Sums of Squares of Integers

Carlos J. Moreno
Samuel S. Wagstaff, Jr.
Contents

1 Introduction
1.1 Prerequisites ........................................ 1
1.2 Outline of the Rest of the Book .......................... 2
1.2.1 Chapter 2 ........................................ 2
1.2.2 Chapter 3 ........................................ 3
1.2.3 Chapter 4 ........................................ 4
1.2.4 Chapter 5 ........................................ 5
1.2.5 Chapter 6 ........................................ 7
1.2.6 Chapter 7 ........................................ 8
1.2.7 Chapter 8 ........................................ 9

2 Elementary Methods ........................................ 11
2.1 Introduction .......................................... 11
2.2 Some Lemmas ......................................... 13
2.3 Two Fundamental Identities ............................ 14
2.4 Euler's Recurrence for $a(n)$ .......................... 18
2.5 More Identities ....................................... 23
2.6 Sums of Two Squares .................................. 26
2.7 Sums of Four Squares .................................. 29
2.8 Still More Identities .................................. 34
2.9 Sums of Three Squares ................................ 38
2.10 An Alternate Method .................................. 43
2.11 Sums of Polygonal Numbers ......................... 54
2.12 Exercises ........................................... 57

3 Bernoulli Numbers .......................................... 61
3.1 Overview ............................................ 61
3.2 Definition of the Bernoulli Numbers .................. 62
3.3 The Euler-MacLaurin Sum Formula ..................... 65
3.4 The Riemann Zeta Function ............................ 73
3.4.1 Functional Equation for the Zeta Function ...... 77
3.4.2 Functional Equation for the Dirichlet $L$-functions 83
3.4.3 Generalized Bernoulli Numbers ................... 89
3.5 Signs of Bernoulli Numbers Alternate ................ 90
3.6 The von Staudt-Clausen Theorem .................... 92
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7 Congruences of Voronoi and Kummer</td>
<td>95</td>
</tr>
<tr>
<td>3.8 Irregular Primes</td>
<td>103</td>
</tr>
<tr>
<td>3.9 Fractional Parts of Bernoulli Numbers</td>
<td>107</td>
</tr>
<tr>
<td>3.10 Exercises</td>
<td>113</td>
</tr>
<tr>
<td>4 Examples of Modular Forms</td>
<td>117</td>
</tr>
<tr>
<td>4.1 Introduction</td>
<td>117</td>
</tr>
<tr>
<td>4.2 An Example of Jacobi and Smith</td>
<td>118</td>
</tr>
<tr>
<td>4.3 An Example of Ramanujan and Mordell</td>
<td>129</td>
</tr>
<tr>
<td>4.4 An Example of Wilton: $\tau(n)$ Modulo 23</td>
<td>139</td>
</tr>
<tr>
<td>4.4.1 Factorization in Nonnormal Extensions of $\mathbb{Q}$</td>
<td>145</td>
</tr>
<tr>
<td>4.4.2 Table for the Computation of Frobeniuses</td>
<td>147</td>
</tr>
<tr>
<td>4.5 An Example of Hamburger</td>
<td>148</td>
</tr>
<tr>
<td>4.6 Exercises</td>
<td>153</td>
</tr>
<tr>
<td>5 Hecke’s Theory of Modular Forms</td>
<td>157</td>
</tr>
<tr>
<td>5.1 Introduction</td>
<td>157</td>
</tr>
<tr>
<td>5.2 Modular Group $\Gamma$ and Its Subgroup $\Gamma_0(N)$</td>
<td>158</td>
</tr>
<tr>
<td>5.3 Fundamental Domains for $\Gamma$ and $\Gamma_0(N)$</td>
<td>160</td>
</tr>
<tr>
<td>5.4 Integral Modular Forms</td>
<td>161</td>
</tr>
<tr>
<td>5.5 Modular Forms of Type $M_k(\Gamma_0(N), \chi)$ and Euler-Poincaré Series</td>
<td>164</td>
</tr>
<tr>
<td>5.6 Hecke Operators</td>
<td>166</td>
</tr>
<tr>
<td>5.7 Dirichlet Series and Their Functional Equation</td>
<td>168</td>
</tr>
<tr>
<td>5.8 The Petersson Inner Product</td>
<td>168</td>
</tr>
<tr>
<td>5.9 The Method of Poincaré Series</td>
<td>170</td>
</tr>
<tr>
<td>5.10 Fourier Coefficients of Poincaré Series</td>
<td>175</td>
</tr>
<tr>
<td>5.11 A Classical Bound for the Ramanujan $\tau$-Function</td>
<td>179</td>
</tr>
<tr>
<td>5.12 The Eichler-Selberg Trace Formula</td>
<td>179</td>
</tr>
<tr>
<td>5.13 $\ell$-Adic Representations and the Ramanujan Conjecture</td>
<td>180</td>
</tr>
<tr>
<td>5.14 Exercises</td>
<td>181</td>
</tr>
<tr>
<td>6 Representation of Numbers as Sums of Squares</td>
<td>185</td>
</tr>
<tr>
<td>6.1 Introduction</td>
<td>185</td>
</tr>
<tr>
<td>6.2 The Circle Method and Poincaré Series</td>
<td>186</td>
</tr>
<tr>
<td>6.3 Explicit Formulas for the Singular Series</td>
<td>194</td>
</tr>
<tr>
<td>6.4 The Singular Series</td>
<td>198</td>
</tr>
<tr>
<td>6.4.1 Quadratic Gaussian Sums</td>
<td>198</td>
</tr>
<tr>
<td>6.4.2 Ramanujan Sums</td>
<td>205</td>
</tr>
<tr>
<td>6.4.3 Fourier Transforms of Gaussian Sums</td>
<td>206</td>
</tr>
<tr>
<td>6.4.4 Local Singular Series $L_p(w, \rho_s)$, s Odd and $p$ Odd</td>
<td>211</td>
</tr>
<tr>
<td>6.4.5 Local Singular Series $L_2(w, \rho_s)$, s Odd</td>
<td>215</td>
</tr>
<tr>
<td>6.4.6 Local Singular Series $L_p(w, \rho_s)$, s Even</td>
<td>219</td>
</tr>
<tr>
<td>6.4.7 Examples</td>
<td>222</td>
</tr>
<tr>
<td>6.5 Exact Formulas for the Number of Representations</td>
<td>233</td>
</tr>
<tr>
<td>6.6 Examples: Quadratic Forms and Sums of Squares</td>
<td>245</td>
</tr>
</tbody>
</table>
## Contents

6.7 Liouville's Methods and Elliptic Modular Forms .......................... 248
  6.7.1 The Basic Elliptic Modular Forms ........................................ 249
  6.7.2 Jacobi's Identity: The Origin of Liouville's Methods ................. 253
6.8 Exercises ................................................................. 258

7 Arithmetic Progressions .................................................. 261
  7.1 Introduction ........................................................................ 261
  7.2 Van der Waerden's Theorem .................................................. 263
  7.3 Roth's Theorem \( \tau_3 = 0 \) .................................................. 265
  7.4 Szemerédi's Proof of Roth's Theorem ...................................... 271
  7.5 Bipartite Graphs .................................................................. 273
  7.6 Configurations ...................................................................... 279
  7.7 More Definitions .................................................................... 291
  7.8 The Choice of \( t_m \) ............................................................ 295
  7.9 Well-Saturated \( K \)-tuples ..................................................... 296
  7.10 Szemerédi's Theorem .......................................................... 307
  7.11 Arithmetic Progressions of Squares ........................................ 312
  7.12 Exercises ................................................................. 315

8 Applications ........................................................................ 317
  8.1 Factoring Integers ............................................................... 317
  8.2 Computing Sums of Two Squares ............................................ 320
  8.3 Computing Sums of Three Squares .......................................... 325
  8.4 Computing Sums of Four Squares ............................................ 327
  8.5 Computing \( r_s(n) \) ............................................................. 329
  8.6 Resonant Cavities ............................................................... 330
  8.7 Diamond Cutting ............................................................... 334
  8.8 Cryptanalysis of a Signature Scheme ....................................... 337
  8.9 Exercises ................................................................. 340

References ................................................................................. 343

Index ......................................................................................... 350