

Harold Davenport

---

# Aritmetica superiore

un'introduzione  
alla teoria dei numeri

0000091  
DAVENPORT  
ARITMETICA  
SUPERIORE

ZANICHELLI

Zanichelli

# Indice

## 6 Prefazione

## 7 Introduzione

### Capitolo I

#### Fattorizzazione e numeri primi

9	1. Le leggi dell'aritmetica
13	2. Dimostrazione per induzione
15	3. Numeri primi
16	4. Il teorema fondamentale dell'aritmetica
19	5. Conseguenze del teorema fondamentale
22	6. L'algoritmo di Euclide
24	7. Un'altra dimostrazione del teorema fondamentale
25	8. Una proprietà del M.C.D.
28	9. Fattorizzare un numero
31	10. La sequenza dei primi
34	Note

### Capitolo II

#### Congruenze

37	1. La notazione di congruenza
39	2. Congruenze lineari
40	3. Il teorema di Fermat
43	4. La funzione di Eulero $\phi(m)$
45	5. Il teorema di Wilson
46	6. Congruenze algebriche
47	7. Congruenze relative a un modulo primo
50	8. Congruenze in più incognite
51	9. Congruenze che comprendono tutti i numeri
52	Note

**Capitolo III****Residui quadratici**

- |    |  |
|----|--|
| 53 | 1. Radici primitive                        |
| 56 | 2. Indici                                  |
| 59 | 3. Residui quadratici                      |
| 61 | 4. Il lemma di Gauss                       |
| 62 | 5. La legge di reciprocità                 |
| 66 | 6. La distribuzione dei residui quadratici |
| 68 | Note                                       |

**Capitolo IV****Frazioni continue**

- |     |   |
|-----|---|
| 70  | 1. Introduzione   |
| 72  | 2. La frazione continua generale                          |
| 74  | 3. La regola di Eulero                                    |
| 76  | 4. I convergenti a una frazione continua                  |
| 78  | 5. L'equazione $ax - by = 1$                              |
| 80  | 6. Frazioni continue infinite                             |
| 83  | 7. Approssimazione diofantea                              |
| 84  | 8. Irrazionali quadratici                                 |
| 86  | 9. Frazioni continue puramente periodiche                 |
| 92  | 10. Il teorema di Lagrange                                |
| 95  | 11. L'equazione di Pell                                   |
| 99  | 12. Un'interpretazione geometrica delle frazioni continue |
| 101 | Note  |

**Capitolo V****Somme di quadrati**

- |     |  |
|-----|--|
| 102 | 1. Numeri rappresentabili come somma di due quadrati |
| 103 | 2. Primi nella forma $4k + 1$                        |
| 106 | 3. Costruzioni per $x$ e $y$                         |
| 110 | 4. Rappresentazioni con quattro quadrati             |
| 112 | 5. Rappresentazioni con tre quadrati                 |
| 113 | Note   |

**Capitolo VI****Forme quadratiche**

- |     |                      |
|-----|----------------------|
| 115 | 1. Introduzione      |
| 116 | 2. Forme equivalenti |
| 119 | 3. Il discriminante  |

- 
- 121 4. La rappresentabilità di un numero con una forma  
 122 5. Tre esempi  
 125 6. La riduzione delle forme definite positive  
 126 7. Le forme ridotte  
 129 8. Il numero di rappresentazioni  
 131 9. Il numero di classi  
 133 Note

## Capitolo VII

### Alcune equazioni diofantee

- 135 1. Introduzione  
 136 2. L'equazione  $x^2 + y^2 = z^2$   
 138 3. L'equazione  $ax^2 + by^2 = z^2$   
 142 4. Il problema di Fermat  
 145 5. L'equazione  $x^3 + y^3 = z^3 + w^3$   
 147 6. Ulteriori sviluppi  
 150 Note

## Capitolo VIII

### I computer e la teoria dei numeri

- 153 1. Introduzione  
 154 2. Test di primalità  
 158 3. Generatori di numeri "casuali"  
 163 4. Il metodo di fattorizzazione di Pollard  
 165 5. Fattorizzare grandi numeri  
 170 6. Il metodo crittografico di Diffie-Hellman  
 173 7. Il metodo crittografico RSA  
 174 Note

• 178 Esercizi

• 187 Suggerimenti

• 189 Risposte

195 Bibliografia

197 Indice analitico