

索引

| | |
|------------|------------|
| あ | |
| RSA 暗号 | 39 |
| アダマール | 16 |
| 暗号化 | 37 |
| 暗号システム | 37 |
| 暗号文 | 37 |
| い | |
| 位数 | 35 |
| う | |
| ウィルソンの定理 | 42 |
| お | |
| オイラー | 3, 4, 15 |
| オイラー関数 | 30 |
| オイラーの規準 | 41 |
| オイラーの定理 | 35 |
| か | |
| ガウス | 16 |
| ガウス和 | 46 |
| 鍵 | 37 |
| 可逆 | 19, 20, 29 |
| 確率的素数 | 34 |
| 完全数 | 4 |
| き | |
| 逆元 | 19, 29 |
| 既約剰余類群 | 29 |
| 共通鍵暗号 | 37 |
| く | |
| クンマー | 3 |
| こ | |
| 公開鍵 | 39 |
| 公開鍵暗号 | 37, 39 |
| 合成数 | 13 |
| 合同式 | 17, 21 |
| 公倍数 | 6 |
| 公約数 | 6 |
| さ | |
| 最小公倍数 | 6 |
| 最小値原理 | 9 |
| 最大公約数 | 6, 11 |
| し | |
| 自然な写像 | 27 |
| 自明な約数 | 13 |
| 剰余類 | 25 |
| 初等数論の基本定理 | 14 |
| す | |
| 数学的帰納法 | 9 |
| せ | |
| 整除関係 | 6 |
| ゼータ関数 | 16 |
| そ | |
| 素因数分解 | 13 |
| 素因数分解の一意性 | 14 |
| 相互法則 | 43 |
| 素数 | 13 |
| 素数定理 | 16 |
| 素数判定法 | 34 |
| ソフィー・ジェルマン | 3 |
| 孫子算経 | 24, 49 |
| た | |
| 第1 補充法則 | 43 |
| 第2 補充法則 | 43 |

| | |
|-------------------------|------------|
| 互いに素..... | 19, 20 |
| 単数..... | 13 |
| <hr/> | |
| ち | |
| 中国の剰余定理..... | 23, 28, 32 |
| <hr/> | |
| て | |
| ディオファントス方程式..... | 1 |
| Diffie-Hellman 鍵共有..... | 37 |
| ディリクレ..... | 3, 4 |
| <hr/> | |
| と | |
| ド・ラ・ヴァレー・プーサン..... | 16 |
| <hr/> | |
| は | |
| 倍数..... | 6 |
| <hr/> | |
| ひ | |
| p 進付値..... | 15 |
| ピタゴラス方程式..... | 2 |
| 秘密鍵..... | 39 |
| 平文..... | 37 |
| <hr/> | |
| ふ | |
| フェルマー..... | 3 |
| フェルマーテスト..... | 34 |
| フェルマーの最終定理..... | 3 |
| フェルマーの定理..... | 33 |
| 復号化..... | 37 |
| 双子素数..... | 4 |
| 不定方程式..... | 1 |
| <hr/> | |
| へ | |
| 平方剰余..... | 41 |
| 平方剰余記号..... | 41 |
| 平方剰余の相互法則..... | 43 |
| 平方非剰余..... | 41 |
| <hr/> | |
| ほ | |
| 法..... | 17 |
| 補充法則..... | 43, 45 |
| <hr/> | |
| め | |
| メルセンヌ素数..... | 4 |

| | |
|-----------------|--------|
| や | |
| 約数..... | 6 |
| <hr/> | |
| ゆ | |
| ユークリッド..... | 15 |
| ユークリッドの互除法..... | 7 |
| <hr/> | |
| り | |
| リーマン..... | 16 |
| リーマン予想..... | 16 |
| 離散対数問題..... | 38 |
| <hr/> | |
| れ | |
| 零因子..... | 20, 29 |
| <hr/> | |
| わ | |
| ワイルズ..... | 3 |
| 割り算の定理..... | 5 |