

## Table des matières

---

Introduction	15	2.2.2. Preuve	46
1. Brève histoire des débuts de l'Arithmétique	21	2.2.3. Combien d'étapes dans l'algorithme d'Euclide $\zeta$	47
1.1. Systèmes de numération écrite	21	2.2.4. Coût d'une factorisation	48
1.1.1. Égypte	22	2.2.5. Coût de calcul du PGCD	49
1.1.2. Mésopotamie	24	2.2.6. L'algorithme de Pollard	49
1.1.3. Grèce et Rome	25	2.3. Somme des diviseurs	50
1.1.4. Chine	26	2.4. Les nombres parfaits	52
1.1.5. La numération de position	27	2.5. Les nombres de Mersenne	52
1.1.6. Petite chronologie	28	2.5.1. Définition et théorèmes	52
1.2. Calculer : les bases	29	2.5.2. Test de Lucas-Lehmer	54
1.3. Multiplier	31	2.6. Codage affine	57
1.3.1. La multiplication arabe	31	3. Encore Fermat, Euler, Legendre, Gauss	59
1.3.2. La multiplication chinoise	31	3.1. Problèmes de divisibilité	61
1.3.3. Multiplier automatiquement	33	3.1.1. Le « petit » Théorème de Fermat	61
1.4. Diviser	34	3.1.2. Le Lemme de Hensel	65
1.4.1. La méthode égyptienne	35	3.1.3. Théorème des restes chinois	65
1.4.2. Une méthode de Fermat	36	3.1.4. Nombres pseudo-premiers	66
1.4.3. Une méthode d'Euler	37	3.2. L'indicatrice d'Euler	68
1.5. L'Arithmétique théorique antique	38	3.2.1. Définition	69
1.5.1. Euclide	38	3.2.2. Sommes	70
1.5.2. Archimède	39	3.2.3. Une autre écriture de $\varphi$	71
1.5.3. Diophante	39	3.2.4. Deux conjectures	72
2. Bachet et Fermat	41	3.3. Corps quadratiques	73
2.1. Quelques bases	42	3.3.1. Corps de nombres algébriques	73
2.1.1. L'algorithme d'Euclide	42	3.3.2. Entiers algébriques	74
2.1.2. Congruences	42	3.3.3. Unités	75
2.1.3. Théorèmes	45	3.3.4. Les unités de $\mathbb{Z}(\sqrt{2})$	76
2.2. Le Théorème de Bachet-Bézout	45	3.3.5. Nombres premiers	77
2.2.1. Calculs	46		

3.3.6. L'algorithme d'Euclide	78	5.3. La loi de réciprocité quadratique	113
3.4. L'hypothèse H	80	5.3.1. Théorème	113
3.4.1. Les polynômes d'Euler	80	5.3.2. Quelques exemples	115
3.4.2. L'hypothèse H de Arthur Schinzel	82	5.3.3. Les symboles de Jacobi et Kronecker	116
3.4.3. La conjecture de Bateman-Horn	84	5.4. Les sommes de Gauss	117
4. Dirichlet et les fonctions arithmétiques	89	5.4.1. Caractère et conducteur	117
4.1. Dirichlet	89	5.4.2. Réciprocité quadratique : 2 <sup>e</sup> démonstration	117
4.2. Fonctions arithmétiques	90	6. Le théorème de Wilson et ses conséquences	121
4.2.1. Une fonction vraiment très simple...	90	6.1. L'épuisette et les poissons	121
4.2.2. Phi et mu sont dans un bateau	90	6.2. Démonstrations	122
4.2.3. Définitions	91	6.2.1. Étape 1 : Si $(p-1)!+1 \equiv 0[p]$ alors $p$ premier.	122
4.2.4. Quelques propriétés	91	6.2.2. Étape 2 : Si $p$ est premier alors $(p-1)!+1 \equiv 0[p]$ .	122
4.2.5. Convolution	92	6.2.3. Généralisation de Gauss	123
4.2.6. Convolution des fonctions arithmétiques	94	6.3. Racines primitives modulo $p$	124
4.2.7. Opérateurs, sommes et composition	95	6.3.1. Vraiment primitives ces racines...	124
4.2.8. Fonction génératrice	97	6.3.2. Exposants	126
4.3. Quelques estimations	99	6.3.3. Combien de racines primitives ?	128
4.3.1. Identité d'Abel et formule sommatoire d'Euler	99	6.3.4. Une mise à l'index	129
4.3.2. Des exemples	100	6.3.5. Quelques propriétés des indices	130
4.3.3. La valeur moyenne de $\sigma_0(n)$	101	6.4. Des codes basés sur le logarithme discret ou la factorisation	132
4.3.4. La valeur moyenne de $\sigma_k(n)$	104	6.4.1. Le codage Diffie-Hellman	132
4.3.5. La valeur moyenne de $\varphi(n)$	104	6.4.2. Le codage El Gamal	132
4.3.6. Sommes partielles du produit de convolution	105	6.4.3. Le codage RSA	133
4.4. Produits eulériens	106	6.5. Divisions	134
4.4.1. Convergences	106	6.5.1. Représentation décimale d'un nombre	134
4.4.2. Quelques exemples	107	6.5.2. Calcul de périodes	135
5. La loi de réciprocité quadratique	109	6.5.3. Permutations et sommes	136
5.1. Les corps $\mathbb{F}_p$	109	7. Fractions continues	139
5.2. Les résidus quadratiques	110	7.1. Théorème de Liouville	139
5.2.1. Définition et critère d'Euler	110		
5.2.2. Le symbole de Legendre	111		
5.2.3. Lemme de Gauss	112		

7.1.1. Définition et théorème	139	7.8. L'équation de Pell-Fermat	170
7.1.2. Preuve	140	7.8.1. Résolution par les fractions continues	171
7.1.3. Mesure de rationalité	142	7.8.2. Solutions modulo un nombre premier	173
7.2. Définitions et propriétés	143	7.9. Les fonctions $L$ de Dirichlet	174
7.2.1. Développement d'un nombre	143	7.10. Fractions continues générales	175
7.2.2. A quoi ça sert $\zeta$	144	7.10.1. Séries	176
7.2.3. Définition par récurrence	145	7.10.2. Quelques exemples	176
7.2.4. Fractions continues régulières	146	7.10.3. Avec des séries entières	177
7.3. Théorèmes sur l'approximation	147	7.10.4. Conclusion	178
7.3.1. Approcher un nombre	147	<b>8. Les suites de Farey</b>	<b>181</b>
7.3.2. Convergence et divergence	147	8.1. Fractions consécutives	181
7.3.3. Meilleures approximations	149	8.2. Propriétés basiques	182
7.3.4. Fractions intermédiaires	149	8.3. Cercles de Ford	184
7.3.5. Autres théorèmes sur l'approximation	150	8.4. Arbre de Stern-Brocot et approximations	185
7.3.6. Les théorèmes de Thue et Roth	151	8.5. Suites de Farey et Hypothèse de Riemann	187
7.3.7. Quelques exemples de fractions continues	152	8.6. Minkowski et la géométrie des nombres	193
7.4. Étude de certaines fractions	153	8.6.1. Réseau	193
7.4.1. Convergence	153	8.6.2. Le théorème de Minkowski	195
7.4.2. Quelques exemples simples	154	8.6.3. Distribution des points visibles depuis l'origine	195
7.4.3. Une relation importante	155	8.6.4. Application à l'approximation d'un réel	195
7.5. Racines carrées	156	8.6.5. Somme de deux et quatre carrés	196
7.5.1. Fractions continues périodiques	156	8.6.6. Théorème de Pick	197
7.5.2. Exemples et propriétés	157	<b>9. Fonctions d'une variable complexe</b>	<b>201</b>
7.5.3. Longueur de période	159	9.1. Introduction	201
7.5.4. Un développement indien	160	9.2. Fonctions holomorphes	203
7.5.5. Passage aux matrices	161	9.2.1. Rappels	203
7.6. Mesure et probabilités	162	9.2.2. Fonctions analytiques	204
7.6.1. Où sont les coefficients $\zeta$	162	9.2.3. Chemins	205
7.6.2. Une interprétation probabiliste	164	9.2.4. Indice d'un chemin	206
7.6.3. Accroissement des dénominateurs des réduites	166	9.2.5. Formule de Cauchy	207
7.7. Le problème de Gauss et le théorème de Kuz'min	167	9.2.6. Séries de Laurent	210
7.7.1. Le théorème de Kuz'min	168	9.2.7. Représentation par des intégrales	212
7.7.2. La constante de Khinchin	169		

9.2.8. Pôles et fonctions méromorphes	213	10.3.4. La fonction <i>Digamma</i> : dérivée logarithmique de <i>Gamma</i>	253
9.2.9. Résidus	214	10.4. La formule de Stirling	254
9.3. Calcul d'intégrales immondes	215	10.4.1. Le lemme de Watson	254
9.3.1. Trois exemples	215	10.4.2. Représentation asymptotique de <i>Gamma</i>	255
9.3.2. Le lemme de Jordan	217	11. La fonction <i>Zêta</i>	257
9.4. Transformations conformes	218	11.1. Nicole Oresme	257
9.4.1. Une fonction holomorphe est une application conforme	218	11.2. Des séries extraites de la série harmonique	258
9.4.2. L'inverse local	219	11.3. Leonhard Euler et la fonction <i>Zêta</i>	260
9.4.3. La fonction homographique ou fonction de Möbius	220	11.3.1. Retour vers le sinus	260
9.4.4. Transformations et géométrie de Poincaré	222	11.3.2. The Golden Key	261
9.4.5. Géométrie de Poincaré	223	11.4. Premières approches	262
9.4.6. Transformations du cercle	226	11.4.1. Les nombres de Bernoulli	262
9.4.7. Conclusion	228	11.4.2. La relation d'Euler	266
9.5. Séries et produits de fonctions	229	11.5. Définir <i>Zêta</i> partout (ou presque)	268
9.5.1. Le prolongement analytique	229	11.5.1. Trouver une formule pour <i>Zêta</i> « valide pour tout $s$ »	268
9.5.2. Principe du maximum	231	11.5.2. L'équation fonctionnelle	270
9.6. Sinus comme produit infini	233	11.5.3. L'équation fonctionnelle, version 2	271
9.6.1. Le problème de Bâle	233	11.6. Pourquoi tant de zéros ?	272
9.6.2. Convergence et résultats	234	11.6.2. Une estimation extraordinaire	274
9.6.3. Produits infinis	237	11.6.3. Le produit infini	275
9.6.4. Les produits de Weierstrass	237	11.6.4. La formule de Riemann – von Mangoldt	277
9.6.5. Ordre d'une fonction	239	11.6.5. La fonction de Riemann - Siegel	280
10. La fonction <i>Gamma</i>	243	11.7. Et si c'était vrai ?	282
10.1. Les débuts d'une star	243	12. Le Théorème des Nombres Premiers	285
10.2. Le point de vue réel	244	12.1. Le 19 <sup>e</sup> siècle	285
10.2.1. Définitions	244	12.1.1. Le crible d'Erathostène et Legendre	286
10.2.2. Propriétés de base	245	12.1.2. Leonhard Euler et les nombres premiers	288
10.2.3. Réduction des fonctions <i>Bêta</i> aux fonctions <i>Gamma</i>	246	12.1.3. Carl-Friedrich Gauss	289
10.2.4. Intégrale de Gauss	246		
10.2.5. Intégrales de Fresnel	247		
10.3. Le point de vue complexe	248		
10.3.1. Fonctions <i>Gamma</i> et <i>Bêta</i> dans le demi-plan $\text{Re}(z) > 0$	248		
10.3.2. Prolongement analytique	250		
10.3.3. Le produit infini de <i>Gamma</i>	250		

12.1.4. Un travail important de Tchebychev	291	13.5.3. Division en trois arcs égaux	325
12.1.5. Jacques Hadamard et Charles-Jean de la Vallée Poussin	293	13.5.4. Une intervention d'Euler	327
12.2. Les théorèmes de Franz Mertens	293	13.6. Longueurs	327
12.2.1. Un premier théorème	293	13.6.1. Les vraies périodes du pendule	328
12.2.2. Un deuxième théorème	295	13.6.2. Première définition des fonctions elliptiques	330
12.2.3. Jamais deux sans trois	297	13.6.3. Une représentation géométrique	331
12.3. Une démonstration du TNP	299	13.6.4. Les calculs	334
12.3.1. Une écriture équivalente du TNP	299	13.6.5. La moyenne arithmético-géométrique	335
12.3.2. Zêta ne s'annule pas sur $\text{Re}(s)=1$ , ni même dans ses environs	301	13.6.6. La moyenne arithmético-géométrique : application à la Lemniscate	337
12.3.3. Démonstration du théorème d'Hadamard par la méthode de Landau	302	13.6.7. Une application étonnante : promenade aléatoire sur un réseau	338
12.4. Une approche « élémentaire » du TNP	304	13.7. Quelques propriétés générales	340
12.4.1. Une deuxième écriture équivalente du TNP	304	13.7.1. Géométrie d'une intégrale	340
12.4.2. Preuve : étape 1	305	13.7.2. Pôles et zéros d'une fonction elliptique	341
12.4.3. Preuve : étape 2	306	13.8. Retour à la fonction $\wp$	344
12.4.4. Une dernière équivalence du TNP	308	13.8.1. Paramétrisation d'une cubique	344
12.4.5. Un exemple d'utilisation	308	13.8.2. Séries d'Eisenstein	345
<b>13. Fonctions elliptiques</b>	<b>311</b>	13.9. Trois vieilles histoires	346
13.1. Quelques personnages...	311	13.9.1. Un problème de Diophante sur les équations de degré 2	346
13.2. Sinus et cotangente	313	13.9.2. Les nombres congruents	347
13.2.2. Quelques remarques supplémentaires	315	13.9.3. Un problème presque résolu par É. Lucas	349
13.3. Des développements plus « complexes »	315	13.9.4. L'équation de Bachet-Mordell	350
13.3.1. La fonction $\sigma$	315	13.10. L'addition sur une cubique	352
13.3.2. La fonction $\zeta$	316	13.10.1. Loi de groupe	352
13.3.3. La fonction $\wp$	317	13.10.2. Cryptographie avec une courbe elliptique	354
13.4. Des questions historiques	320	13.10.3. Factorisation par l'algorithme de Lenstra	356
13.5. Un premier point de vue : Giulio Fagnano	323	13.10.4. Aperçu de quelques développements	359
13.5.1. La lemniscate de Bernoulli	323		
13.5.2. Division en deux arcs égaux	324		

<b>14. Les fonctions <i>thêta</i> de Jacobi</b>	<b>365</b>	15.3.4. Les séries d'Eisenstein	400
14.1. Prolégomènes	365	15.3.5. Développement de l'invariant modulaire $j$	402
14.1.1. Définitions	365	15.4. L'espace des formes modulaires	403
14.1.2. Relations	367	15.4.1. Dimensions	403
14.1.3. Les zéros des fonctions $\theta$	368	15.4.2. La fonction <i>êta</i> de Dedekind	405
14.2. Relations algébriques	370	15.4.3. La fonction <i>tau</i> de Ramanujan	407
14.2.1. Quelques relations entre les carrés des fonctions $\theta$	370	<b>16. Partitio numerorum</b>	<b>411</b>
14.2.2. Formules d'addition	371	16.1. Quelques anciennes idées	411
14.2.3. Produits infinis	373	16.2. Partitions d'un entier	413
14.3. Dérivées	374	16.2.1. Fonctions génératrices	413
14.3.1. Équation de la chaleur	374	16.2.2. Euler et les nombres pentagonaux	415
14.3.2. Produits infinis, 2 <sup>e</sup> époque	376	16.3. La formule du triple produit de Jacobi	417
14.4. Fonctions <i>thêta</i> et fonctions elliptiques	378	16.4. Les relations de Rogers & Ramanujan	418
14.4.1. Connexion avec les fonctions de Jacobi	378	16.4.1. Des formules d'Euler	418
14.4.2. Connexion avec les fonctions $\sigma$ de Weierstrass	379	16.4.2. Naissance d'un génie	420
14.4.3. Connexions avec la fonction $\wp$ de Weierstrass	381	16.5. La fraction continue de Ramanujan	425
14.4.4. Valeurs des fonctions $\theta$ pour $z = 1/2$	383	16.6. La méthode du cercle	427
14.5. Transformations	383	16.6.1. Un peu d'analyse complexe	427
14.5.1. Transformation de Jacobi algébrique	384	16.7. Preuves et conjectures	429
14.5.2. Transformation de Jacobi par Poisson et Fourier	385	16.7.1. Le problème de Waring	429
14.5.3. L'identité de Landsberg & Schaar	387	16.7.2. L'exposant $k = 1$	431
<b>15. Formes modulaires</b>	<b>389</b>	16.7.3. Somme de deux carrés	432
15.1. L'équation modulaire	390	16.8. La conjecture de Goldbach	434
15.2. Idées algébriques et bases	391	16.8.2. Mise en route	435
15.2.1. Le groupe modulaire	391	16.8.3. Valeur moyenne de $ f_N(\theta) ^2$	438
15.2.2. Fonctions modulaires	394	16.8.4. Grandes valeurs de $f_N(\theta)$	438
15.2.3. Fonctions de réseau	395	16.8.5. Grands et petits arcs	439
15.3. Quelques formes modulaires	396	16.8.6. Série singulière	440
15.3.1. Avec les fonctions <i>thêta</i>	396	16.8.7. Arcs mineurs	441
15.3.2. Le discriminant de $\wp$ et l'invariant modulaire	397	<b>17. Formes quadratiques</b>	<b>443</b>
15.3.3. Solution de l'équation modulaire	398	17.1. Équivalences	444

17.1.1. Formes quadratiques binaires	444	17.2.1. Caractères	452
17.1.2. Formes quadratiques positives	445	17.2.2. Encore une équation fonctionnelle	454
17.1.3. Le nombre de classes est fini	445	17.2.3. Cent et quelques années plus tard...	456
17.1.4. Un algorithme de calcul	446	Abréviations et Symboles	461
17.1.5. Minimum des formes	447	Bibliographie	463
17.1.6. Formes réduites	448	Index	471
17.1.7. Représentations des entiers	449		
17.1.8. Nombre de représentations des entiers	450		
17.2. Formule analytique du nombre de classes	452		