暗号の整数論

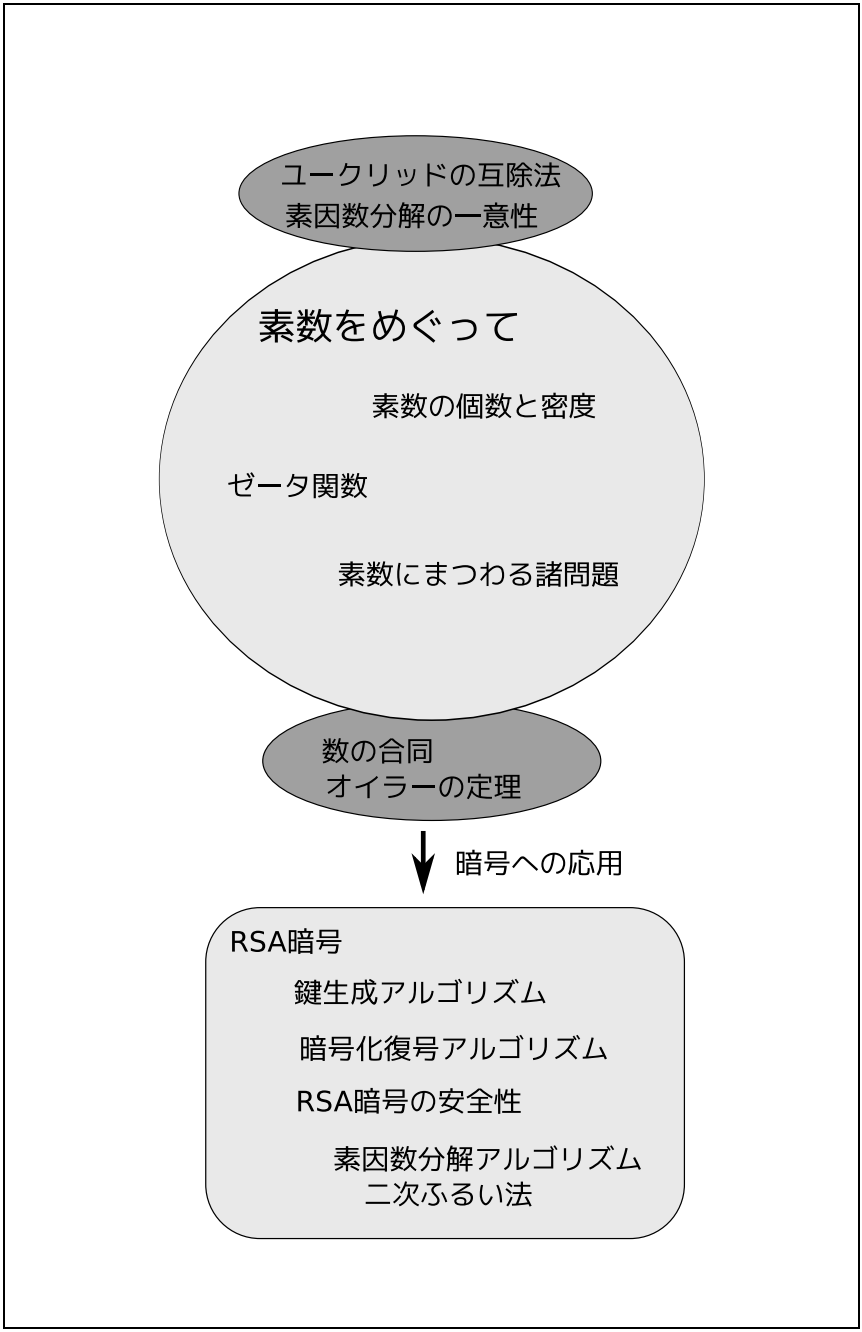
金子 昌信・境 隆一

第1章　公開鍵暗号

第2章　初等整数論から，特に素数をめぐって

第3章　RSA 暗号と素因数分解

第4章　文献案内


ユークリッドの互除法
素因数分解の一意性
素数をめぐって
素数の個数と密度
ゼータ関数
素数にまつわる諸問題
数の合同
オイラーの定理
暗号への応用
RSA暗号
鍵生成アルゴリズム
暗号化復号アルゴリズム
RSA暗号の安全性
素因数分解アルゴリズム
二次ふるい法

第 1 章

公開鍵暗号

暗号の歴史は古い．たとえば古代ギリシャで使用されていたといわれるスキュタレ暗号というものがある．「スキュタレ」とは木棒のことで，この木棒に紙テープを螺旋(らせん)状に巻きつけ，その棒を横向きに置く．そして，暗号化したい文章を横書きに書いた後，紙テープを解けば，その紙テープ上にはある一定の規則により文字の順序が入れかえられた暗号文が完成する．この紙テープに書かれた暗号文を受け取った者は，同じ太さの木棒にこの紙テープを螺旋状に巻きつけて横向きに文字を読めば，暗号文を復号できるのである．復号とは，

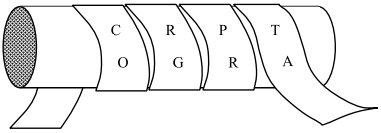


図 1.1 スキュタレ暗号

暗号化された文章をもとの文章に復元することをいう．このスキュタレ暗号では「暗号化」「復号化」の「手順」は紙を木棒に巻きつけるということであり，その際の重要な情報（「鍵」と呼ばれる）は木棒の太さである．「手順」と「鍵」が知られれば暗号は復号される．また，ローマ時代のシーザー暗号と呼ばれる暗号は，すべてのアルファベットを ABC 順である決まった字数だけずらして暗号文を作るというもので，この場合暗号化，復号化の手順は文字をずらすということであり，鍵は何文字ずらすかという数字である．これらの暗号では，手順や鍵を暗号作成者と復号者の間で秘密裡に共有する必要がある．そのどれかが他者に知られると，それが暗号解読の手がかりになるのは明らかであろう．

紀元前から近代まで，主として軍事・外交の場で「情報の秘匿」を目的とし