Table des matières

CHAPITRE 1 : LA MAITRISE DE MATHEMATICA

Introduction	10
I. Les notions de base	12
1. Les diverses notions d'égalité en calcul formel	12
1.1 L'affectation	12
1.2 La comparaison	12
2. Les règles de substitution	13
2.1 Généralités sur les règles de substitution	13
2.2 Les primitives ReplaceAll et ReplaceRepeated	14
2.3 Conversion de règles	15
3. Listes et expressions	16
3.1 Etude des listes	16
3.2 Etude des expressions	28
4. Les fonctions	30
4.1 Généralités sur les fonctions	30
4.2 Définition d'une fonction avec conditions	33
4.3 Définition d'une fonction avec variables locales	35
4.4 Les fonctions pures	36
4.5 Les fonctions à mémoire et la récursivité	37
4.6 Compilation d'une fonction	38
4.7 Compléments sur les fonctions	40

5. Simplifier en calcul formel	41
5.1 La problématique de la simplification	41
5.2 Les primitives fondamentales de simplification	41
5.3 Exemples de simplification d'expressions	42
6. Le filtrage et la reconnaissance des formes	44
6.1 Les primitives de reconnaissance des formes	44
6.2 Exemples élémentaires	44
6.3 Les fonctions-tests	45
6.4 Fonctions-tests et fonctions pures	48
6.5 Les formes	49
7. Les fichiers de commandes	54
7.1 Généralités sur les packages	54
7.2 Charger un fichier de commandes	54
7.3 Ecrire un package	55
II. Initiation à la programmation	56
1. Les instructions conditionnelles	56
1.1 Le test If	56
1.2 La primitive Which	57
1.3 La primitive Switch	57
1.4 Les règles de réécriture	58
2. Les boucles	59
2.1 Les boucles en programmation procédurale	59
2.2 Les boucles dans le pur style Mathematica	62
3. Les différents styles de programmation	64
3.1 En quoi consiste la programmation	64
3.2 La programmation procédurale	64
3.3 La programmation par reconnaissance de formes	65
3.4 La programmation fonctionnelle	66
3.5 La programmation par règles de réécriture	67

4. Conseils de programmation	68
4.1 Maîtriser la syntaxe	68
4.2 Choisir des identificateurs explicites	69
4.3 Diviser le programme en fonctions élémentaires	69
4.4 Eviter la programmation procédurale	69
4.5 Purger la mémoire fréquemment	70
4.6 Exploiter messages d'erreur et avertissements	70
4.7 Utiliser l'aide du menu Help	70
4.8 Compléments	71
III. Mathematica en action	72
1. Exemple en arithmétique	72
1.1 Résolution en calcul formel	72
1.2 Solution arithmétique : neurones en action	73
2. Rang d'une famille de fonctions itérées	74
2.1 Résolution pas à pas	74
2.2 Généralisation	75
3. Résolution d'une équation intégrale	76
3.1 Analyse : recherche des solutions possibles	76
3.2 Vérification	78
4. Exemple en géométrie : recherche d'un ensemble de points	78
4.1 Solution Mathematica	78
4.2 Solution théorique	80
IV. Exercices	81

CHAPITRE 2 : ARITHMETIQUE

I. Les fonctions du système	134
1. Division euclidienne, pgcd, ppcm	134
2. Décomposition d'un entier en facteurs premiers	134

3. Nombres premiers	135
II. Divisibilité et nombres premiers	136
1. Division euclidienne	136
1.1 Algorithme de la division euclidienne par soustractions	136
1.2 Programmation fonctionnelle	136
1.3 Programmation récursive	139
2. Diviseurs d'un entier	141
2.1 Recherche des diviseurs d'un entier	141
2.2 Nombre de diviseurs d'un entier	142
2.3 Nombres parfaits, amiables et nombres d'Euclide	143
3. PGCD et PPCM d'entiers naturels	146
3.1 Algorithme d'Euclide	146
3.2 Calcul du pgcd d'une liste entiers naturels	148
3.3 Algorithme d'Euclide étendu	149
3.4 La fonction indicateur d'Euler et la fonction de Möbius	151
4. Applications	154
4.1 Nombres dont le pgcd et le ppcm sont donnés	154
4.2 Entiers dont le pgcd et la somme des carrés sont fixés	156
4.3 Entiers dont le ppcm et la somme des carrés sont fixés	157
4.4 Equation diophantienne du type $ax + by = c$	158
5. Les nombres premiers	160
5.1 Le crible d'Erathostène	160
5.2 Algorithme de Meissel-Lehmer	163
6. Les nombres de Fermat	164
6.1 Présentation des nombres de Fermat	164
6.2 Primalité des nombres de Fermat	165
6.3 Limites de la décomposition en facteurs premiers	166
6.4 Remarques	166
6.5 Le test de Pépin	167
6.6 Nombre de chiffres des nombres de Fermat	168
6.7 Conclusion	169
6.8 Questions d'arithmétique sur les nombres de Fermat	169

7. Les nombres de Mersenne	170
7.1 Présentation des nombres de Mersenne	170
7.2 Diviseurs des nombres de Mersenne	170
7.3 Le test de primalité de Lucas	171
7.4 Une alternative : le petit théorème de Fermat	173
7.5 Les nombres pseudo-premiers	175
8. Méthodes de factorisation des grands entiers	176
8.1 La factorisation ρ de Pollard	176
8.2 Algorithme de Dixon	179
III. Arithmétique modulaire	184
1. L'anneau $\mathbb{Z}/n\mathbb{Z}$	184
1.1 La relation de congruence dans $\mathbb{Z}$	184
1.2 Exemples de congruences	184
2. Eléments inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$	189
2.1 Définition du groupe des unités	189
2.2 Détermination des unités	189
2.3 Théorème d'Euler et petit théorème de Fermat	190
3. Le théorème des restes chinois	191
3.1 Exemple	192
3.2 Programmation par passage au crible	192
3.3 Le théorème des restes chinois version algébrique	193
3.4 Enoncé du théorème	193
3.5 Algorithme de résolution	194
3.6 Le programme	194
3.7 Le théorème des restes chinois version Mathematica	195
4. Application à la cryptographie	195
4.1 Le codage RSA	195
4.2 Théorie arithmétique	196
4.3 La programmation	196
4.4 Authentification des auteurs de messages	197
IV. Etude des résidus quadratiques	198

1. Symbole de Legendre et de Jacobi	198
1.1 Résidus quadratiques	198
1.2 Définition du symbole de Legendre	199
1.3 Formule d'Euler	199
1.4 Symbole de Jacobi	200
2. Loi de réciprocité quadratique	201
2.1 Énoncé de la loi	201
2.2 Vérification expérimentale	201
3. Racines primitives de l'unité	202
3.1 Notion de racine primitive	202
3.2 Recherche des racines primitives	203
4. Test probabiliste de Soloway Strassen	204
4.1 Résultats théoriques	204
4.2 Témoins de non primalité	204
4.3 Nombres probablement premiers	205
5. Test de Miller-Rabin	206
5.1 Témoins de Miller	207
5.2 Nombres premiers probables	207
V. Les entiers de Gauss	208
1. L'anneau euclidien des entiers de Gauss	208
1.1 Définition d'un anneau euclidien	208
1.2 Anneau des entiers de Gauss	208
1.3 Calcul de pgcd d'entiers de Gauss	209
1.4 Décomposition en facteurs irréductibles	210
1.5 Décomposition en facteurs irréductibles sous Mathematica	211
2. Décomposition d'un entier en somme de deux carrés	213
2.1 Généralités	213
2.2 Cas d'un nombre premier congru à 1 modulo 4	214
2.3 Cas d'un entier naturel quelconque	216
2.4 Un autre algorithme de décomposition d'un nombre premier	218
VI. Exercices	221

CHAPITRE 3 : ANNEXES

I. Notions avancées	280
1. Définition d'une fonction à options	280
2. Définition d'une fonction avec variables optionnelles	281
2.1 Sélection dans une liste	281
2.2 Sélection dans une liste d'une sous-liste de longueur donnée	282
2.3 Sélection avec argument optionnel	283
3. Définition d'un fichier de commandes	284
3.1 Généralités	284
3.2 Ecriture d'un package de fonctions	284
3.3 Appel et utilisation du package	285
 II. Thèmes d'étude	 287
1. Problème du monnayeur, le système monétaire européen	287
1.1 Thème	287
1.2 Enoncé	287
1.3 Solution Mathematica	289
2. Le Mastermind	293
2.1 Parties de Mastermind	293
2.2 Règles	293
2.3 Mathematica codeur	293
2.4 Mathematica décodeur	297
2.5 Mathematica joue seul	299
2.6 Parties longues, parties courtes	304
2.7 Parties bien jouées, parties mal jouées	305
2.8 Questions proposées	307
3. Le critère de Lucas	307
3.1 Enoncé du problème (ENS)	307
3.2 Corrigé détaillé	309

III. Compléments d'algèbre	316
1. Structure de groupe	316
1.1 Notion de groupe, sous-groupe d'un groupe	316
1.2 Morphisme de groupes, noyau et image	316
1.3 Groupe fini, ordre d'un élément	316
1.4 Groupe cyclique	317
1.5 Le groupe symétrique d'ordre n	317
2. Structure d'anneau	317
2.1 Notion d'anneau	317
2.2 Groupe des éléments inversibles d'un anneau	318
2.3 Sous-anneau, idéal d'un anneau	318
2.4 Formule du binôme de Newton	318
2.5 Anneau intègre et anneau principal	318
2.6 PGCD et relation de Bézout dans un anneau principal	319
3. Structure de corps	319
3.1 Définition d'un corps	319
3.2 Caractéristique d'un corps	319
3.3 Propriétés	319
Bibliographie	321
Index	323