1.7　既約剰余類

合同類の積のところで述べたように，$\mathbb{Z}_m - \{[0]\}$ は，m が素数でなければ，積に関して群にならない。例えば，$m = pq$ となっているなら，$pq \equiv 0 \mod m$ であるから，$[p], [q] \in \mathbb{Z}_m$ に対し $[p][q] = [0] \in \mathbb{Z}_m$ となってしまい，p, q は $\mathbb{Z}_m - \{[0]\}$ の中では積に関する逆元をもたないからである。

$\mathbb{Z}_n - \{[0]\}$ は積に関して群をなさない。しかし集合を制限して群にすることができる。$\mathbb{Z}_9$ を考える。$\mathbb{Z}_9^* = \{[a] \in \mathbb{Z}_9 \mid a \text{ と } 9 \text{ は互いに素}\}$ と定義する。今の場合 9 と互いに素なのは $1, 2, 4, 5, 7, 8$ なので $\mathbb{Z}_9^* = \{[1], [2], [4], [5], [7], [8]\}$ である。$[2][5] = [10] = [1]$，$[4][7] = [28] = [1]$，$[8][8] = [64] = [1]$ なので $[2]^{-1} = [5], [4]^{-1} = [7], [5]^{-1} = [2], [7]^{-1} = [4], [8]^{-1} = [8], [1]^{-1} = [1]$ で $\mathbb{Z}_9^*$ の元はすべて逆元をもつ。よって $\mathbb{Z}_9^*$ は乗法にかんして郡をなす。

定理 1.28 n を自然数とする。$\mathbb{Z}_n^* = \{[a] \in \mathbb{Z}_n \mid (a, n) = 1\}$ とおくと，$\mathbb{Z}_n^*$ は乗法に関し郡をなす。

証明　逆元を持つことを示せばよい。$[a] \in \mathbb{Z}_n^*$ を任意の元とする。このとき a と n は互いに素なので定理 1.4 により

$$k_1 a + k_2 n = 1$$

となる整数 k_1, k_2 が存在する。k_1 と n が互いに素でない場合，その最大公約数を d とすると $d > 1$ である。このとき d は k_1 および n の約数なので $k_1 a + k_2 n$ の約数でもある。よって $d > 1$ が 1 の約数になり矛盾。よって k_1 は n と互いに素である。$\mathbb{Z}_n$ で合同式を考えると

$$[1] = [k_1 a + k_2 n] = [k_1 a] + [k_2 n] = [k_1][a] + [k_2][n] = [k_1][a] + [k_2][0] = [k_1][a]$$

となる。$[k_1] \in \mathbb{Z}_n^*$ なので $[a]$ は逆元 $[k_1]$ を持つ。∎

定義 1.29　$m \geqq 2$ を自然数とする。

(1)　$p \in \{1, \cdots, m-1\}$ が m と互いに素であるなら，p を含む $\mathbb{Z}_m$ の剰余類を **既約剰余類** という。

(2)　$\mathbb{Z}_m$ における既約剰余類全体の集合を $\mathbb{Z}_m^*$ で表す。m が素数なら $\mathbb{Z}_m^* = \mathbb{Z}_m - \{[0]\}$ であるが，一般にはそうなるとは限らない。

(3)　$\mathbb{Z}_m^*$ の元は積に関して逆元を持っているので，この集合は積に関して群をなす。これを **既約剰余類群** という。

(4)　$\varphi(m) = |\mathbb{Z}_m^*|$ とおき，これを **オイラー関数** という。$\varphi(1) = 1$ と決める。

注意 1。　オイラー関数 $\varphi(m)$ は，$\{1, \cdots, m-1\}$ の中で m と互いに素であるものの個数を表す。例えば，p が素数ならば $\varphi(p) = p - 1$ である。また，

$$\varphi(4) = 2, \quad \varphi(6) = 2, \quad \varphi(8) = 4, \quad \varphi(9) = 6, \quad \varphi(10) = 4$$

など。

注意 2。 一般に，既約剰余類群は巡回群とは限らない。例えば，$\mathbb{Z}_8^* = \{1,3,5,7\}$ であるが，$\mathbb{Z}_8^*$ において，

$$3^2 = 1 \qquad 5^2 = 1 \qquad 7^2 = 1$$

となって，単位元以外の全ての元の位数が 2 であり，どの元も $\mathbb{Z}_8^*$ 全体を生成しない。

定理 1.21 およびその直後の演習問題 1.7 より次の定理が成り立つ。これは，フェルマーの小定理の一般形であり，オイラーによって証明された。

定理 1.30 (一般化されたフェルマーの小定理) $m \geqq 2$ を自然数とする。
任意の $[a] \in \mathbb{Z}_m^*$ に対して

$$a^{\varphi(m)} = 1$$

が成り立つ。言い換えると，$a \in \mathbb{Z}$ が m と互いに素ならば，

$$a^{\varphi(m)} \equiv 1 \mod m$$

である。

演習問題 1.9 定理 1.21 および演習問題 1.7 を用いて，定理 1.30 の定理を証明せよ。

1.8 拡張ユークリッド・アルゴリズム

前セクションで見たように，$m \geqq 2$ を自然数とすると，$\mathbb{Z}_m^*$ の任意の元 e は積に関する逆元 e^{-1} を持つ。(なお，ここで e は積に関する単位元ではなく，単なる $\mathbb{Z}_m^*$ の元の意味で使っているので注意。)

それでは具体的に，m と互いに素な $e \in \{1,2,\cdots,m-1\}$ が与えられた時，それの $\mathbb{Z}_m^*$ における逆元 $e^{-1} \in \{1,2,\cdots,m-1\}$ はどのように計算したら良いのだろうか？ 実はこの計算は，RSA 暗号において，その根幹をなす重要な部分となる。

m と e は互いに素なので，定理 1.9 より，ある整数 k_1, k_2 があって，$k_1 e + k_2 m = 1$ となる。$k_1 e = -k_2 m + 1$ なので，$k_1 e \equiv 1 \mod m$ であり，これは，k_1 を含む剰余類が e の逆元であることを示している。

従って，$e \in \mathbb{Z}_m^*$ の逆元を求める問題は，

- $k_1 e + k_2 m = 1$ を満たす k_1 を求める問題である。

と言える。k_1 が求まれば自動的に k_2 も決まってしまうので，これは，

- $k_1 e + k_2 m = 1$ を満たす (k_1, k_2) を求める問題。

と言うことができる。

この (k_1, k_2) は，実はユークリッドの互除法を利用することにより求めることができる。この方法を **拡張ユークリッド・アルゴリズム** という。それは，以下のようにして行う。

$e \in \{1, 2, \cdots, m-1\}$ であるので $e < m$ である。$GCD(m, e)$ を求めるユークリッドの互除法を行ってみる。$GCD(m, e) = 1$ なので，これは最後の余りが 1 になった時点で終了する。

$$\begin{aligned} m &= q_1 e + r_1 \\ e &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ r_2 &= q_4 r_3 + r_4 \\ \cdots &\quad \cdots \\ r_{s-2} &= q_s r_{s-1} + r_s \\ r_{s-1} &= q_{s+1} r_s + r_{s+1} \\ r_s &= q_{s+2} r_{s+1} + 1 \end{aligned}$$

となったとする。

- $m = q_1 e + r_1$ より $r_1 = m - q_1 e$ である。すなわち，最初の余り r_1 は m と e の 1 次結合で表されている。
- $e = q_2 r_1 + r_2$ より $r_2 = e - q_2 r_1$ である。すなわち，r_2 は e と r_1 の 1 次結合で表されている。しかし，最初の式から，r_1 は m と e の 1 次結合で表されているので，結局，r_2 は m と e の 1 次結合で表される。
- $r_1 = q_3 r_2 + r_3$ より $r_3 = r_1 - q_3 r_2$ である。すなわち，r_3 は r_1 と r_2 の 1 次結合で表されている。しかし，r_1 と r_2 は共に m と e の 1 次結合で表されているので，結局，r_3 は m と e の 1 次結合で表される。
- このプロセスを繰り返すことにより，全ての余り r_i は，m と e の 1 次結合で表されることになる。
- 最後の余りは 1 なので，最終的に，1 が m と e の 1 次結合で表されることになる。これにより，$k_1 e + k_2 m = 1$ という式に到達する。

この方法を見るとわかるように，基本的にこれはユークリッド互除法であり，アルゴリズムの計算量はユークリッド互除法とほとんど同じである。すなわち，200 桁程度の m や e に対しては，現在の計算機の能力からすれば，極めて短時間で計算可能である。

例: 具体例で見てみよう。

$$36\,a + 47\,b = 1$$

を満たす整数 a, b を求めることを考える。

47 は素数なので，当然 $GCD(36, 47) = 1$ であり，定理 1.4 より，求める整数解 a, b は存在する。

ユークリッド互除法により，36, 47 の最大公約数 1 を求めるプロセスを実行してみると，

$$
\begin{aligned}
47 &= 36 + 11 \\
36 &= 3 \cdot 11 + 3 \\
11 &= 3 \cdot 3 + 2 \\
3 &= 2 + 1
\end{aligned}
$$

となる。

拡張ユークリッド・アルゴリズムは，ユークリッド互除法を実行しながら，この余りの数 11, 3, 2, 1 を 36 と 47 の 1 次結合で表して行く，というプロセスである。

具体的には，

$$
\begin{aligned}
11 &= -36 + 47 \\
3 &= 36 - 3 \cdot 11 = 36 - 3 \cdot (-36 + 47) = 4 \cdot 36 - 3 \cdot 47 \\
2 &= 11 - 3 \cdot 3 = (-36 + 47) - 3 \cdot (4 \cdot 36 - 3 \cdot 47) = -13 \cdot 36 + 10 \cdot 47 \\
1 &= 3 - 2 = (4 \cdot 36 - 3 \cdot 47) - (-13 \cdot 36 + 10 \cdot 47) = 17 \cdot 36 - 13 \cdot 47
\end{aligned}
$$

となり，$a = 17, b = -13$ が得られた。

ちなみに，この $17 \cdot 36 - 13 \cdot 47 = 1$ より，

$$36 \cdot 17 \equiv 1 \mod 47$$

がわかる。すなわち，$\mathbb{Z}_{47}^*$ において，36 の積に関する逆元は 17 である。

演習問題 1.10　互いに素である 2 つの自然数 m, n を入力すると，$\mathbb{Z}_m^*$ における n の逆元 n^{-1} を出力するプログラムを作れ。可能なものは BigInteger クラスを用いていくらでも大きい自然数に対応可能なものを作れ。