 : Congruences Polynômes

|                                                                      |     |
|----------------------------------------------------------------------|-----|
| Introduction                                                         | 171 |
| 1. Congruences polynômes à une inconnue                              | 171 |
| 1.1. Congruences polynômes de module $p$ premier                     | 171 |
| 1.2. Congruences polynômes de module composé                         | 174 |
| 2. Résolution des congruences quadratiques                           | 182 |
| 2.1. Cas où le module est un nombre premier                          | 182 |
| 2.2. Cas où le module est un entier $m$ quelconque                   | 186 |
| 2.2.1. Cas où $m = p^k$ avec $p$ premier impair et $k \geq 1$ entier | 187 |
| 2.2.2. Cas où $m = 2^k$ avec $k \geq 1$ entier                       | 188 |

|                                                    |     |
|----------------------------------------------------|-----|
| 3. Utilisation des racines primitives .....        | 190 |
| 3.1. Résolution des congruences de degré $k$ ..... | 191 |
| 3.2. Critère d' <i>Euler</i> .....                 | 192 |
| Exercices .....                                    | 195 |

## Chapitre 6 : Fractions Continues

|                                                             |     |
|-------------------------------------------------------------|-----|
| Introduction .....                                          | 199 |
| 1. Fractions continues simples .....                        | 200 |
| 1.1. Egalité de deux Fractions continues simples finies ... | 202 |
| 1.2. Réduites .....                                         | 203 |
| <b>Applications :</b>                                       |     |
| Résolution de l'équation Diophantienne linéaire             |     |
| à deux variables $ax - by = c$ .....                        | 208 |
| 1. Recherche d'une solution particulière de                 |     |
| l'équation Diophantienne linéaire $ax - by = 1$ .....       | 208 |
| 2. Recherche de la solution générale de                     |     |
| l'équation Diophantienne linéaire $ax - by = \pm 1$ .....   | 209 |
| 3. Résolution de l'équation Diophantienne                   |     |
| linéaire $ax - by = c$ .....                                | 210 |
| 2. Fractions continues simples infinies .....               | 211 |
| 2.1. Propriétés des réduites .....                          | 211 |
| 2.2. Développement d'un nombre irrationnel                  |     |
| en fraction continue .....                                  | 213 |
| 2.3. Approximation d'un nombre irrationnel .....            | 214 |
| 3. Fractions continues périodiques .....                    | 217 |
| 3.1. Fractions continues périodiques .....                  | 217 |
| 3.2. Fractions continues purement périodiques .....         | 223 |
| 4. Equation de <i>Pell-Fermat</i> .....                     | 227 |
| 5. Développement en fraction continue de $\pi$ .....        | 236 |
| 3. Développement en fraction continue de $e$ .....          | 237 |
| Exercices .....                                             | 238 |

## Chapitre 7 : Critères de primalité

|                                 |     |
|---------------------------------|-----|
| 1. Tests de primalité .....     | 243 |
| Théorème de <i>Lucas</i> .....  | 245 |
| Théorème de <i>Lehmer</i> ..... | 245 |

|                                                                 |     |
|-----------------------------------------------------------------|-----|
| Théorème de <i>Lucas-Lehmer</i> .....                           | 246 |
| Théorème de <i>Brillhart-Selfridge</i> .....                    | 246 |
| Théorème de <i>Pocklington</i> .....                            | 247 |
| Théorème de <i>Proth</i> .....                                  | 248 |
| 2. Tests de primalité pour des entiers particuliers .....       | 248 |
| 2.1. Test de primalité pour les nombres de <i>Fermat</i> .....  | 248 |
| Théorème de <i>Pépin</i> .....                                  | 249 |
| 2.2. Test de primalité pour les nombres de <i>Mersenne</i> .... | 250 |

## Chapitre 8 : Cryptographie

|                                                             |     |
|-------------------------------------------------------------|-----|
| 1. Les algorithmes de base .....                            | 253 |
| 1.1. L'algorithme d' <i>Euclide</i> .....                   | 254 |
| 1.2. L'algorithme étendu d' <i>Euclide</i> .....            | 254 |
| 1.3. Le théorème des restes chinois .....                   | 254 |
| 1.4. Algorithme des puissances .....                        | 254 |
| 1.5. Le cas modulaire .....                                 | 255 |
| 1.6. Les symboles de <i>Legendre</i> et <i>Jacobi</i> ..... | 255 |
| 1.7. Racine carrée modulaire .....                          | 255 |
| 2. Protocoles de cryptographie .....                        | 257 |
| 3. Protocole R.S.A. ....                                    | 258 |

## Corrigé des Exercices .....

|                                           |     |
|-------------------------------------------|-----|
| Corrigé des Exercices du chapitre 1 ..... | 262 |
| Corrigé des Exercices du chapitre 2 ..... | 278 |
| Corrigé des Exercices du chapitre 3 ..... | 296 |
| Corrigé des Exercices du chapitre 4 ..... | 312 |
| Corrigé des Exercices du chapitre 5 ..... | 320 |
| Corrigé des Exercices du chapitre 6 ..... | 326 |

## Annexe .....

## Index Terminologique .....

## Index des Noms Propres .....

## Bibliographie .....