

# Tables des Matières

<b>1</b>	<b>LES NOMBRES ENTIERS .....</b>	<b>1</b>
1.1	NOTATIONS	1
1.2	LES BASES DE NUMERATION	1
1.3	LES OPERATIONS DE BASE	2
1.3.1	L'addition	2
1.3.1.1	Quelques propriétés de l'opération d'addition :	2
1.3.1.2	Table d'addition	3
1.3.2	La soustraction	3
1.3.2.1	Un tour de magie arithmétique	3
1.3.3	La multiplication	4
1.3.3.1	Propriétés de l'opération de multiplication	5
1.3.3.2	La multiplication égyptienne	6
1.3.3.3	Multiplication à la russe	7
1.3.3.4	La multiplication italienne	8
1.3.3.5	Exercice :	9
1.3.4	La division	10
1.3.4.1	Un peu de terminologie	10
1.4	LE ROLE DES PARENTHESES	11
1.5	LA NOTION DE PARITE	12
1.6	LA PREUVE PAR NEUF	12
1.7	L'ELEVATION A LA PUISSANCE	13
1.7.1	Propriétés :	13
1.8	EXTRACTION DE RACINE CARREE	13
1.9	L'OPERATION FACTORIELLE	13
1.9.1	La primorielle	14
1.10	RELATION D'ORDRE	15
1.11	LA NOTION DE MOYENNE	15
1.12	LES CHANGEMENTS DE BASE	16
1.13	EXERCICES	18
1.14	RAPPELS : LES IDENTITES ET INEGALITES REMARQUABLES	18
<b>2</b>	<b>QUELQUES TECHNIQUES DE CALCUL MENTAL ET MANUEL ....</b>	<b>21</b>
2.1	LES IDENTITES REMARQUABLES	21
2.2	L'ADDITION	21
2.3	LA MULTIPLICATION	22
2.3.1	Multiplication par 10 et par 5	22
2.3.2	Multiplication par 9	22

2.3.3	Multiplication par 11	22
2.3.3.1	Multiplication par 11 d'un entier à 2 chiffres	22
2.3.3.2	Multiplication par 11 d'un nombre quelconque	22
2.3.4	multiplication de 2 nombres de 2 chiffres $1x$ par $1y$	23
2.4	ÉLEVATION AU CARRE D'UN NOMBRE ENTIER DE 2 CHIFFRES	23
2.5	MULTIPLICATION DE 2 ENTIERS EQUIDISTANTS D'UN AUTRE NOMBRE	24
2.6	ÉLEVATION D'UN NOMBRE DE 2 CHIFFRES SE TERMINANT PAR 5 AU CARRE	24
2.7	DIFFERENCE DE 2 CARRES	25
2.8	CALCUL DE CUBES	25
2.9	LES TECHNIQUES DE MULTIPLICATION RAPIDE	26
2.10	CALCUL APPROCHE D'UNE RACINE CARREE	27
2.11	EXTRACTION SANS CALCULETTE D'UNE RACINE CARREE	27
2.12	EXTRACTION SANS CALCULETTE D'UNE RACINE CUBIQUE	30
2.13	EXERCICES	31
<b>3</b>	<b>DES TOURS DE MAGIE MATHÉMATIQUE.....</b>	<b>33</b>
3.1	INTRODUCTION	33
3.2	LE RESTE EST TOUJOURS 6	33
3.3	DEVINER LE RESULTAT FINAL	33
3.4	DEVINER LES AUTRES CHIFFRES	34
3.5	DEVINER LES DIVISEURS	35
3.6	DEVINER LE RESTE	36
3.7	MULTIPLICATION DONNANT LES MEMES CHIFFRES :	36
3.8	DEVINER LA DATE D'ANNIVERSAIRE	36
3.9	DEVINER LE RESTE	37
3.10	RETROUVER LE CHIFFRE OUBLIE	38
3.11	EXTRACTION DE TETE D'UNE RACINE 5 EME	38
3.12	EXTRACTION DE TETE D'UNE RACINE CUBIQUE	39
3.13	LE JEU DE MARIENBAD	41
3.14	CONCLUSION	42
<b>4</b>	<b>LES TECHNIQUES DE DEMONSTRATION .....</b>	<b>43</b>
4.1	INTRODUCTION	43
4.2	UN PEU DE TERMINOLOGIE	43
4.3	LA DEMONSTRATION DIRECTE	43
4.4	LA DEMONSTRATION PAR RECURRENCE	44
4.5	LA DEMONSTRATION PAR L'ABSURDE	44
4.6	LA TECHNIQUE DE LA DESCENTE INFINIE	44
4.7	LA VERIFICATION PAR ORDINATEUR	47
4.8	LES FAUSSES DEMONSTRATIONS	47
4.9	UN PARADOXE INTERESSANT	48
<b>5</b>	<b>SOMME DE SUITES DE NOMBRES ENTIERS.....</b>	<b>51</b>
5.1	SOMME DES N PREMIERS NOMBRES ENTIERS	51

5.2	SOMME DES NOMBRES IMPAIRS DE $1$ A $2N + 1$ :	51
5.2.1	Lemme relatif aux sommes $S_{pp}(2n)$	52
5.3	SOMME DES CARRES DES $N$ PREMIERS NOMBRES	52
5.4	SOMME DES CARRES DES NOMBRES PAIRS DE $2$ A $2N$	53
5.5	SOMME DES CARRES DES $N$ PREMIERS NOMBRES IMPAIRS	53
5.6	SOMME DES CUBES DES $N$ PREMIERS NOMBRES	53
5.7	SOMME DES PUISSANCES TROISIEMES DES $N$ PREMIERS ENTIERS PAIRS	54
5.8	SOMME DES PUISSANCES TROISIEMES DES $N$ PREMIERS ENTIERS IMPAIRS	55
5.9	SOMME DES PUISSANCES QUATRIEMES DES $N$ PREMIERS NOMBRES ENTIERS	55
5.10	TABLEAU RECAPITULATIF DES RESULTATS OBTENUS	56
5.11	SOMME ALTERNEE DE CARRES	56
5.12	LE TRIANGLE DE NICOMAUQUE	57
5.12.1	Corollaire 1	58
5.12.2	Corollaire 2	58
5.13	LA RELATION DE JACOBI	59
5.14	CONCLUSION	60
<b>6</b>	<b>LA DIVISIBILITE .....</b>	<b>61</b>
6.1	INTRODUCTION	61
6.2	RESTE LORS D'UNE DIVISION	61
6.3	RESTE DE LA DIVISION D'UNE SOMME DE NOMBRES	62
6.4	RESTE DE LA DIVISION D'UN PRODUIT DE NOMBRES	62
6.5	LE PGCD (PLUS GRAND COMMUN DIVISEUR)	62
6.5.1	Techniques de calcul du PGCD de 2 nombres	63
6.6	LE PPCM (PLUS PETIT COMMUN MULTIPLE)	63
6.7	THEOREME DE BACHET	64
6.8	QUELQUES THEOREMES RELATIVES A LA DIVISIBILITE	65
6.8.1	Un théorème de Fermat démontré en 1640 :	65
6.8.2	Théorème de Sophie Germain	66
6.8.3	Théorème de Wilson	66
6.9	NOTION DE CONGRUENCES	66
6.10	DIVISIBILITE PAR 2, 3, 5, 6, 9 ET 18	67
6.11	DIVISIBILITE PAR $2^p$ ET PAR $5^p$	67
6.12	DIVISIBILITE PAR 7	68
6.12.1	1 <sup>er</sup> critère	68
6.12.2	2 <sup>ème</sup> critère	68
6.13	DIVISIBILITE PAR 11	69
6.14	DIVISIBILITE PAR 13	70
6.15	DIVISIBILITE PAR 17	71
6.16	DIVISIBILITE PAR 19	71
6.17	DIVISIBILITE PAR 23	73
6.18	DIVISIBILITE PAR 25	73
6.19	DIVISIBILITE PAR 29	73
6.20	DIVISIBILITE PAR 31	74

6.21	DIVISIBILITE PAR 37	74
6.22	DIVISIBILITE PAR 41	75
6.23	DIVISIBILITE PAR 73	75
6.24	DIVISIBILITE PAR 101	76
6.25	DIVISIBILITE PAR 137	76
6.26	UN CRITERE GENERAL	76
6.27	THEOREME DE WOLSTENHOLME	77
6.28	EXERCICES	77
6.28.1	Le produit de 2 ou 3 nombres consécutifs ne peut pas être un carré	77
6.28.2	La somme des cubes de 3 entiers consécutifs est divisible par 9	78
6.28.3	Si $n$ est entier positif, alors la somme $S = n^3/6 + n^2/2 + n/3$ est entière.	78
6.28.4	Démontrer que $n^5 - n$ est divisible par 30	79
6.28.5	Si la somme des 3 entiers naturels $a + b + c$ est divisible par 6, alors la somme $S = a^3 + b^3 + c^3$ est aussi divisible par 6	79
6.28.6	Multiplies ne s'écrivant qu'avec des 1	79
6.28.7	$2000^{1653} - 1$ divisible par 1999	80
6.28.8	Nombres palindromes qui sont des carrés	80
6.29	CONCLUSION	81
<b>7</b>	<b>LES FRACTIONS .....</b>	<b>83</b>
7.1	DEFINITION	83
7.2	SIMPLIFICATION D'UNE FRACTION	83
7.2.1	Cas particulier de fractions égales	83
7.3	ADDITION ET SOUSTRACTION DE 2 FRACTIONS	84
7.4	MULTIPLICATION DE 2 FRACTIONS	84
7.5	DIVISION DE 2 FRACTIONS	84
7.6	LA SIMPLIFICATION DU CANCRE	84
7.6.1	Une démonstration montrant comment on peut trouver ces nombres	85
7.7	L'ADDITION DU CANCRE	86
7.8	DECOMPOSITION EN FRACTIONS EGYPTIENNES	87
7.9	CONJECTURE D'ERDÖS	87
7.10	LES ERREURS DE SIMPLIFICATION	87
7.11	L'APPROXIMATION AU MOYEN D'UNE FRACTION CONTINUE	88
7.12	EXERCICES	91
7.12.1	La durée de vie de Diophante	91
7.12.2	Vitesse du radeau	92
7.12.3	Vitesse moyenne d'une automobile	92
7.12.4	Comment arriver à l'heure	93
7.12.5	Fractionner le nombre 45	93
7.12.6	Les dosages	94
7.12.7	Les départs du tramway	95
7.12.8	Les problèmes de robinets	96
7.12.8.1	Problème de base :	96
7.12.8.2	Second problème de robinets	96
7.12.9	Bacchus et Silène	97

<b>8</b>	<b>LES MOYENNES.....</b>	<b>99</b>
8.1	INTRODUCTION	99
8.2	LES DIFFERENTES MOYENNES	99
8.3	LA MOYENNE ARITHMETIQUE	99
8.4	LA MOYENNE GEOMETRIQUE	100
8.5	LA MOYENNE HARMONIQUE	100
8.6	LA MOYENNE QUADRATIQUE	102
8.7	COMPARAISON DES 4 MOYENNES PRECEDENTES	102
8.7.1	La moyenne géométrique est toujours inférieure à la moyenne arithmétique	103
8.8	MOYENNE PONDEREE	103
8.9	EXERCICES	105
8.9.1	Un petit problème de Physique	105
8.10	CONCLUSION	106
<b>9</b>	<b>NOMBRES PREMIERS.....</b>	<b>107</b>
9.1	INTRODUCTION	107
9.2	DEFINITION	107
9.3	RECHERCHE DES NOMBRES PREMIERS	107
9.3.1	Le crible d'Eratosthène	108
9.3.1.1	Une amélioration dans la recherche :	108
9.4	METHODE PAR DIVISION	109
9.5	INTERPRETATION GEOMETRIQUE	109
9.5.1	Interprétation des nombres premiers :	109
9.5.2	Interprétation des nombres premiers entre eux.	110
9.6	RECHERCHE DE TRES GRANDS NOMBRES PREMIERS	110
9.6.1	Le test de Fermat :	111
9.7	NOMBRES PREMIERS ENTRE EUX	111
9.8	UN TOUR DE MAGIE AVEC LES NOMBRES PREMIERS	111
9.9	NOMBRES PREMIERS JUMENTS	113
9.10	LA SUITE DES NOMBRES PREMIERS EST ILLIMITEE	114
9.11	THEOREME DE DIRICHLET	116
9.12	LE POSTULAT DE BERTRAND	116
9.12.1	Une digression vers les séries :	116
9.13	CONJECTURE DE LEGENDRE :	117
9.14	RECAPITULATION DES RESULTATS :	118
9.15	DECOMPOSITION DES NOMBRES PREMIERS	118
9.15.1	Décomposition en différence de 2 carrés	118
9.15.2	Un théorème de Fermat	119
9.16	DECOMPOSITION EN FACTEURS PREMIERS	119
9.17	CONJECTURE DE GOLDBACH	120
9.18	THEOREME DE FERMAT ET WILSON	121
9.19	NOMBRES PREMIERS ENTRE EUX	121
9.20	THEOREMES DE SOPHIE GERMAIN	121
9.21	CLASSIFICATION DES NOMBRES PREMIERS	122

9.22	LA RAREFACTION DES NOMBRES PREMIERS	123
9.22.1	Combien de nombres premiers entre 1 et N ?	123
9.22.2	La fonction $\pi(m)$	123
9.23	SPIRALE D'ULAM	124
9.24	NOMBRES PSEUDO-PREMIERS	125
9.25	LES TESTS DE PRIMALITE	126
9.25.1	Un critère de primalité	126
9.25.1.1	Le test de Fermat	127
9.26	DES POLYNOMES DONNANT DES NOMBRES PREMIERS	127
9.27	QUELQUES PROBLEMES AMUSANTS	129
9.27.1	Réponses à ces 3 problèmes	130
<b>10</b>	<b>LES TRIPLETS ET TRIANGLES PYTHAGORICIENS.....</b>	<b>131</b>
10.1	DEFINITION	131
10.2	TRIPLETS PYTHAGORICIENS IRREDUCTIBLES	131
10.3	THEOREME D'INFINITUDE	132
10.3.1	une propriété curieuse	133
10.3.2	Exercices	133
10.4	TRIANGLES PYTHAGORICIENS	135
10.4.1	Le périmètre d'un triangle pythagoricien est toujours un nombre pair.	135
10.4.2	Triangles rectangles dont la surface est égale au périmètre	136
10.4.3	Surface d'un triangle pythagoricien	137
10.4.3.1	Conjecture de Bachet	137
10.5	LES BRIQUES DE PYTHAGORE	139
10.5.1	Exercices :	141
<b>11</b>	<b>NOMBRES FIGURES .....</b>	<b>143</b>
11.1	DEFINITIONS	143
11.2	NOMBRES TRIANGULAIRES, CARRES, PENTAGONAUX ET HEXAGONAUX	143
11.3	DEFINITION DES NOMBRES FIGURES AU MOYEN D'UNE SUITE	144
11.3.1	Nombres triangulaires	144
11.3.2	Nombres carrés	144
11.3.2.1	Nombres carrés impairs : un nombre carré impair est obligatoirement de la forme $4n + 1$	145
11.4	QUELQUES PROPRIETES DES NOMBRES TRIANGULAIRES	145
11.4.1	Un nombre triangulaire $> 3$ ne peut pas être un nombre premier :	146
11.4.2	Si T est un nombre triangulaire, alors $8T+1$ est un carré	146
11.4.3	Lemme : la somme de 2 nombres triangulaires consécutifs est un carré	147
11.4.4	Une autre propriété : Si $T_n$ est un carré parfait alors $T_{4n(n+1)}$ l'est aussi	147
11.4.5	Quelques relations entre nombres triangulaires	148
11.4.6	Autre relation	149
11.5	INVERSE DES NOMBRES TRIANGULAIRES	150
11.5.1	Décomposition d'un entier en nombres triangulaires	150
11.5.2	Généralisation à d'autres nombres figurés	151
11.5.3	Nombres triangulaires et triangle de Pascal	151
11.6	LES NOMBRES TRIANGULAIRES CARRES	152

11.7	LES NOMBRES PRONIQUES	153
11.8	INTERPRETATION GEOMETRIQUE DE LA SOMME ALTERNEE DE CARRES	155
11.9	LES NOMBRES TRAPEZOÏDAUX	156
11.10	LES NOMBRES CARRES	156
11.11	LES NOMBRES PENTAGONAUX	157
11.12	LES NOMBRES HEXAGONAUX	157
11.13	NOMBRES ETOILES ET HEXAGONAUX CENTRES	158
11.14	LES NOMBRES HEPTAGONAUX	159
11.15	LES NOMBRES TETRAEDRIQUES	159
	11.15.1 Retour sur le triangle de Pascal	161
11.16	UNE FORMULE CURIEUSE	161
11.17	LES NOMBRES GNOMONIQUES	162
	11.17.1 Les nombres gnomoniques carrés	162
	11.17.2 Technique simplifiée de l'extraction de la racine carrée	163
	11.17.3 La technique du goutte à goutte (racine carrée)	163
11.18	EXERCICES	164
	11.18.1 Rectangles dont périmètre et surface ont la même mesure	164
11.19	LES PROBLEMES DU VOL DE CANARDS	165
	11.19.1 Vol de canards en formation carrée	167
	11.19.2 Moyenne des carrés des nombres d'une ligne du triangle de Pascal	168
<b>12</b>	<b>NOMBRES PARFAITS.....</b>	<b>171</b>
12.1	INTRODUCTION	171
12.2	QUELQUES DEFINITIONS	171
12.3	RECHERCHE DES NOMBRES PARFAITS	172
12.4	PROPRIETES DES NOMBRES PARFAITS	172
	12.4.1 somme des fractions « égyptiennes »	172
	12.4.2 Liaison avec les nombres de Mersenne	173
	12.4.3 Les nombres parfaits sont tous hexagonaux	174
	12.4.4 Chiffre des unités d'un nombre parfait	174
	12.4.5 Tout nombre parfait $>6$ est la somme de cubes impairs consécutifs	175
	12.4.6 Si $p$ est parfait, alors pour tout $n > 1$ le nombre $np$ est abondant.	178
	12.4.7 Une curiosité des nombres parfaits	178
12.5	FONCTION SOMME DES DIVISEURS	179
12.6	NOMBRES UNITAIREMENT PARFAITS	179
12.7	NOMBRES PRESQUE PARFAITS	180
12.8	THEOREME : LES PUISSANCES DE 2 SONT DES NOMBRES PRESQUE PARFAITS	181
12.9	NOMBRES TRIPARFAITS	182
12.10	CONCLUSION	182
<b>13</b>	<b>DECOMPOSITION DES NOMBRES .....</b>	<b>183</b>
13.1	INTRODUCTION	183
13.2	DECOMPOSITION EN CARRES	183
	13.2.1 Théorème de Lagrange	183
	13.2.2 Théorème des trois carrés	184

13.2.3	Théorème des deux carrés	185
13.2.4	Décomposition en somme de 3 carrés	186
13.2.5	Théorème : tout nombre impair est égal à une différence de 2 carrés	186
13.2.5.1	Théorème d'Eisenstein	188
13.2.5.2	Tout nombre de la forme $4n + 2$ n'est pas décomposable en différence de deux carrés.	188
13.3	CONJECTURE DE GOLDBACH	188
13.3.1	Tout nombre pair $> 2$ est décomposable en une somme de 2 nombres premiers	189
13.3.2	Tout nombre impair $\geq 7$ est la somme d'au plus 3 nombres premiers	189
13.4	CONJECTURE DE WARING	189
13.5	DECOMPOSITION D'UN NOMBRE EN NOMBRES FIGURES	192
13.6	DECOMPOSITION DE CARRES	192
13.6.1	En nombres premiers	192
13.6.2	En nombres triangulaires :	193
13.7	A PROPOS DU GRAND THEOREME DE FERMAT	193
<b>14</b>	<b>DES FAMILLES DE NOMBRES ENTIERS.....</b>	<b>195</b>
14.1	INTRODUCTION	195
14.2	QUELQUES SUITES	195
14.3	LES NOMBRES DE MERSENNE	196
14.3.1	Quelques théorèmes portant sur les nombres de Mersenne	196
14.4	LES NOMBRES DE FERMAT	197
14.5	LES NOMBRES DE CATALAN	199
14.5.1	Historique	199
14.5.2	Définition par récurrence	200
14.5.3	Relation avec les coefficients du binôme	200
14.5.4	Autres relations	201
14.5.5	Valeur asymptotique	201
14.5.6	Triangle de Pascal et nombres de Catalan	201
14.5.7	Applications	202
14.6	NOMBRES SEMI-PREMIERS	202
14.7	NOMBRES PSEUDO-PREMIERS OU NOMBRES DE POULET	202
14.8	LES NOMBRES DE CARMICHAËL	202
14.8.1	Critère ou théorème de Korselt :	203
14.8.2	Autres propriétés :	203
14.9	NOMBRES AMIABLES	204
<b>15</b>	<b>LES EQUATIONS DIOPHANTIENNES DU PREMIER DEGRE .....</b>	<b>206</b>
15.1	DEFINITIONS	206
15.2	RAPPELS	206
15.2.1	Identité ou théorème de Bezout	207
15.2.2	Théorème de Gauss et sa généralisation :	207
15.3	LES FORMES D'EQUATIONS ETUDIEES	207
15.4	L'EQUATION DIOPHANTINNE LINEAIRE $AX + BY = C$	208
15.4.1	Un peu de théorie	208
15.4.2	La méthode d'Euler	208

15.4.3	La méthode générale	209
15.4.4	Interprétation géométrique	210
15.5	SYSTEMES D'EQUATIONS DIOPHANTIENNES LINEAIRES	211
15.6	EXERCICES :	211
15.6.1	L'auberge d'Euler	211
15.6.2	La vente de poulets	212
15.6.3	L'achat de produits frais	213
15.6.4	Les dimensions du rectangle	214
15.6.5	La date d'anniversaire	215
15.6.6	Achat de fruits	216
15.6.7	Achat et vente de bibelots	217
<b>16</b>	<b>LES EQUATIONS DIOPHANTIENNES DE DEGRE 2 ET SUPERIEUR</b>	
	<b>218</b>	
16.1	EQUATION DU SECOND DEGRE $AX^2 + BXY + CY^2 = 0$	218
16.2	L'EQUATION DIOPHANTINNE $AX^2 + BY^2 + CZ^2 = 0$	219
16.3	L'EQUATION DE PELL	220
16.3.1	Analyse du problème	221
16.3.2	Exemple d'application	221
16.3.3	Recherche de la solution minimale	222
16.3.4	Seconde approche	223
16.3.5	Exercices	225
16.3.5.1	L'âge du général	225
16.3.5.2	La bataille de Hastings	226
16.3.6	L'équation $x^2 - ny^2 = m$	226
16.4	EQUATIONS DE DEGRE SUPERIEUR A 2	227
16.4.1	équation diophantienne $x^2 + 3y^2 = z^3$	227
16.4.2	Conjecture de Catalan	227
16.4.3	Théorème de V. A. Lebesgue :	228
16.4.4	Théorème de Ko Chao :	228
16.4.5	Conjecture de Mordell	228
16.5	RESOLUTION DE QUELQUES EQUATIONS PARTICULIERES	228
16.5.1	Equation diophantienne $x^2 + 3y^2 = z^3$	228
16.5.2	Pas de solution pour l'équation $x^4 - 8y^4 = 1$	229
16.5.3	Équation $x^2 - 8y^4 = 1$	229
16.5.4	Équation $x^4 - 2y^2 = 1$	230
16.5.5	Les équations $x^4 - ay^2 = 1$ et $4x^4 - ay^2 = 1$	231
16.5.6	Equation polynomiale	231
16.6	STRATEGIE COMPLEMENTAIRE	232
16.7	POUR APPROFONDIR	232
<b>17</b>	<b>LE GRAND THEOREME DE FERMAT .....</b>	<b>233</b>
17.1	ÉNONCE	233
17.2	REMARQUES A PROPOS DU GRAND THEOREME DE FERMAT	233
17.3	DEMONSTRATION POUR $N=4$	234
17.3.1	Démonstration via les triangles pythagoriciens	234

---

17.3.2	Démonstration via une équation plus générale	234
17.4	DEMONSTRATION POUR $N=3$	235
17.5	LE THEOREME DE SOPHIE GERMAIN	236
17.6	COMMENT POURSUIVRE LA DEMONSTRATION ?	236
<b>18</b>	<b>DIVERS</b> .....	<b>237</b>
18.1	INTRODUCTION	237
18.2	NOMBRES HARMONIQUES	237
18.3	LES NOMBRES PALINDROMES	237
18.4	LES NOMBRES AUTOMORPHES	238
18.5	QUELQUES NOMBRES AYANT DE DROLES DE PROPRIETES	239
18.5.1	Le nombre 145	239
18.5.2	Le nombre 153	239
18.5.3	Les nombres 370, 371 et 407	240
18.5.4	Les nombres 27 et 37	240
18.6	CONCLUSIONS	240
<b>19</b>	<b>EXERCICES DIVERS</b> .....	<b>241</b>
19.1	INTRODUCTION	241
19.2	L'AGE DU CALIFE ET L'AGE DU VIZIR	241
19.3	COMMENT PAYER L'ESSENCE	241
19.4	TROUVER UN ENTIER $N$ $\overline{xxyy}$ TEL QUE $\overline{xxyy}$ SOIT UN CARRE	242
19.5	UN PROBLEME DE LOGIQUE ET DE DIVISIBILITE	243
19.6	LES NOUVEAUX LAPINS DE FIBONACCI	244
<b>20</b>	<b>BIBLIOGRAPHIE</b> .....	<b>247</b>
<b>21</b>	<b>INDEX ALPHABETIQUE</b> .....	<b>249</b>

## Avant propos

L'histoire des mathématiques montre que les mathématiciens avaient déjà trouvé de nombreuses notions sur les nombres, en particulier sur les nombres entiers, bien avant le 18<sup>ème</sup> siècle.

L'arithmétique a passionné les mathématiciens, dont Lagrange, Fermat, etc. Des théories relatives aux carrés magiques, à la suite de Fibonacci, etc. ont été développées, au départ sans espérance d'applications pratiques. Cependant des applications ont ultérieurement été trouvées, par exemple en agriculture.

Alors que les progrès ont été assez rapides, notamment en arithmétique, on constate que les notations ont progressé beaucoup plus lentement comme le montre la liste de dates suivante.

L'arithmétique est la branche des mathématiques qui s'intéresse aux nombres entiers. Cela ne signifie pas qu'elle se limite à ce qu'on enseigne dans l'enseignement primaire et secondaire. Dès que l'on avance un peu dans cette discipline, on a besoin des techniques habituelles des mathématiques : le formalisme, le raisonnement par l'absurde, la récurrence, etc.

L'arithmétique ne dispense pas de l'utilisation du calcul « algébrique », c'est à dire de l'utilisation de lettres pour désigner des variables, de l'écriture d'équations, etc. Par manque de place tous les rappels relatifs au calcul algébrique ne sont pas faits. On rappelle cependant quelques identités remarquables.

Cette discipline est difficile : de nombreuses conjectures ont été énoncées. Pour certaines les démonstrations sont arrivées avec un retard de plusieurs années et pour d'autres nous attendons toujours les démonstrations. Il faut se contenter alors d'une vérification partielle avec un ordinateur.

Les applications sont assez peu nombreuses avec cependant quelques exceptions comme les codes correcteurs d'erreurs et le chiffrement, encore appelée cryptographie. Elle donne lieu, en contrepartie à des problèmes amusants.

On conçoit aisément qu'il y ait une liaison entre l'arithmétique et l'algèbre et cela pour la simple raison que les nombres entiers ne sont qu'un cas particulier des nombres réels. Mais on constate qu'il y a parfois une interprétation géométrique de certains résultats obtenus en arithmétique.

En toute rigueur, il faudrait souvent faire appel aux notions de **corps** et **d'anneau**, notamment pour les entiers gaussiens. Cela a été évité autant que possible afin de ne pas donner une allure trop abstraite à ce livre, quitte à réduire un peu la rigueur mathématique.

Ce livre ne prétend surtout pas être un livre théorique, mais cherche seulement à rassembler divers théorèmes et à montrer des problèmes amusants que l'on peut rencontrer en arithmétique.

Pour faciliter la compréhension, les démonstrations sont faites en utilisant un vocabulaire aussi simple que possible et ne font appel aux notions modernes que lorsque cela est indispensable.

A la fin de ce livre figure une courte bibliographie. Une bibliographie complète aurait comporté de nombreuses pages inutiles pour la majorité des lecteurs. Il faut cependant signaler le site Internet de Serge MEHL qui est très intéressant ainsi que l'encyclopédie en ligne Wikipedia qui contient de très nombreuses informations concernant les mathématiques.

La seconde édition se différencie de la première, par quelques extensions, par l'adjonction de quelques exercices et aussi par un effort d'amélioration de la mise en page.

L'auteur recevra avec plaisir, toute critique constructive qui sera envoyée à l'adresse Internet suivante :

[jean-pierre.lamoitier@gadz.org](mailto:jean-pierre.lamoitier@gadz.org)

## Bref panorama de l'évolution de l'arithmétique :

Quelques dates historiques :

- Vers 1900-1800 avant JC numérotation sexagésimale chez les savants babyloniens
- Vers 2<sup>ème</sup> siècle avant JC première trace de numération positionnelle décimale chez les mathématiciens chinois.
- 4<sup>ème</sup> à 5<sup>ème</sup> siècle après JC Les premiers chiffres indiens vont servir de base à la numérotation décimale.
- 629 Le mathématicien indien Brahmagupta publie un document montrant qu'il manipule la notation décimale au moyen de 9 chiffres décimaux et du zéro.
- 972-982 Lors d'un voyage en Espagne, Gerbert d'AURILLAC (qui deviendra en 999 le pape Sylvestre II), s'initie aux chiffres arabes et les introduit en Europe occidentale.
- 12<sup>ème</sup> siècle Introduction du chiffre zéro en Europe occidentale.
- 1484 Nicolas CHUQUET introduit les nombres négatifs.
- 1489 Johann WIDMANN introduit les signes + et - en remplacement des lettres *p* et *m* pour désigner l'addition et la soustraction.
- 1557 Robert RECORDE introduit le symbole = pour marquer l'égalité.
- 1591 François VIETE introduit une notation littérale : voyelle pour les inconnues, et consonnes pour les constantes indéterminées.
- 1608 Le néerlandais Willebrord SNELLIUS propose d'utiliser la virgule pour séparer la partie entière de la partie décimale.
- 1631 Introduction des symboles d'inégalités < et >.
- 1632 Fermat énonce de nombreuses conjectures et théorèmes.
- 1633 Utilisation de la croix × comme symbole de la multiplication.

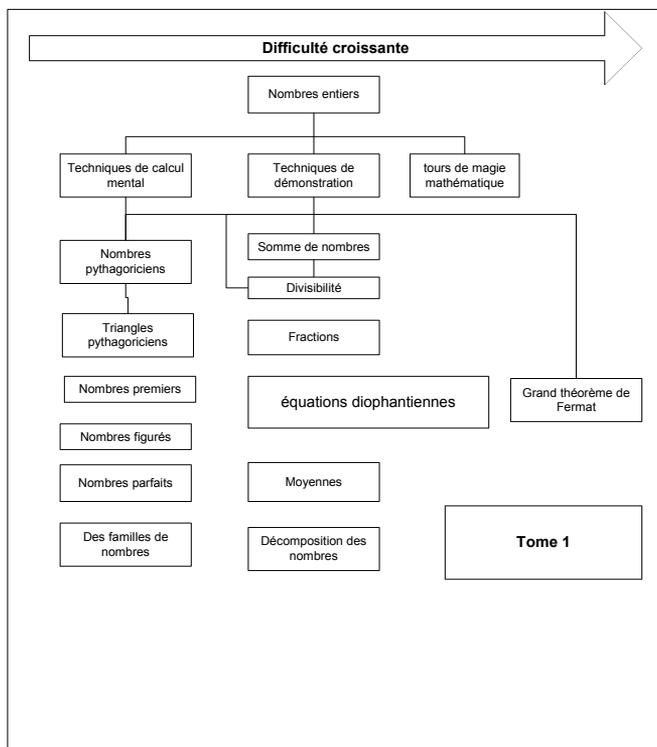
- 1795 Adoption du système métrique.
- 1831 Gauss introduit les entiers complexes appelés entiers de Gauss.
- 1994 Andrew Wiles démontre le grand théorème de Fermat.

## Mathématiciens ayant beaucoup étudié l'arithmétique

Le tableau suivant, bien que très incomplet, montre que les mathématiciens qui se sont intéressés à l'arithmétique sont très nombreux.

Pythagore	vers – 600	Grec
Euclide	–350 --275 ?	Grec
Eratosthène	-276 – 194 ?	Grec
Nicomaque	vers –150 avant JC	
Héron d'Alexandrie	1 <sup>er</sup> siècle	Grec
Diophante d'Alexandrie	vers 300	Grec
Brahmagupta	vers 598-670	Indien
Claude Gaspard BACHET DE MEZIRIAC	1581-1638	Français
Marin MERSENNE	1588-1648	Français
Pierre de FERMAT	1601-1665	Français
John PELL	1611-1685	Anglais
Christian GOLDBACH	1690-1764	Russe
Leonhard EULER	1707-1783	Suisse
Edward WARING	1734-1798	Ecossais
Joseph Louis LAGRANGE	1736-1813	Français
John WILSON	1741-1793	Anglais
André Marie LEGENDRE	1752-1834	Français
Sophie GERMAIN	1776-1831	Française
Karl Friedrich GAUSS	1777-1855	Allemand
Augustin-Louis CAUCHY	1789-1857	Français
Auguste Ferdinand MÖBIUS	1790-1868	Allemand
Pierre Frédéric SARRUS	1798-1861	Français
Niels Henrik ABEL	1802-1829	Norvégien
Charles Gustav JACOBI	1804-1851	Allemand
Peter Gustav DIRICHLET	1805-1859	Allemand
Joseph LIOUVILLE	1808-1882	Français
Ernst KUMMER	1810-1893	Allemand
Evariste GALOIS	1811-1832	Français
Eugène-Charles CATALAN	1814-1894	Français et Belge
Pafnouty TCHEBYCHEV	1821-1894	Russe
Jean-Joseph Louis BERTRAND	1822-1900	Français
Ferdinand EISENSTEIN	1823-1852	Allemand
Edouard LUCAS	1842-1891	Français
François PROTH	1852-1879	Français

Giuseppe PEANO	1858-1932	Italien
Kurt HENSEL	1861-1941	Allemand
Jacques HADAMARD	1865-1963	Français
Charles Jean de la VALLEE POUSSIN	1866-1962	Belge
Joseph WEDDERBURN	1882-1948	Ecossais ayant travaillé aux USA
Viggo BRUN	1882-1978	Norvégien
Maurice KRAITCHIK	1882-1957	Belge d'origine russe
Louis Joseph MORDELL	1892-1972	Anglais
Paul ERDÖS	1913-1996	Hongrois
Andrew WILES	1953	Anglais
Gerd FALTINGS	1954-	Allemand



## Tome 2 : L'arithmétique modulaire et ses applications

Schéma de Lecture montrant les chapitres que l'on peut "sauter"

Ce diagramme montre les différents chapitres avec une appréciation de leur difficulté.



# 1 Les nombres entiers

Les nombres entiers ont été très étudiés par les premiers mathématiciens, dont évidemment les grecs, mais aussi vers la fin du moyen âge. Des propriétés très curieuses ont été trouvées. Quelques astuces facilitent le calcul mental. Pour ces raisons, nous consacrerons plusieurs chapitres à ce sujet.

## 1.1 Notations

Nous appelons  $N$  l'ensemble des nombres entiers positifs.

Nous appelons  $Z$  l'ensemble des « entiers relatifs » c'est à dire négatifs, nuls ou positifs.

$Z(i)$  désigne l'ensemble des entiers de Gauss. Il s'agit de nombres complexes dont les parties réelles et imaginaires sont entières. Dans le tome 2, un chapitre spécial leur est consacré.

Pour l'initiation, l'ensemble  $N$  des entiers naturels suffit. Cependant, pour s'attaquer à des problèmes plus complexes, il faut utiliser les nombres relatifs.

## 1.2 Les bases de numération

Dès l'école maternelle, on apprend aux enfants à compter en base 10, comme si d'autres formes de représentation des nombres n'étaient pas possibles. Or on peut parfaitement compter en base 2, 8, en base 12, 16 ou autre. La base de numération doit être un nombre entier positif  $\geq 2$ .

Les babyloniens utilisaient la base 60. Il en reste des traces avec des heures divisées en 60 minutes qui elles-mêmes sont divisées en 60 secondes. De même la mesure des angles dont le degré est divisé en 60 minutes. Enfin il reste des traces dans l'expression soixante-dix alors que le bon sens aurait voulu que l'on dise septante !

Les Mayas travaillaient avec la base 20. Elle a également été utilisée en Europe. Il en reste quelques traces, par exemple avec l'expression quatre-vingt au lieu d'octante.

La base 16, encore appelée base hexadécimale est maintenant très utilisée en informatique.

La base 12 a certainement une origine religieuse marquée par les douze apôtres, les 12 signes du zodiaque et explique certainement la division du jour en 24 heures : en moyenne 12 heures de jour et 12 heures de nuit. 12 a aussi de nombreux diviseurs : 2, 3, 4 et 6; les chiffres 3 et 4 représentant certaines valeurs symboliques dans les religions et mythologies. Il en reste la vente des œufs ou des huîtres par douzaines.

La base huit, encore appelée base octale a été très utilisée en informatique.

Certaines tribus d'Amérique du Sud ont utilisé les bases 3 et 4.

Dans tout ce livre nous travaillerons en base 10, mais il ne faut pas oublier que la quasi totalité du contenu de ce livre reste bonne si on travaille dans une autre base. Les exceptions sont certaines techniques de calcul mental.

La fin de ce chapitre comporte un paragraphe portant sur les changements de base.

## 1.3 Les opérations de base

Les opérations de base sont évidemment : l'addition, la soustraction, la multiplication et la division. Les additions et soustractions sont des opérations simples qui peuvent assez souvent se faire de tête, alors que les deux autres sont plus difficiles.

D'autres opérations ont été ajoutées par la suite :

- Élévation à la puissance
- Extraction de racines carrées, cubiques, etc.
- Factorielle, primorielle, super et hyperfactorielle, etc.

### 1.3.1 L'addition

L'addition est, de loin, l'opération la plus simple.

#### 1.3.1.1 Quelques propriétés de l'opération d'addition :

L'addition est **commutative** c'est à dire que  $a + b = b + a$

Elle est **associative** : Pour effectuer 2 additions consécutives, l'ordre dans lequel on effectue les additions n'a pas d'importance. Cela s'écrit :

$$(a + b) + c = a + (b + c)$$

### 1.3.1.2 Table d'addition

La table d'addition ci-dessous permet d'additionner 2 entiers positifs inférieurs ou égaux à 13.

+	1	2	3	4	5	6	7	8	9	10	11	12	13
1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	3	4	5	6	7	8	9	10	11	12	13	14	15
3	4	5	6	7	8	9	10	11	12	13	14	15	16
4	5	6	7	8	9	10	11	12	13	14	15	16	17
5	6	7	8	9	10	11	12	13	14	15	16	17	18
6	7	8	9	10	11	12	13	14	15	16	17	18	19
7	8	9	10	11	12	13	14	15	16	17	18	19	20
8	9	10	11	12	13	14	15	16	17	18	19	20	21
9	10	11	12	13	14	15	16	17	18	19	20	21	22
10	11	12	13	14	15	16	17	18	19	20	21	22	23
11	12	13	14	15	16	17	18	19	20	21	22	23	24
12	13	14	15	16	17	18	19	20	21	22	23	24	25
13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figure 1 Table d'addition

### 1.3.2 La soustraction

Cette opération apparaît comme l'opération inverse de l'addition puisque si

$$x = a + b \quad \text{on peut écrire} \quad a = x - b$$

La soustraction n'est pas commutative :  $a - b$  ne donne pas le même résultat que  $b - a$

#### 1.3.2.1 Un tour de magie arithmétique

Voici un petit tour de magie mathématique destiné à montrer ce qu'on peut faire. Le lecteur intéressé pourra lire le chapitre 3 qui est consacré à ce sujet.

André pense à un nombre entier de 3 chiffres, par exemple à 742. Il permute les chiffres de gauche et de droite, ce qui donne, dans l'exemple 247. Il calcule la différence entre les 2 nombres, ici  $742 - 247 = 495$ .

André communique le chiffre de gauche du résultat à Bernard et Bernard trouve les 2 autres chiffres, 9 et 5 dans l'exemple. Comment fait Bernard ?

**Explication** : le nombre d'André, composé de 3 chiffres  $a$ ,  $b$  et  $c$  est tel que  $a$  représente les centaines,  $b$  représente les dizaines et  $c$  les unités. La valeur de ce nombre est donc :

$$x = 100a + 10b + c$$

Après permutation des chiffres de gauche et de droite, on obtient un nombre  $y$  qui vaut :

$$y = 100c + 10b + a$$

Le lecteur peut revoir en fin de ce chapitre un rappel relatif aux identités remarquables

La différence  $x - y$  s'écrit :

$$x - y = 100(a - c) + (c - a)$$

Pour ne pas entrer dans les nombres négatifs, nous supposons que  $a > c$ . Il s'en suit que  $(c - a)$  est négatif et que nous devons écrire :

$$x - y = 100(a - c) - 10 + (10 + c - a)$$

Mais alors le chiffre des dizaines serait négatif. Il faut donc retirer une centaine pour que le chiffre des dizaines devienne 9, ce qui donne :

$$x - y = 100(a - c - 1) + 90 + (10 + c - a)$$

On constate que le chiffre des dizaines est toujours 9.

Le chiffre des unités est égal à  $9 - \text{chiffre des centaines}$  car

$$9 - a + c + 1 = 10 + c - a$$

Quand André annonce le chiffre des centaines, par exemple 4, Bernard peut répondre sans se tromper : les 2 autres chiffres sont 9 et 5 ( $5 = 9 - 4$ ).

### 1.3.3 La multiplication

L'opérateur de multiplication est habituellement noté  $\times$ , mais parfois on utilise le point ou même aucun signe.

### 1.3.3.1 Propriétés de l'opération de multiplication

La multiplication est **commutative** :  $a \times b = b \times a$

Elle est également **associative** :  $(a \times b) \times c = a \times (b \times c)$

Elle est **distributive** par rapport à l'addition, c'est à dire que :

$$a(b+c) = ab + bc$$

Autrement dit, on peut soit d'abord effectuer l'addition  $b + c$  puis on multiplie le résultat par  $a$  ou alors on calcule les produits  $ab$  et  $ac$  et on additionne ensuite les 2 produits.

La multiplication a un **élément neutre** qui est noté 1 car :

$$a \times 1 = a$$

**Remarque** : Avec les nombres entiers, contrairement aux nombres réels, un élément n'est pas **inversible**, c'est à dire que si  $a$  est premier, on ne peut pas trouver un entier  $a'$  tel que :

$$a \times a' = 1$$

nous reviendrons sur ce sujet dans le Tome 2 car l'arithmétique modulaire donne une autre approche de l'inversibilité.

**Terminologie** : quand on multiplie un nombre par lui-même, on dit qu'on l'élève au carré ; si on multiplie un nombre 2 fois par lui-même, on dit qu'on l'élève au cube. Nous reviendrons sur cette terminologie

La table suivante est une table de multiplication de  $13 \times 13$ .

X	1	2	3	4	5	6	7	8	9	10	11	12	13
1	1	2	3	4	5	6	7	8	9	10	11	12	13
2	2	4	6	8	10	12	14	16	18	20	22	24	26
3	3	6	9	12	15	18	21	24	27	30	33	36	39
4	4	8	12	16	20	24	28	32	36	40	44	48	52
5	5	10	15	20	25	30	35	40	45	50	55	60	65
6	6	12	18	24	30	36	42	48	54	60	66	72	78
7	7	14	21	28	35	42	49	56	63	70	77	84	91
8	8	16	24	32	40	48	56	64	72	80	88	96	104
9	9	18	27	36	45	54	63	72	81	90	99	108	117
10	10	20	30	40	50	60	70	80	90	100	110	120	130
11	11	22	33	44	55	66	77	88	99	110	121	132	143
12	12	24	36	48	60	72	84	96	108	120	132	144	156
13	13	26	39	52	65	78	91	104	117	130	143	156	169

Figure 2 : Table de multiplication

Plusieurs méthodes ont été proposées pour réaliser cette opération en minimisant les risques d'erreur, parmi lesquelles, on peut citer :

- La multiplication égyptienne,
- La multiplication à la russe.
- La multiplication italienne,

### 1.3.3.2 La multiplication égyptienne

Les égyptiens utilisaient une méthode particulière pour effectuer les multiplications. Soient 2 nombres  $A$  et  $B$ , par exemple, 29 et 35. On trace 2 colonnes :

Dans la colonne de gauche, on écrira la suite des divisions par 2 de  $A$  (en arrondissant à l'entier inférieur quand le nombre à diviser est impair), jusqu'à ce que l'on atteigne la valeur 1.

Dans la colonne de droite, on écrit le résultat des multiplications successives de  $B$ , ce qui donne le résultat suivant :

Ensuite, on additionne dans la colonne de droite, les nombres dont leur homologue de gauche est impair.

$$\begin{array}{r}
 29 \qquad 35 \\
 \underline{14} \quad \underline{70} \\
 7 \qquad 140 \\
 3 \qquad 280 \\
 \underline{1} \qquad \underline{560} \\
 \hline
 1015
 \end{array}$$

A partir de cette méthode, on peut établir le programme suivant en Basic :

```

REM multiplication égyptienne
DIM t(100)
CLS
debut:
INPUT "Donner les nombres à multiplier"; a, b
IF a = 0 THEN STOP
s = 0
DO WHILE a > .9
  c = INT(a / 2)
  IF 2 * c <> a THEN s = s + b
  a = c
  b = 2 * b
LOOP
PRINT "le produit est"; s
GOTO debut

```

### Exemple d'exécution

```

Donner les nombres à multiplier? 27,35
le produit est 945
Donner les nombres à multiplier? 25,25
le produit est 625
Donner les nombres à multiplier? 12,12
le produit est 144
Donner les nombres à multiplier? 5,8
le produit est 40
Donner les nombres à multiplier? 15,15
le produit est 225
Donner les nombres à multiplier? 13,26
le produit est 338
Donner les nombres à multiplier? 0,2

```

#### 1.3.3.3 Multiplication à la russe

Cette multiplication ne fait appel qu'aux opérations de multiplication et de division par 2 et à l'addition.

**Exemple** : soit à calculer  $A = 517 \times 46$

On peut multiplier par 2 le premier nombre et diviser par 2 le second, ce qui donne :

$$A = 1034 \times 23 = 1034 + 1034 \times 22$$

$$A = 1034 + 2068 \times 11$$

$$A = 1034 + 2068 + 2068 \times 10$$

$$A = 1034 + 2068 + 4136 \times 5$$

$$A = 1034 + 2068 + 4136 + 4136 \times 4$$

$$A = 1034 + 2068 + 4136 + 16544 = 23\ 782$$

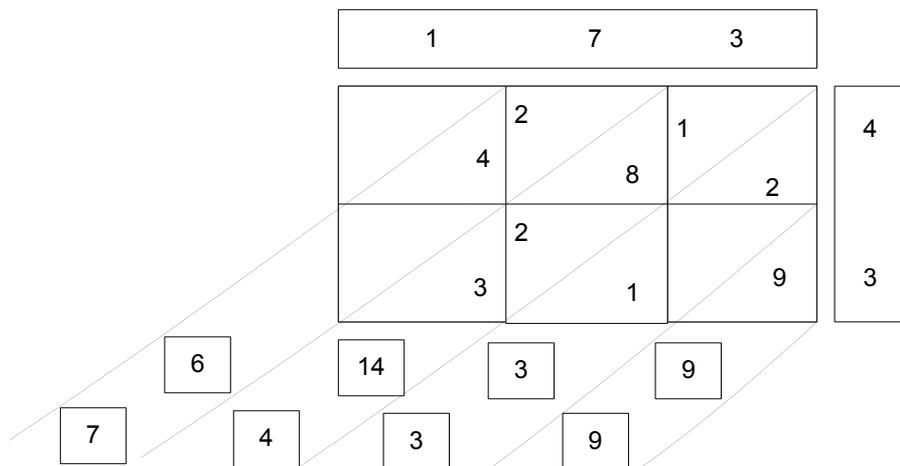
**Remarque** : La multiplication égyptienne et la multiplication à la russe décomposent la multiplication comme on le ferait si on travaillait en base 2.

### 1.3.3.4 La multiplication italienne

Cette méthode, qui vient de l'orient, est apparue en Italie vers le 15<sup>ème</sup> siècle. Elle repose sur l'utilisation d'un rectangle quadrillé et d'obliques comme nous allons le voir sur un exemple.

Soit à multiplier 173 par 43. Nous commençons par dessiner 3 rectangles :

- un rectangle horizontal qui contiendra le multiplicande
- un rectangle vertical qui contiendra le multiplicateur
- un rectangle plus grand qui permettra les multiplications élémentaires



Ensuite, nous traçons les obliques qui permettront de séparer les chiffres de « poids différents ».

Puis nous faisons les multiplication de chiffre par chiffre, mais en séparant bien les résultats. Par exemple le produit des unités, ici  $3 \times 3$ , va dans la partie inférieure du rectangle inférieur de droite.

Le produit  $4 \times 7 = 28$  va donner lieu au chiffre 8 écrit au bas du rectangle et le chiffre 2 (de « poids supérieur ») écrit dans le haut du rectangle.

Lorsque toutes les multiplications élémentaires sont effectuées, nous faisons l'addition des chiffres se trouvant dans la même séparation formée par les obliques et recopions les résultats dans les petits rectangles, En fait nous additionnons des chiffres de même poids. Si un rectangle comporte un nombre à 2 chiffres, cela signifie qu'il y a une « retenue » et nous apportons la correction comme avec une multiplication classique. Cela donne alors la ligne inférieure..

Dans la pratique, on peut cumuler les 2 dernières opérations.

Cette méthode réduit les risques d'erreur, dans la mesure où chaque opération est simple, mais elle est encombrante dès que les nombres deviennent un peu importants.

### 1.3.3.5 Exercice :

Certains nombres de 2 chiffres ont une propriété particulière : leur produit ne change pas si on permute le chiffre des dizaines et celui des unités du multiplicande et du multiplicateur. Par exemple :  $12 \times 42 = 21 \times 24$  . Trouver tous les couples de nombres qui ont cette propriété.

**La solution est simple :** Si nous appelons  $a$  le chiffre des dizaines et  $b$  celui des unités du multiplicande et  $c$  et  $d$  ceux du multiplicateur, la valeur de chaque nombre est

$$10a + b \text{ et } 10c + d \text{ et si on permute } 10b + a \text{ et } 10d + c$$

Leur produit est  $(10a + b)(10c + d)$  doit être égal à  $(10b + a)(10d + c)$ , ce qui donne :

$$100ac + 10ad + 10bc + bd = 100bd + 10bc + 10ad + ac$$

$$99ac = 99bd$$

La condition à satisfaire est donc  $ac = bd$ . Si nous éliminons les solutions triviales, par exemple celles où les chiffres des unités et des dizaines sont égaux, nous obtenons les solutions suivantes :

$12 \times 42$	$14 \times 82$	$24 \times 84$
$12 \times 63$	$23 \times 64$	$36 \times 84$
$12 \times 84$	$23 \times 96$	$39 \times 62$
$13 \times 62$	$24 \times 63$	$46 \times 96$
$13 \times 93$		

Dans cette liste, nous nous sommes limités aux nombres tels que  $a < b$ , mais il est évident que les solutions symétriques existent.

### 1.3.4 La division

Nous appellerons division euclidienne la division entière avec reste.

#### 1.3.4.1 Un peu de terminologie

Nous appelons **division euclidienne**, la division qui donne un quotient entier et un reste qui est inférieur au diviseur

Dans la division  $a = bq + r$  où  $r < b$

$a$  est appelé le dividende,

$b$  est appelé le diviseur,

$q$  est le quotient et

$r$  est le reste qui doit être inférieur au diviseur  $b$ . Ce reste est parfois appelé *résidu*, notamment à propos des *congruences* présentées dans le tome 2.

On dit que  $p$  **divise**  $n$  si la division euclidienne de  $n$  par  $p$  donne un reste nul.

**Notation** : on écrit  $p | n$  pour dire que  $p$  divise  $n$  (avec un reste nul)

La division est **réflexive** : tout entier  $a$  divise lui-même.

**La division n'est pas commutative** :  $a/b$  ne donne pas le même résultat que  $b/a$

Exemple :  $10/2$  donne pour résultat 5 alors que  $2/10$  donne 0,2

**La division est transitive** : si  $a$  divise  $b$  et si  $b$  divise  $c$ , alors  $a$  divise  $c$ .

Elle est **antisymétrique** : si  $a$  divise  $b$  et si  $b$  divise  $a$ , alors  $a = b$ .

**La division avec un diviseur nul n'est pas possible** : elle donne en théorie un résultat infini, mais est en fait la cause d'un grand nombre d'erreurs.

L'exemple suivant montre comment on peut faire un raisonnement apparemment juste qui conduit à un résultat faux.

Nous allons montrer que le nombre  $a$  est égal au nombre  $b$ . Supposons que  $a > b$ , nous pouvons donc écrire :

$$a = b + c, \quad a, b \text{ et } c \text{ étant positifs}$$

Multiplions le tout par  $(a-b)$ , ce qui donne :

$$a(a-b) = (a-b)(b+c)$$

$$a^2 - ab = ab + ac - b^2 - bc \quad \text{ôtons } ac \text{ de chaque côté}$$

$$a^2 - ab - ac = ab - b^2 - bc$$

$$a(a-b-c) = b(a-b-c) \quad \text{divisons tout par } (a-b-c)$$

$$a = b$$

Le résultat  $a = b$  semble avoir été obtenu par un calcul sans faute à ceci près que nous avons divisé par  $(a-b-c)$  qui vaut zéro ! La division était donc impossible.

**Théorème** : Dans une relation  $a + b = c$ , si un entier  $p$  divise 2 termes, alors il divise le 3<sup>ème</sup> terme.

La démonstration est aisée : Par exemple si  $n$  divise  $a$  et  $c$ , nous pouvons écrire :

$$a = np \text{ et } b = nq \text{ donc } c = n(p + q)$$

Le nombre  $c$  est donc divisible à la fois par  $n$  et par  $(p + q)$ .

## 1.4 Le rôle des parenthèses

Si on écrit l'expression :  $a \times b + a \times c$ , dans quel ordre faut-il effectuer les calculs ?

Les règles habituelles sont les suivantes :

- On effectue d'abord les multiplications et divisions,
- On effectue ensuite les additions et soustractions.

Dans l'exemple précédent, cela signifie qu'il faut préalablement calculer les produits  $ab$  et  $cd$  puis effectuer l'addition.

Les parenthèses permettent d'imposer un ordre différent, par exemple :

$a \times (b + a) \times c$  signifie qu'il faut d'abord additionner  $b$  à  $a$  et ensuite effectuer les multiplications.

## 1.5 La notion de parité

Un nombre est dit pair s'il est divisible par 2, c'est à dire si son chiffre des unités est : 0, 2, 4, 6 ou 8. Dans les autres cas, il est dit impair.

Cette parité est utile pour certains raisonnements : la parité est conservée ou changée dans certaines opérations :

Addition :            Pair + Pair donne résultat pair  
                          Impair + Impair donne résultat pair  
                          Pair + Impair donne résultat impair

Multiplication :    Pair  $\times$  Pair = Pair  
                          Pair  $\times$  Impair = Pair  
                          Impair  $\times$  Impair = Impair

Le contrôle de parité permet parfois de détecter une erreur, mais de façon moins sûre que la vieille "preuve par neuf".

## 1.6 La preuve par neuf

Cette preuve permettait souvent de détecter une erreur dans les multiplications et divisions lorsqu'elles étaient faites à la main. Le principe est le suivant :

Dans une multiplication, si le multiplicande ou le multiplicateur est divisible par 9, le résultat doit l'être également. Mais ici on va un peu plus loin :

On calcule les restes d'une éventuelle division par 9, ce qui est très facile : il suffit d'additionner les chiffres du multiplicateur ou du multiplicande.

L'explication détaillée du fonctionnement de cette preuve est donnée dans le chapitre relatif aux congruences dans le tome 2.

**Attention** : si la preuve par 9 indique qu'il y a une erreur de calcul, elle a raison. Mais si elle ne détecte pas les erreurs causées par :

- la permutation de 2 ou plusieurs chiffres dans le résultat,

- un résultat différent d'un multiple de 9 du bon résultat.

Elle reste cependant très pratique quand on ne dispose pas de calculette.

## 1.7 L'élevation à la puissance

L'élevation à la puissance consiste à multiplier un nombre avec lui même, une ou plusieurs fois. Par exemple, pour élever 3 à la puissance 2, on multiplie 3 par 3, ce qui donne 9. Pour élever 4 à la puissance 3, on multiplie 4, 2 fois avec lui même, ce qui donne :  $4 \times 4 \times 4 = 64$ .

On utilise la notation suivante :  $4^3 = 64$

### 1.7.1 Propriétés :

$$a^x \times a^y = a^{x+y}$$

$$(a^x)^y = a^{xy}$$

L'élevation à la puissance fait croître le résultat très rapidement. Pour cette raison, on parle de croissance exponentielle.

$$2^2 = 4 \quad 2^3 = 8 \quad 2^4 = 16 \quad 2^5 = 32 \quad 2^{10} = 1024$$

L'élevation à une puissance négative correspond à l'écriture d'une fraction, par exemple  $a^{-b}$ ,  $b$  étant  $>0$  est égal à  $1/a^b$ .

La racine carrée se note également par la puissance  $1/2$  et la racine cubique par la puissance  $1/3$  :

$$x^{\frac{1}{2}} = \sqrt{x} \quad x^{\frac{1}{3}} = \sqrt[3]{x}$$

L'élevation à une puissance non entière est également possible, mais sort du cadre de ce livre consacré à l'arithmétique.

## 1.8 Extraction de racine carrée

Cette opération est de loin, la plus compliquée. Elle correspond à l'inverse de l'élevation au carré. Elle est présentée dans la chapitre 2.

## 1.9 L'opération factorielle

L'une des caractéristiques des mathématiques est le fait que les mathématiciens n'hésitent pas à créer un opérateur lorsque cela leur semble

utile. C'est le cas notamment de l'opérateur factorielle qui est noté par un point d'exclamation.

Cet opérateur ne porte que sur un seul opérande :

$$2! = 1 \times 2 = 2$$

$$3! = 1 \times 2 \times 3 = 6$$

$$n! = 1 \times 2 \times 3 \times \dots \times (n-1) \times n$$

Cet opérateur est très utile, notamment pour les calculs en combinatoire. On constate que les factorielles croissent très vite :

$$4! = 24 \quad 5! = 120 \quad 6! = 720 \quad 7! = 5\,040$$

$$8! = 40\,320 \quad 9! = 362\,880$$

**Remarque** : la fonction factorielle se généralise en analyse sous le nom de « fonction gamma » notée  $\Gamma$ .

### 1.9.1 La primorielle

La primorielle ressemble à la factorielle à ceci près qu'on ne multiplie que les nombres premiers. On notera  $p\#$  le produit des nombres premiers de 2 à  $p$  inclus (si  $p$  est premier).

$$\text{Exemples : } 3\# = 6 \quad 5\# = 30 \quad 7\# = 210, \quad 11\# = 2310, \text{ etc.}$$

Les primorielles n'ont pas donné lieu à des développements intéressants surtout d'un point de vue pratique.

Les mathématiciens ont imaginé :

- des multifactorielles : on prend un nombre sur 2 ou sur 3, etc.
- double factorielle :  $6!! = 2 \times 4 \times 6$
- des hyperfactorielles notées  $H(n) = 1 \times 2^2 \times 3^3 \times 4^4 \dots n^n$
- des superfactorielles notée  $sf(n) = 1^n \times 2^{n-1} \times 3^{n-2} \times \dots \times (n-1)^2 \times n$
- des sous-factorielles notée  $!n = n! \Sigma(-1)^k / k!$

Les sous-factorielles sont reliées à la fonction Gamma, mais l'intérêt des autres notions est discutable.

## 1.10 Relation d'ordre

Un nombre entier  $a$  peut être plus petit, plus grand ou égal à un autre nombre  $b$ . Nous noterons :

$a < b$  pour dire que  $a$  est plus petit que  $b$

$a \leq b$  pour dire que  $a$  est plus petit ou égal à  $b$

$a = b$  signifie que  $a$  est égal à  $b$

$a > b$  indique que  $a$  est plus grand que  $b$

$a \geq b$  indique que  $a$  est plus grand ou égal à  $b$

Le symbole  $\neq$  est l'opposé du symbole  $=$ . Il signifie différent.

Cette relation d'ordre est **transitive** c'est à dire que si :

$$a < b \text{ et } b < c, \text{ alors } a < c$$

## 1.11 La notion de moyenne

Habituellement, nous considérons que la moyenne de 2 nombres  $a$  et  $b$  est donnée par :

$$m = (a + b)/2$$

Cette moyenne est la **moyenne arithmétique**. Il existe 2 autres moyennes :

La moyenne géométrique est donnée par

$$m = \sqrt{(a + b)}$$

La moyenne harmonique  $h$  est donnée par :

$$2/h = 1/a + 1/b$$

Il ne faut pas croire que les mathématiciens ont inventé ces notions pour le plaisir. Elles sont utiles. Par exemple, en électricité la résistance équivalente de 2 résistances montée en parallèle est égale à la moitié de la moyenne harmonique des 2 résistances.

$$1/R = 1/R_1 + 1/R_2$$

## 1.12 Les changements de base

**Rappel** : quand nous écrivons en base 10, par exemple, le nombre 2345, tout se passe comme si nous écrivions :

$$2 \times 10^3 + 3 \times 10^2 + 4 \times 10 + 5$$

En base 8, nous disposerons uniquement des chiffres de 0 à 7. 10 ne représentera plus une dizaine, mais une « octaine »

Le nombre 2345 écrit en base 8 signifie

$$2 \times 8^3 + 3 \times 8^2 + 4 \times 8 + 5 = 1253 \text{ en base } 10$$

Le passage d'une représentation en base 10 en représentation dans une autre base et inversement n'est pas une opération difficile, mais il faut faire attention : une petite erreur est vite arrivée !

Si nous voulons représenter un nombre en base 16, les 10 chiffres habituels ne suffisent pas et nous devons ajouter 6 chiffres supplémentaires. Par convention, nous représenterons par *A, B, C, D, E* et *F* les chiffres 10, 11, 12, 13, 14 et 15

Le nombre *1A* signifie, en base 10 :  $16 + 10 = 26$

Le nombre *7AF* signifie en base 10 :  $15 + 160 + 7 \times 256 = 1967$

### Procédé de changement de base :

Plusieurs méthodes sont possibles. Nous présentons ici la méthode qui semble la plus naturelle.

**Passage de la base *n* à la base 10.** C'est le cas le plus simple :

Si le nombre en base *n* s'écrit  $\overline{abcde}$  : il suffit de faire le calcul :

$$e + d \times n + c \times n^2 + b \times n^3 + a \times n^4$$

Ce calcul peut être réalisé plus rapidement sous la forme

$$(((an + b)n + c)n + d)n + e$$

Exemple : convertir *3 456 543* de la base 8 en base 10

$$((((((3 \times 8 + 4) \times 8 + 5) \times 8) + 6) \times 8 + 5) \times 8 + 4) \times 8 + 3 = 941\,411$$

**Passage de la base 10 à la base *n*** : le calcul est un peu plus compliqué.

Supposons que le nombre s'écrive  $\overline{abcdef}$  en base 10. Nous allons opérer des divisions euclidiennes par  $n$  pour et noter les différents restes.

La première division donne un reste qui sera le chiffre des unités. Nous diviserons le quotient obtenu par  $n$  et le reste sera le chiffre qui ira immédiatement à droite. Nous continuons de la sorte jusqu'à ce que la division ne soit plus possible. Alors le dernier quotient est le chiffre le plus à gauche.

Exemple 1 : reprenons le nombre précédent :  $941\ 411$

$$941\ 411 = 8 \times 117676 + 3 \quad 3 \text{ sera le chiffre des unités}$$

$$117676 = 8 \times 14709 + 4 \quad 4 \text{ sera le chiffre suivant}$$

$$14709 = 8 \times 1838 + 5 \quad 5$$

$$1838 = 8 \times 229 + 6$$

$$229 = 8 \times 28 + 5$$

$$28 = 8 \times 3 + 4 \quad 4 \text{ est retenu mais aussi le quotient } 3 \text{ qui est}$$

sera le chiffre de poids le plus élevé.

Nous retrouvons donc notre nombre  $3456543$

Exemple 2 : soit à convertir le même nombre  $941411$  en base 16. Le processus est le même à ceci près qu'il faudra utiliser les lettres  $A, B, C, D, E$  et  $F$  comme des chiffres représentant respectivement les chiffres  $10, 11, 12, 13, 14$  et  $15$  de la base  $16$ .

Nous obtenons :

$$941411 = 16 \times 58838 + 3 \quad 3 \text{ sera le chiffre des unités}$$

$$58838 = 16 \times 3677 + 6 \quad 6 \text{ sera le chiffre immédiatement à gauche}$$

$$3677 = 16 \times 229 + 13 \quad 13 \text{ donnera le chiffre } D$$

$$229 = 16 \times 14 + 5 \quad 5 \text{ sera le chiffre suivant à gauche et le}$$

quotient  $14$  donne le chiffre  $E$  tout à gauche.

Le nombre en base  $16$  est donc  $E5D63$

D'un strict point de vue théorique, les calculs se font de la même manière quelle que soit la base utilisée. Dans la pratique quand on est habitué à travailler en base  $10$ , les calculs dans une autre base sont pénibles.

## 1.13 Exercices

**Exercice 1 :** Dans un document, on trouve l'écriture suivante :  $9 \times 8 = 48$ . Comment expliquer un tel résultat ?

**Réponse :** Si le résultat est juste, il s'explique par le fait que les auteurs travaillent dans une autre base. Soit  $b$  cette base. Nous devons avoir :

$$4b + 8 = 72 \text{ ce qui donne } b = 16$$

L'auteur a donc calculé en base 16.

**Exercice 2 :** trouver la base dans laquelle est écrit le nombre 999 sachant que sa valeur en base 10 est 2457.

**Réponse :** Soit  $b$  la base. Nous pouvons écrire :

$$9(b^2 + b + 1) = 2457 \text{ soit } b^2 + b + 1 = 273 \quad b(b+1) = 272 = 16 \times 17$$

999 est donc écrit en base 16.

## 1.14 Rappels : Les identités et inégalités remarquables

Les identités qualifiées de remarquables sont d'une très grande utilité pour le calcul algébrique qui est évidemment utilisé en arithmétique. Voici les principales identités :

**Identités du second degré :**

$$(a + b)^2 = a^2 + 2ab + b^2$$

$$(a - b)^2 = a^2 - 2ab + b^2$$

$$a^2 - b^2 = (a + b)(a - b)$$

**Identités du 3<sup>ème</sup> degré :**

$$(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

$$(a - b)^3 = a^3 - 3a^2b + 3ab^2 - b^3$$

$$a^3 - b^3 = (a - b)(a^2 + ab + b^2)$$

$$a^3 + b^3 = (a + b)(a^2 - ab + b^2)$$

**Identités de degré  $n$  :**

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + b^{n-1})$$

$$(a + b)^n = a^n + na^{n-1} + \frac{n(n-1)}{2}a^{n-2} + \dots + b^n$$

développement avec les « coefficients du binôme »

$$(a - b)^n = a^n - na^{n-1} + \frac{n(n-1)}{2}a^{n-2} + \dots + (-1)^nb^n$$

**Identité de Diophante, ou de Legendre (ou de Fibonacci)<sup>1</sup> :**

$$(a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2$$

**Identité de Brahmagupta**

$$(a^2 - nb^2)(c^2 - nd^2) = (ac + nbd)^2 - n(ad + bc)^2$$

**L'inégalité de Young**

La forme simplifiée de cette inégalité est :

$$ab \leq \frac{a^2}{2} + \frac{b^2}{2}, \quad a \text{ et } b \text{ étant des nombres réels}$$

**Démonstration** : on peut supposer que  $a < b$ , ce qui conduit à poser  $b = a + h$

Multiplions tout par 2. Nous pouvons écrire :

$$2a(a + h) \leq a^2 + (a + h)^2 = 2a^2 + 2ah + h^2$$

Il y a égalité seulement lorsque  $a = b$

La forme générale de l'inégalité d'Young est :

$$ab \leq \frac{a^p}{p} + \frac{b^q}{q}$$

Cette inégalité est utilisée pour diverses démonstrations.

---

<sup>1</sup> Il semble que Diophante d'Alexandrie soit le premier à l'avoir trouvée.