代数学 I 第 4 回講義資料

担当：大矢 浩徳 (OYA Hironori)*

前回，新たな数の体系として整数の剰余類環 $\mathbb{Z}/n\mathbb{Z}$ と呼ばれるものを導入し，そこで $+, -, \times$ という二項演算が整数の場合と同様に定まる (well-defined) ということを見た．また，$(\mathbb{Z}/n\mathbb{Z}, +)$ が群となることを確かめ，その部分群を全て決定した．今回は，$\mathbb{Z}/n\mathbb{Z}$ における $\times$ を二項演算として実現される群を扱う．ポイントは「$\mathbb{Z}/n\mathbb{Z}$ において $\times$ に関する逆元を持つのはいつか?」ということである．さらに，$\times$ という演算の応用としてフェルマーの小定理を証明する．

3.1 $\mathbb{Z}/n\mathbb{Z}$ の乗法群

n を 2 以上の整数とする．$\mathbb{Z}/n\mathbb{Z}$ における $\times$ を二項演算として実現される群について考えよう．まず，$\times$ は

$$\times\colon \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z},\ ([a]_n, [b]_n) \mapsto [a]_n[b]_n \coloneqq [ab]_n$$

というように $\mathbb{Z}$ の積をそのまま用いて定義されていたので，結合法則は

$$([a]_n[b]_n)[c]_n = [abc]_n = [a]_n([b]_n[c]_n)\ (a, b, c \in \mathbb{Z})$$

となって成立する．また，$[1]_n \in \mathbb{Z}/n\mathbb{Z}$ は

$$[1]_n[a]_n = [a]_n = [a]_n[1]_n\ (a \in \mathbb{Z})$$

を満たすので，単位元の性質を満たしている．

それでは，逆元を持つ $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ はどのようなものだろうか．$[1]_n$ を単位元としているので，逆元は以下のように定義される．

定義 3.1

$[a]_n \in \mathbb{Z}/n\mathbb{Z}$ に対して，$[a]_n^{-1}$ を

$$[a]_n[a]_n^{-1} = [1]_n$$

を満たす $\mathbb{Z}/n\mathbb{Z}$ の元とする．この元を $[a]_n$ の $\times$ **に関する逆元**という．$\mathbb{Z}/n\mathbb{Z}$ においては $[a]_n[b]_n = [ab]_n = [b]_n[a]_n$ が成立するので，$[a]_n[a]_n^{-1} = [1]_n$ のとき，$[a]_n^{-1}[a]_n = [1]_n$ も成立することに注意．

まず注意しないといけないのは，$a \in \mathbb{Z}$ が ± 1 でないとき，$[a]_n^{-1}$ は$\underline{[1/a]_n \text{ ではない！}}$ この場合 $1/a$ は整数では無いので，$[1/a]_n$ という元は $\mathbb{Z}/n\mathbb{Z}$ に存在しないのである．それにもかかわらず，$\mathbb{Z}/n\mathbb{Z}$ において $\times$ に関する逆元を持つ元は ($\mathbb{Z}$ の場合とは違って)$[\pm 1]_n$ だけではない．例えば，以下のような例がある．

例 1. $\mathbb{Z}/7\mathbb{Z}$ において，

$$[4]_7[2]_7 = [8]_7 = [1]_7$$

となるので，$[4]_7^{-1} = [2]_7$.

$\mathbb{Z}/12\mathbb{Z}$ において，

$$[5]_{12}[5]_{12} = [25]_{12} = [1]_{12}$$

となるので，$[5]_{12}^{-1} = [5]_{12}$.

一方で，$\times$ に関する逆元は常に存在するわけではない．

* *e-mail* : hoya@shibaura-it.ac.jp

例 2. $\mathbb{Z}/n\mathbb{Z}$ において，任意の $a \in \mathbb{Z}$ に対し，

$$[0]_n[a]_n = [0]_n$$

となるので，$[0]_n$ は $\times$ に関する逆元を持たない．

$\mathbb{Z}/6\mathbb{Z}$ において，

$$[2]_6[0]_6 = [0]_6 \qquad [2]_6[1]_6 = [2]_6 \qquad [2]_6[2]_6 = [4]_6$$
$$[2]_6[3]_6 = [6]_6 = [0]_6 \qquad [2]_6[4]_6 = [8]_6 = [2]_6 \qquad [2]_6[5]_6 = [10]_6 = [4]_6$$

となるので，$[2]_6$ は $\times$ に関する逆元を持たない．

そこで，逆元を持つ元からなる $\mathbb{Z}/n\mathbb{Z}$ の部分集合を定義しておく．

定義 3.2

$(\mathbb{Z}/n\mathbb{Z})^\times := \{[a]_n \mid [a]_n^{-1}$が存在 $\} = \{[a]_n \mid$ ある $b \in \mathbb{Z}$ が存在して，$[a]_n[b]_n = [1]_n\}$.[*1]

このとき，以下が成立する．

命題 3.3

(1) $(\mathbb{Z}/n\mathbb{Z})^\times$ は演算 $\times$ で閉じている．すなわち，任意の $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，

$$[a]_n[b]_n = [ab]_n \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

(2) $(\mathbb{Z}/n\mathbb{Z})^\times$ は逆元を取る操作で閉じている．すなわち，任意の $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，

$$[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times.$$

証明. (1) 任意の $[a]_n, [b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ に対し，$[a]_n[b]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ であること，つまり $[a]_n[b]_n$ に $\times$ に関する逆元が存在することを示せばよい．$[a]_n^{-1}, [b]_n^{-1}$ が存在することより，

$$([a]_n[b]_n)([b]_n^{-1}[a]_n^{-1}) = [a]_n([b]_n[b]_n^{-1})[a]_n^{-1} = [a]_n[1]_n[a]_n^{-1} = [a]_n[a]_n^{-1} = [1]_n.$$

よって，$[b]_n^{-1}[a]_n^{-1}$ が $[a]_n[b]_n$ の $\times$ に関する逆元となり，逆元の存在が示された． □

(2) $[a]_n[a]_n^{-1} = [a]_n^{-1}[a]_n = [1]_n$ は $[a]_n^{-1}$ の $\times$ に関する逆元が $[a]_n$ であるという式でもある．よって，$[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ であるとき，$[a]_n^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$ である． □

命題 3.3 (1) より，集合 $(\mathbb{Z}/n\mathbb{Z})^\times$ に二項演算

$$\times\colon (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times,\ ([a]_n, [b]_n) \mapsto [ab]_n$$

が定義される．これにより，$((\mathbb{Z}/n\mathbb{Z})^\times, \times)$ は群をなす．実際，結合法則の成立，単位元の存在については本節の冒頭で述べた通り ($[1]_n^{-1} = [1]_n$ なので，$[1]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$)，逆元の存在については命題 3.3 (2) よりわかる．この群を $\mathbb{Z}/n\mathbb{Z}$ **の乗法群**という．

3.2 $\times$ に関する逆元の計算方法

本節では，乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の構造についてより具体的に見ていくことにする．まずは $(\mathbb{Z}/n\mathbb{Z})^\times$ に具体的にどのような元が含まれるかについて調べよう．

命題 3.4

$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a]_n \mid \gcd(a, n) = 1\}$.[*2]

[*1] $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ に対し，$\mathbb{K}^\times := \mathbb{K} \setminus \{0\}$ も $\mathbb{K}$ の中で $\times$ に関する逆元を持つものの集まりとなっていたことに注意しよう，

[*2] 負の数に対応する gcd については，補足プリント「拡張ユークリッド互除法について」を参照のこと．

証明. 次の同値関係をたどっていけばよい.

$$\begin{aligned}[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times &\Leftrightarrow \text{ある } x \in \mathbb{Z} \text{ が存在して，} [ax]_n (= [a]_n[x]_n) = [1]_n \\ &\Leftrightarrow \text{ある } x, y \in \mathbb{Z} \text{ が存在して，} ax + ny = 1 \\ &\Leftrightarrow \gcd(a, n) = 1 \ (a \text{ と } n \text{ は互いに素}). \text{ (第 3 回講義資料, 系 2.5 より)}\end{aligned}$$

□

例 3.

$$(\mathbb{Z}/12\mathbb{Z})^\times = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\} \qquad (\mathbb{Z}/7\mathbb{Z})^\times = \{[1]_7, [2]_7, [3]_7, [4]_7, [5]_7, [6]_7\}$$

命題 3.4 の証明を見ると，各 $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ の $\times$ に関する逆元 $[a]_n^{-1}$ は，整数の組 (x, y) が

$$ax + ny = 1 \tag{3.1}$$

を満たすとき,

$$[a]_n^{-1} = [x]_n$$

として求められるということがわかる．(3.1) を満たす整数の組 (x, y) は拡張ユークリッド互除法で見つけることができる (第 3 回講義資料参照)．例題でこれを確かめてみよう．

例題

$\mathbb{Z}/60\mathbb{Z}$ において，$[17]_{60}$ の $\times$ に関する逆元を求めよ．

解答. まず，$\gcd(17, 60) = 1$ なので，命題 3.4 より，$[17]_{60}$ は確かに $(\mathbb{Z}/60\mathbb{Z})^\times$ の元である．

$$17x + 60y = 1$$

を満たす整数の組 (x, y) を拡張ユークリッド互除法で求める．

$$\begin{aligned}60 &= 3 \times 17 + 9 & \qquad 17 &= 1 \times 9 + 8 \\ 9 &= 1 \times 8 + 1 & \qquad 8 &= 8 \times 1 + 0\end{aligned}$$

であるので,

$$\begin{aligned}1 &= 9 - 1 \times 8 \\ &= 9 + (-1) \times (17 - 1 \times 9) \\ &= (-1) \times 17 + 2 \times 9 \\ &= (-1) \times 17 + 2 \times (60 - 3 \times 17) \\ &= (-7) \times 17 + 2 \times 60\end{aligned}$$

より，$(x, y) = (-7, 2)$ が $17x + 60y = 1$ を満たす整数の組の例である．よって，求める逆元は

$$[17]_{60}^{-1} = [-7]_{60} = [53]_{60}.$$

□

検算してみると，確かに $[17]_{60}[-7]_{60} = [-119]_{60} = [1]_{60}$ となっている．

さて，$(\mathbb{Z}/n\mathbb{Z})^\times$ の元の個数を表す有名な関数をここで導入しておこう．

定義 3.5

正の整数 n に対し，n と互いに素な 1 以上 n 以下の自然数の個数を $\varphi(n)$ と書く．つまり，

$$\varphi(n) \coloneqq \#\{m \in \mathbb{N} \mid 1 \le m \le n, \gcd(m, n) = 1\}^{*3}$$

とする．n に対して $\varphi(n)$ を与える関数 $\varphi\colon \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}, n \mapsto \varphi(n)$ を**オイラー (Euler) の φ 関数**という．

[*3] $\#\{\dots\}$ は集合 $\{\dots\}$ の元の個数を表す記号である.

例 4. $\varphi(n)$ の計算は定義通り考えると以下のように行うことができる．

- $\gcd(1,1)=1$ より，$\varphi(1)=1$.
- $\gcd(1,2)=1, \gcd(2,2)=2$ なので，1 以上 2 以下の自然数 m で，$\gcd(m,2)=1$ を満たすものは 1 つであるから，$\varphi(2)=1$.
- $\gcd(1,3)=1, \gcd(2,3)=1, \gcd(3,3)=3$ なので，1 以上 3 以下の自然数 m で，$\gcd(m,3)=1$ を満たすものは 2 つであるから，$\varphi(3)=2$.
- $\gcd(1,4)=1, \gcd(2,4)=2, \gcd(3,4)=1, \gcd(4,4)=4$ なので，1 以上 4 以下の自然数 m で，$\gcd(m,4)=1$ を満たすものは 2 つであるから，$\varphi(4)=2$.
- $\gcd(1,5)=1, \gcd(2,5)=1, \gcd(3,5)=1, \gcd(4,5)=1, \gcd(5,5)=5$ なので，1 以上 5 以下の自然数 m で，$\gcd(m,5)=1$ を満たすものは 4 つであるから，$\varphi(5)=4$.

この調子で進めて行くと以下のようになる．

n	1	2	3	4	5	6	7	8	9	10	11	12
$\varphi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

ここで，2 以上の自然数 n について，

$$n \text{ が素数} \quad \Leftrightarrow \quad 1,\dots,n-1 \text{ は全て } n \text{ と互いに素} \quad \Leftrightarrow \quad \varphi(n)=n-1 \tag{3.2}$$

となることに注意する．

命題 3.4 とオイラーの φ 関数の定義より，以下のことは直ちにわかる．

命題 3.6

$\#(\mathbb{Z}/n\mathbb{Z})^\times=\varphi(n)$．つまり，乗法群 $(\mathbb{Z}/n\mathbb{Z})^\times$ の位数は $\varphi(n)$ である．

命題 3.6 と (3.2) での考察から，

$$\#(\mathbb{Z}/n\mathbb{Z})^\times=n-1 \quad \Leftrightarrow \quad n \text{ は素数}$$

であることがわかる．ここで例 2 で見たように，$[0]_n$ は $\times$ に関する逆元を持たないので，$\#(\mathbb{Z}/n\mathbb{Z})^\times=n-1$ であるとき，

$$(\mathbb{Z}/n\mathbb{Z})^\times=(\mathbb{Z}/n\mathbb{Z})\setminus\{[0]_n\}$$

である．つまり，

$$(\mathbb{Z}/n\mathbb{Z})^\times=(\mathbb{Z}/n\mathbb{Z})\setminus\{[0]_n\} \quad \Leftrightarrow \quad n \text{ が素数.} \tag{3.3}$$

となる．これより，p が素数のとき，$\mathbb{Z}/p\mathbb{Z}$ は「和 $+$ と積 $\times$ が定まっていて，$[0]_n$ 以外のすべての元が $\times$ に関する逆元を持つ」という性質を持つことがわかる．これは，$\mathbb{Q},\mathbb{R},\mathbb{C}$ と似た性質である．こういった加減乗除のできる代数系の抽象化が第 1, 2 回講義資料でも現れた**体**と呼ばれるものであった．この言葉を用いれば，以下のように言うこともできる．

$$\mathbb{Z}/n\mathbb{Z} \text{ が体である} \quad \Leftrightarrow \quad n \text{ が素数.}$$

$\mathbb{Z}/p\mathbb{Z}$ (p は素数) という形の体は，有限個の元からなる体ということで，**有限体**と呼ばれるものの例となり，$\mathbb{F}_p$ とも書かれる．有限体は符号理論，暗号理論等でも用いられる応用上も重要な代数系である．

3.3 フェルマーの小定理

今回調べた $\mathbb{Z}/n\mathbb{Z}$ の積構造の応用として，フェルマーの小定理について紹介しよう．まず，フェルマーの小定理を示すために，以下の命題を準備する．

命題 3.7

p を素数とする．このとき，任意の $a, b \in \mathbb{Z}$ に対し，

$$([a]_p + [b]_p)^p = ([a]_p)^p + ([b]_p)^p$$

ここで p 乗は，$\mathbb{Z}/p\mathbb{Z}$ における $\times$ を p 回繰り返し行うという意味である．

証明.

$$\begin{aligned}([a]_p + [b]_p)^p &= ([a+b]_p)^p \\ &= [(a+b)^p]_p \\ &= \left[a^p + {}_p\mathrm{C}_1 a^{p-1}b + {}_p\mathrm{C}_2 a^{p-2}b^2 + \cdots + {}_p\mathrm{C}_{p-1}ab^{p-1} + b^p\right]_p \quad \text{(二項定理)}.\end{aligned}$$

ここで，${}_p\mathrm{C}_k = \dfrac{p!}{k!(p-k)!}$ $(k = 1, \ldots, p-1)$ である．いま，p は素数なので，$k = 1, \ldots, p-1$ のとき，$k!(p-k)!$ は p では割り切れない．一方で，$p!$ は p で割り切れることに注意すると，${}_p\mathrm{C}_k$ は $k = 1, \ldots, p-1$ のとき，p の倍数であることがわかる．これより，$\mathbb{Z}/p\mathbb{Z}$ における同一視のルールから，

$$\left[a^p + {}_p\mathrm{C}_1 a^{p-1}b + {}_p\mathrm{C}_2 a^{p-2}b^2 + \cdots + {}_p\mathrm{C}_{p-1}ab^{p-1} + b^p\right]_p = [a^p + b^p]_p.$$

以上より，$([a]_p + [b]_p)^p = [a^p + b^p]_p = ([a]_p)^p + ([b]_p)^p$ となる． □

以下がフェルマーの小定理 (Fermat's little theorem)[*4]と呼ばれる定理である．

定理 3.8

p を素数する．このとき，任意の $a \in \mathbb{Z}$ に対し，

$$[a^p]_p = [a]_p.$$

さらに，a が p の倍数でないとき (つまり $[a]_p \neq [0]_p$ のとき)，

$$[a^{p-1}]_p = [1]_p.$$

証明. まず $[a^p]_p = [a]_p$ を示す．$a = 0$ のとき，$[0]_p = [0]_p$ となって成立する．

$a > 0$ のとき，命題 3.7 を繰り返し用いると，

$$\begin{aligned}[a^p]_p = ([a]_p)^p = ([1]_p + [a-1]_p)^p &= ([1]_p)^p + ([a-1]_p)^p \\ &= ([1]_p)^p + ([1]_p + [a-2]_p)^p = ([1]_p)^p + ([1]_p)^p + ([a-2]_p)^p \\ &\cdots \\ &= \underbrace{([1]_p)^p + ([1]_p)^p + \cdots + ([1]_p)^p}_{a \text{ 個}} = \underbrace{[1]_p + [1]_p + \cdots + [1]_p}_{a \text{ 個}} = [a]_p\end{aligned}$$

$a < 0$ のとき，

$$[a^p]_p = [(-1)^p(-a)^p]_p = (-1)^p[(-a)^p]_p = (-1)^p[-a]_p \quad (-a > 0 \text{ なので上で示したことよりわかる})$$

となる．ここで，$p = 2$ のとき，$[-a]_2 = [a]_2$ なので，$(-1)^2[-a]_2 = [a]_2$．$p > 2$ のとき，p は奇数なので，$(-1)^p[-a]_p = -[-a]_p = [a]_p$．これより，いずれの場合も，

$$[a^p]_p = (-1)^p[-a]_p = [a]_p$$

が成立する．以上で，任意の $a \in \mathbb{Z}$ に対し，$[a^p]_p = [a]_p$ が示された．

[*4] フェルマーの「小」定理と呼ばれているのは，有名なフェルマーの最終定理 (Fermat's last theorem) との区別のためである．フェルマーの最終定理とは「$n \geq 3$ のとき，$x^n + y^n = z^n$ を満たす正の整数 x, y, z は存在しない」という定理で，P.Fermat(1607–1665) がこの主張を述べてから 350 年以上かかって A.Wiles によって 1995 年に完全に証明された．

次に，$[a]_p \neq [0]_p$ のとき，(3.3) より $[a]_p^{-1}$ が存在することがわかる．よって，$([a]_p)^p = [a^p]_p = [a]_p$ の両辺に $[a]_p^{-1}$ を掛けて，

$$([a]_p)^{p-1} = [a^{p-1}]_p = [1]_p$$

を得る． □

例 5.

$$[1^4]_5 = [1]_5 \qquad [2^4]_5 = [16]_5 = [1]_5 \qquad [3^4]_5 = [81]_5 = [1]_5 \qquad [4^4]_5 = [256]_5 = [1]_5$$

$$[2^{30}]_{31} = [1073741824]_{31} = [31 \times 34636833 + 1]_{31} = [1]_{31}$$

フェルマーの小定理の一般化：オイラーの定理. フェルマーの小定理は，以下のような形で p が素数でない場合に一般化される．これはオイラーの定理 (Euler's theorem) と呼ばれる．

定理 3.9

n が正の整数，$a \in \mathbb{Z}, \gcd(a, n) = 1$ のとき，

$$[a^{\varphi(n)}]_n = [1]_n.$$

オイラーの定理で n を素数とすると，a が n の倍数でさえなければ $\gcd(a, n) = 1$ となり，しかも $\varphi(n) = n - 1$ となるので ((3.2))，確かにこの定理はフェルマーの小定理を含んでいる．この定理は群論を学ぶと，群論における一般的な定理から直ちに証明することができる．今後の講義内で扱うので楽しみにしていてほしい．

例 6. 上で見たように $\varphi(12) = 4$ なので，

$$[5^4]_{12} = [625]_{12} = [1]_{12} \qquad [7^4]_{12} = [2401]_{12} = [1]_{12} \qquad [11^4]_{12} = [14641]_{12} = [1]_{12}$$

フェルマーの小定理と素数判定. フェルマーの小定理の主張において，p が素数であるという仮定は本質的である．例えば，n が 4 以上の素数でない自然数のとき，a を $\gcd(a, n) > 1$ となる数 (つまり a は n と互いに素でない．例えば a が n の 1 でない約数) とすると，必ず

$$[a^{n-1}]_n \neq [1]_n$$

となる．なぜなら，$[a^{n-1}]_n = [1]_n$ であるとすると，$[a^{n-2}]_n$ が $[a]_n$ の $\times$ に関する逆元であるということになるので，とくに $[a]_n \in (\mathbb{Z}/n\mathbb{Z})^\times$ となるが，これは命題 3.4 に反するためである．これより，以下がわかる．

定理 3.10

2 以上の自然数 n に対し，以下は同値である．

(1) n は素数である．
(2) $1 \leq a \leq n - 1$ なる全ての自然数 a について，$[a^{n-1}]_n = [1]_n$ となる．
(3) $1 \leq q \leq n - 1$ なる全ての素数 q について，$[q^{n-1}]_n = [1]_n$ となる．

証明. (1) と (2) の同値性については，上で述べた通りである．(2) $\Rightarrow$ (3) は自明なので，(3) $\Rightarrow$ (2) のみ示せば良いが，これは，$[a^{n-1}]_n = [1]_n, [b^{n-1}]_n = [1]_n$ のとき，$[(ab)^{n-1}]_n = [1]_n$ となることからわかる． □

定理 3.10 は素数判定に用いることができる．n を 2 以上の自然数とする．$a \in \mathbb{Z}_{>0}$ に対し，

$$[a^{n-1}]_n = [1]_n$$

が成立するとき，n は底 a について**フェルマーテスト**にパスしたという．この言葉を用いれば，n が $1 \leq q \leq n - 1$ なる全ての素数 q についてのフェルマーテストにパスする場合，n は素数であると言える．上で考察したように，n が合成数 (素数でない数) のとき，q が n の約数となる素数である場合 n は底 q について**フェル**

マーテストにパスしない．合成数で，その約数とならない全ての素数についてフェルマーテストにパスする数を**絶対偽素数**，あるいは**カーマイケル数**という．絶対偽素数は小さい方から $561, 1105, 1729, \ldots$ と続き，無限に存在することが知られている．

フェルマーの小定理と RSA 暗号．フェルマーの小定理は **RSA 暗号**と呼ばれる暗号の基本原理にもなっている．これは Ron Rivest, Adi Shamir, Leonard Adleman の 3 名によって 1977 年に考案された公開鍵暗号と呼ばれる暗号の 1 つである．その仕組みをここで簡単に説明しよう．

私が A さんから情報を貰いたいとする．このとき，私は以下のものを準備すればよい．

- (大きな) 相異なる素数 p, q.
- $(p-1)(q-1)$ と互いに素な自然数 e.

ここで，私は A さんに

$$n = pq, e$$

のみを伝える．この 2 つが**公開鍵**と呼ばれる情報になる．それに対して，素数 p と q が**秘密鍵**である．その名の通り，公開鍵は第三者に見られても良い情報，秘密鍵は他の人に見せてはいけない情報である．「$n = pq$ が公開鍵なのだから n を知っていればそれを因数分解すれば p や q がわかるではないか」と思われるかもしれないが，実は p と q が非常に大きな素数の場合，n を因数分解して p, q を見つけるというのはコンピュータでも膨大な時間がかかる問題となる．このため，「実質 n からはわからない」情報になる．このため，もしどんなに大きい整数でもその因数分解が簡単に計算できるようなアルゴリズムが発明されてしまったら，今から説明する暗号は破綻してしまう．

さて，n と e を知った A さんは，1 以上 n 未満の x を私に暗号化して伝えることができる[*5]．それは以下のようにする．

$$[x^e]_n = [r]_n$$

を満たす $0 \leq r < n$ を計算し (つまり x^e を n で割った余り)，その r を私に伝える．

つまり，この r が x を暗号化した数字である．この r から元の x(つまり $\mathbb{Z}/n\mathbb{Z}$ における “e 乗根”) を p, q の情報を知らずに n と e だけを使って計算するのが一般には難しいということがこの暗号の安全性の根拠となっている．さて，p, q の情報を用いてどのように x が計算できるだろうか．これは次のようにすれば良い．$L := (p-1)(q-1)$ とする．まず，$\gcd(e, L) = 1$ だったことを思い出し，拡張ユークリッド互除法 (第 3 回講義資料 2.3 節，系 2.5) を用いて，

$$ed - Lf = 1$$

を満たす整数 (d, f) を求めておく．ここで，第 3 回講義資料 p.6 に述べたこの方程式の一般解の形を見ると，d, f は必ず正の値のもので取れることがわかるので正の値になるように取っておく．このとき，上の r に対し，以下が成立する．

次のように x が復元される．

$$[r^d]_n = [x]_n$$

ここで，x は 1 以上 n 未満としていたので，r^d からただ 1 つに定まることに注意する．

[*5] 「数字じゃなくて文章を送りたい」と思うかもしれないが，その場合は単に文字を数字に対応させれば良いので，問題にはならない．また，ここでは数字の大きさに制限を付けたが，それより大きい数字も数字の桁でいくつかに区切って送れば良いので，送れないというわけではない．

証明. $1 = ed - Lf = ed - (p-1)(q-1)f, d > 0, f > 0$ に注意すると，

$$[r^d]_p = [x^{ed}]_p = [x^{1+(p-1)(q-1)f}]_p = [x]_p([x^{p-1}]_p)^{(q-1)f}$$
$$[r^d]_q = [x^{ed}]_q = [x^{1+(p-1)(q-1)f}]_q = [x]_q([x^{q-1}]_q)^{(p-1)f}$$

ここで，p, q は素数なので，フェルマーの小定理より，$[x^{p-1}]_p = [1]_p, [x^{q-1}]_q = [1]_q$．よって，

$$[r^d]_p = [x]_p \quad \text{かつ} \quad [r^d]_q = [x]_q.$$

このとき，$r^d - x$ は p でも q でも割り切れるということになるので，p, q は相異なる素数であるから，$r^d - x$ は $n = pq$ でも割り切れるということがわかる．よって，

$$[r^d]_n = [x]_n.$$

□

注意 1. ここで，いくつかの注意を述べておこう．

- RSA 暗号において行った操作のみを要約すると，
  - $1 \leq x < n$ を送りたいとき，$[x^e]_n = [r]_n$ $(1 \leq r < n)$ として，r を送信．
  - r を受信した側は $[r^d]_n = [x]_n$ $(1 \leq x < n)$ として，x を復元．

  となる．これを見ると，一旦 d を求めてしまえば，p, q, L はもう使用しないということがわかる．よって，これらは安全に廃棄してしまっても構わない．
- ここでは簡単のために，$L = (p-1)(q-1)$ とおいたが，証明中に用いたのは，e と L が互いに素 ($1 = ed - Lf$ なる $d, f > 0$ が求まる)，L が $p-1, q-1$ で割り切れるという事実のみである．このため，L は $p-1$ と $q-1$ の最小公倍数として取れば問題ない．実際，このようにした方が d としては一般に小さいものが得られるため，最小公倍数を用いて説明されているものも多い．

例 7. $p = 17, q = 31$ としてみよう．このとき，$L = (p-1)(q-1) = 480$ なので，例えば，$e = 37$ ととる．ここで，私は A さんに $n = pq = 527$ と $e = 37$ を伝える (これらは A さん以外に漏れても問題ない)[*6]．一方で，$ed - Lf = 37d - 480f = 1$ を満たす d, f を拡張ユークリッド互除法で求めておく．

$$480 = 12 \times 37 + 36 \qquad 37 = 1 \times 36 + 1$$

であるので，

$$\begin{aligned} 1 &= 37 - 1 \times 36 \\ &= 37 + (-1) \times (480 - 12 \times 37) \\ &= 13 \times 37 + (-1) \times 480 \end{aligned}$$

より，$(d, f) = (13, 1)$ が $37d - 480f = 1$ を満たす整数の組の例である ($d > 0, f > 0$ も成立しているのでこれをそのまま使えば良い)．

さて，A さんが私に 12 という数字を暗号化して送りたかったとしよう．A さんは私から $e = 37$ と聞いているので，12^{37} を

$$12^{37} = 850562249982110214457613168411482993459 2$$

と計算し，これを $n = 527$ で割った余り 241 を私に送信する[*7]．

241 を受け取った私は，先ほど計算した $d = 13$ を用いて，241^{13} を

$$241^{13} = 92517002510467100946797213599 21$$

と計算する．すると，これを $n = 527$ で割った余りを計算することで，12 が復元される．

[*6] 527 の因数分解はすぐに計算できるので，この例は実際の暗号としての意味はない．これはただ様子を説明するための例である．

[*7] ちなみにここではコンピュータを用いて 12^{37} を計算しているが，$[12^{37}]_{527}$ のみ求めればよいので，12^{37} を実際に計算する必要はない．例えば，$12^3 = 1728$ なので，$[12^3]_{527} = [147]_{527}$．$147^2 = 21609$ なので，$[12^6]_{527} = [147^2]_{527} = [2]_{527}$．$2^6 = 64$ なので，$[12^{36}]_{527} = [2^6]_{527} = [64]_{527}$．$64 \times 12 = 768$ なので，$[12^{37}]_{527} = [64 \times 12]_{527} = [241]_{527}$ というようにすれば，普通の電卓でも簡単に計算できる．次の 241^{13} についても同様である．