本章では暗号の数学について解説します．具体的には公開鍵暗号として，RSA暗号と楕円曲線暗号を，共通鍵暗号として，AES暗号を取り上げます．それぞれの詳細な説明は後述するとして，暗号を実社会に実装する際には，その実装の効率性と安全性を考慮することが重要です．本章ではスペースの関係で安全な実装についての詳細な議論は行いませんが，現在知られている基本的な実装法について解説します．

● 暗号実装の基礎知識

暗号実装において重要となる概念として，群・体があります．群とは1つの演算が定義された元の集合です．このときの演算とは，集合の中の2つの元を取って，その2つの元を結合して，また集合の中の元になるようなものを指します．体とは2つの演算を定義したものです．もう少し詳しい説明を本誌サポート・ページにのせましたので，そちらもご覧ください．

本誌サポート・ページ
https://interface.cqpub.co.jp/202404gou/

8-1 モンゴメリ乗算

三好 茜音，野上 保之

● 概要

暗号の分野では剰余演算は計算コストの大きな演算です．これを効率的に行う手法としてモンゴメリ表現を用いた剰余演算が知られています．これはモンゴメリ乗算と呼ばれます．

● モンゴメリ演算

モンゴメリ乗算とは$a \times b \pmod{p}$を求める際に最もコストが大きい除算を減らし，高速に乗算剰余算を求めることのできるアルゴリズムです．モンゴメリ乗算は整数値をモンゴメリ表現に変換し，乗算を行い，乗算結果を整数に逆変換することで除算を減らしています（**図1**）．

▶モンゴメリ・リダクション

モンゴメリ乗算で重要になる演算にモンゴメリ・リダクションという関数があります．ここで，自然数rとpが$r > p$かつrとpが互いに素（rとpを共に割り切る正の整数が1のみ）であるとき，整数値tに関するモンゴメリ・リダクションは下記のように定義されています．

$$\mathrm{MR}(t) = tr^{-1}$$

ここで，p'を$p \times p' \equiv -1 \pmod{r}$の成り立つ整数値とするとモンゴメリ・リダクションの計算は次のような手順で行えます．

①$k' = t \times p' \pmod{r}$を計算する
②$k = \{t + (k' \times p)\} / r$を計算する
③$k \geq p$の場合は$k - p$が整数値tに関するモンゴメリ・リダクション結果となり，$k < p$の場合はkが整数値tに関するモンゴメリ・リダクション結果となる

このとき，rを2のべき乗にすると，ある任意の整数xに対して$x \pmod{r}$はxと$r-1$のビットANDをとると求めることができ，x/rは$r = 2^n$とした際にxをnビット右シフトした値になります．剰余算や除算をビット演算に置き換えることでコストの重い演算を削減することができます．そのため，今回はrが2のべき乗の際のプログラムを示します．

▶モンゴメリ変換

整数aからモンゴメリ表現Aへの変換は以下のように定義されています．

$$A = ar \pmod{p}$$

これはモンゴメリ・リダクションを用いて求めることができます．

$$A \leftarrow \mathrm{MR}(ar^2)$$

▶モンゴメリ逆変換：

モンゴメリ表現Aから整数aへの変換は以下のように定義されています．

$$a = Ar^{-1} \pmod{p}$$

これはモンゴメリ・リダクションを用いて求めることができます．

$$a \leftarrow \mathrm{MR}(A)$$

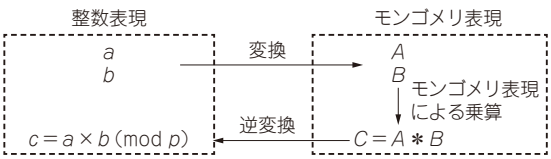

図1 モンゴメリ乗算の仕組み

● コード

$c = a \times b \pmod{p}$はモンゴメリ・リダクションとモンゴメリ表現の変換と逆変換を次のように用いると求めることができます．この計算のコードを**リスト1**～**リスト3**に示します（次の番号①～④はリスト中の番