

Delphine Massenet

L'ARITHMÉTIQUE

EN PRATIQUE

De la division
au chiffrement
de messages secrets



Table des matières

Chapitre I. Les mots clefs de la logique mathématique.....	9
1 Hypothèse, proposition, proposition réciproque, contraposée, théorème	9
2 Condition nécessaire, condition suffisante.....	10
3 Conjecture, théorème, proposition	11
4 Généralités sur les démonstrations.....	13
5 Démonstration par récurrence.....	13
6 Démonstration par l'absurde	14
Chapitre II. Rappels sur les techniques de calcul.....	15
1 Calcul littéral.....	15
1.1 Simple développement.....	15
1.2 Double développement	17
1.3 Les identités remarquables	19
1.4 Règles de suppression des parenthèses.....	23
2 Notations somme et produit	23
3 Les fractions	24
3.1 Définitions	24
3.2 Règles de calcul	25
4 Les puissances d'un nombre.....	28
4.1 Définition et propriétés.....	28
4.2 Puissance de puissance d'un nombre	30
4.3 Les puissances de dix	30
5 Inégalité et opérations	33
6 Fonction.....	34
7 Partie entière d'un nombre	36
Chapitre III. Les nombres entiers - Divisibilité.....	37
1 Les nombres entiers.....	37
2 Divisibilité.....	39
3 Critères de divisibilité	46
4 Application : les années bissextiles	47
5 Février 2021, un bel exemple de « fake news ».....	48

Chapitre IV. Les codes détecteurs d'erreur de saisie	51
1 Deux outils pour comprendre.....	51
1.1 La division euclidienne dans \mathbb{N}	51
1.2 Les nombres premiers.....	54
2 La carte Vitale.....	62
3 Les codes ISBN des livres.....	64
4 Les codes-barres.....	66
5 Les cartes bancaires - Algorithme de Luhn.....	67
Chapitre V. Les congruences	69
1 Les outils pour comprendre	70
1.1 Tout le monde connaît les congruences.....	70
1.2 Règles de calcul	73
1.3 Éléments inversibles	75
1.4 PGCD.....	76
1.5 Calcul du PGCD par l'algorithme d'Euclide.....	78
1.6 Théorème de Bézout.....	80
1.7 Lemme de Gauss.	82
1.8 Algorithme d'Euclide étendu.....	85
2 Démonstration des critères de divisibilité.....	87
3 Les numéros RIB et IBAN des comptes bancaires.....	88
Chapitre VI. Le théorème des restes chinois.....	91
1 Le théorème des restes chinois	91
2 Comprendre par l'exemple	92
3 Méthode de résolution d'un système de congruences	93
4 Solstice d'été et pleine Lune.....	94
5 Exemples historiques chinois	96
5.1 Le problème des objets de Sun Zi	96
5.2 Un problème de Qin Jiushao.....	98
5.3 Le problème des voleurs, de Qin Jiushao	101
6 Les pièces d'or, les pirates et le cuisinier	101
7 Le problème des œufs	101
7.1 Les outils pour comprendre - Le PPCM	102
7.2 Le problème des œufs.....	102
Chapitre VII. Le chiffrement RSA	105
1 Quelques généralités sur la cryptographie et ses méthodes.....	105
2 Comprendre le chiffrement RSA par l'exemple	107

3	Les outils pour comprendre	109
3.1	Les éléments inversibles modulo n	109
3.2	Le petit théorème de Fermat.....	110
3.3	L'indicatrice d'Euler	113
3.4	Algorithme d'exponentiation rapide modulo n	115
4	Procédure générale argumentée.....	116
5	Un autre exemple.....	117
6	Tests de primalité	118
7	Un programme Python pour chiffrer et déchiffrer RSA.....	120
8	Attaquer RSA par la factorisation des nombres entiers ?	121
9	Utilisations de RSA.....	124
Chapitre VIII. Le chiffrement Diffie-Hellman		125
1	Les outils pour comprendre : les générateurs d'un ensemble.....	125
2	Fonctionnement.....	127
3	L'attaque de l'homme au milieu.....	129
Chapitre IX. Conjectures célèbres		131
1	Les nombres amis - Les nombres parfaits	131
2	Les nombres de Fermat	133
3	Les nombres de Mersenne.....	135
4	Les nombres premiers de Sophie Germain.....	136
5	La conjecture de Goldbach.....	137
6	D'autres conjectures célèbres	137
Chapitre X. Corrigé des exercices		139
Bibliographie		193
Index.....		195
Notations		197