暗号の数理要綱 #2　　2010–10–14　　河野

1　整数と剰余類

RSA 暗号の理論の基礎には整数に関する理論がある。ここでは整数に関する，重要な定理を証明する。最初に，整数に関するいくつかの定義を行う。

1.1　整数

定義 1.1　(1) a を 0 ではない整数とする。$a = km$ となる整数 k と m が存在する時，k と m は a の**約数** (*divisor*) であると言い，$k|a$, $m|a$ と書く。またこの時，a は k や m の**倍数** (*multiple*) であると言う。k, m は 1 や a 自身でも良い。$a \neq 0$ なので，0 が約数となることはない。$10 = 2 \cdot 5$ なので，10 は 2 や 5 の倍数である。また 2 および 5 は 10 の約数である。$10 = (-1) \cdot (-10)$ なので，10 は -1 や -10 の倍数であり，-1 および -10 は 10 の約数である。

(2) 正の整数を**自然数**という。整数と同じ様に自然数の中でも約数･倍数を定義することができる。10 の約数を自然数の中で考えると，$1, 2, 5, 10$ の 4 個だが，整数の中で考えると $\pm 1, \pm 2, \pm 5, \pm 10$ の 8 個あることに注意すること。

(3) a, b を 0 ではない整数とする。ある整数 k があって，$k|a$, $k|b$ となる時，k を a と b の**公約数** (*common divisor*) という。24 と 36 に対し $24 = 6 \cdot 4, 36 = 6 \cdot 6$ となるので 6 は 24 と 36 の公約数である。

(4) a, b を 0 ではない整数とする。k が a と b の公約数なら，$-k$ も公約数である。a と b の公約数の中で，最大のものを**最大公約数** (*GCD: Greatest Common Divisor*) と言い，(a, b) という記号で表す。1 は必ず公約数となるので，$(a, b) \geqq 1$ である。24 の約数は自然数の中では $1, 2, 3, 4, 6, 8, 12, 24$ の 8 個であり，36 の約数は自然数の中では $1, 2, 3, 4, 6, 9, 12, 18, 36$ の 9 個である。公約数になるのは $1, 2, 3, 4, 6, 12$ である。よって最大公約数は 12 である。即ち $(24, 36) = 12$ である。

(5) a, b を 0 ではない整数とする。$(a, b) = 1$ となる時，a と b は**互いに素** (*relatively prime*) であると言う。$(8, 9) = 1$ なので 8 と 9 は互いに素である。

(6) a, b を 0 ではない整数とする。ある整数 m があって，$a|m$, $b|m$ となる時，m を a と b の**公倍数** (*common multipul*) という。

m が a と b の公倍数なら，$-m$ も公倍数である。kab という形の整数は全て公倍数となるが，公倍数がこのような形になるとは限らない。正の公倍数の中で最小のものを，a と b の**最小公倍数**)(*LCM: Least Common Multiple*) と言う。a と b の最小公倍数を $[a, b]$ で表す。24 の正の倍数は $24, 48, 72, 96, 120, 144, \ldots$ であり，36 の正の倍数は $36, 72, 108, 144, \ldots$ である。144 は 24 と 36 の公倍数であり，72 は 24 と 36 の最小公倍数である。即ち $[24, 36] = 72$ である。

(7) 自分自身と 1 以外に約数を持たない自然数を**素数** (*prime number*) という。素数ではない自然数を**合成数** (*composite number*) という。

(8) 整数全体の集合を $\mathbb{Z}$，自然数全体の集合を $\mathbb{N}$ で表す。「$\dots$」を用いた厳密ではない表現であるが，

$$\mathbb{N} = \{1, 2, 3, \dots\}$$
$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

となる。

次の定理は整数論の基礎になる重要な定理である。

定理 1.2 [**整数の剰余定理**] a を任意の整数，b を任意の自然数とするとき次をみたす整数 q, r が存在する。

$$a = qb + r \qquad (0 \le r < b)$$

このような q, r は一意的 (一通り) である。即ち $a = qb+r$ $(0 \le r < b)$ および $a = q'b+r'$ $(0 \le r' < b)$ となる q, r, q', r' が存在するとき，$q = q'$ かつ $r = r'$ が成立する。

定理 1.3 [**素因数分解の存在と一意性**] n を 2 以上の自然数とする。このとき素数の積に分解できる。即ち素数 $p_1, p_2 \dots, p_k$ と自然数 $e_1, e_2, \dots, e_k$ が存在して

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

となる。またこの分解は一意的 (一通り) である。即ち $p_1, \dots, p_k, q_1, \dots, q_\ell$ を素数，$e_1, \dots, e_k, f_1, \dots, f_\ell$ を自然数とするとき，

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \cdots q_\ell^{f_\ell}$$

が成立するとき，$k = \ell$ であり，$q_1, \dots, q_k$ の順序を適当に入れ替えると (それにともなって $f_1, \dots, f_k$ の順序も入れ替える)，

$$p_1 = q_1, \dots, p_k = q_k, e_1 = f_1 \dots, e_k = f_k$$

が成立する。

これらの定理の証明は (*) 印付きの演習問題にしておく。(*) 印付きの演習問題はすべての学生が解くことを想定してはいない。意欲的にチャレンジしたい学生は説くことを試みて欲しい問題である。以下でててきた場合も同様である。

演習問題 *1.1　定理 1.2 および定理 1.3 を証明せよ。

次の定理はこれからの議論の基礎になる重要な定理である。

定理 1.4 p_1, p_2 を互いに素な２つの整数とすると，

$$k_1 p_1 + k_2 p_2 = 1$$

を満たす整数 k_1, k_2 が存在する。

この定理を示すために次を定義する。

定義 1.5 整数 $\mathbb{Z}$ の部分集合 I が次の性質を満たすとき**イデアル**と呼ぶ。

(1) $I \neq \emptyset$

(2) $\forall m, n \in I \implies m+n \in I$

(3) $\forall a \in \mathbb{Z}\ \forall n \in I \implies an \in I$

n を整数とする。$n\mathbb{Z}$ という集合を

$$n\mathbb{Z} = \{\, nk \mid k \in \mathbb{Z} \,\} = \{\, m \in \mathbb{Z} \mid \exists k \in \mathbb{Z}\ m = nk \,\} = \{\, \ldots, -3n, -2n, -n, 0, n, 2n, 3n, \ldots \,\}$$

で定義する。例えば

$$5\mathbb{Z} = (-5)\mathbb{Z} = \{\, \ldots, -15, -10, -5, 0, 5, 10, 15, \ldots \,\}$$

である。特に $n = 0$ のときは 0 に何をかけても 0 なので，$0\mathbb{Z} = \{\, 0 \,\}$ である。

命題 1.6 n を整数とするとき $n\mathbb{Z}$ はイデアルである。

証明は (*) 印のつかない演習問題とする。

演習問題 1.2　命題 1.6 を証明せよ。

$n\mathbb{Z}$ の形のイデアルを**単項イデアル**という。次の命題が定理の証明のキーポイントになる。

命題 1.7 $\mathbb{Z}$ のイデアルはすべて単項イデアルである。

証明　I を Z のイデアルとする。$I = \{\, 0 \,\}$ のときは $I = 0\mathbb{Z}$ で単項イデアルである。よって $I \neq \{\, 0 \,\}$ としてよい。イデアルの (1) の性質より $m \in I$ となる元 m が存在するが，$m \neq 0$ としてよい。イデアルの性質 (3) より $-m = (-1)m \in I$ なので $m < 0$ のとき，$-m \in I$ であり，$-m > 0$ である。よって I は正の元を含む。I に含まれる正の元で最小なものを n とする。このとき $I = n\mathbb{Z}$ が成立することを示す。

m を任意の整数とするとイデアルの性質 (3) より $mn \in I$ となる。よって $n\mathbb{Z} \subseteq I$ が成立する。a を I の任意の元とする割り算の可能性 (定理 1.2) より整数 q, r で

$$a = qn + r \qquad (0 \leq r < n)$$

を満たすものが存在する。このとき $r = a + (-q)n$ であり，イデアルの性質 (3) から $(-q)n \in I$ である。また $a \in I$ なのでイデアルの性質 (2) より $r = a + (-q)n \in I$ である。今 $r \neq 0$ と仮定すると，$r \in I$ であり，$0 < r < n$ である。n は I に含まれる正の最小元としたのでこれは矛盾である。$r \neq 0$ の仮定が不合理だったので，$r = 0$ となる。即ち $a = qn$ となり，$I \subseteq n\mathbb{Z}$ が示された。以上により $I = n\mathbb{Z}$ となり I は単項イデアルである。 ∎

定理 1.4 の証明：　命題 1.7 を用いると定理 1.4 が証明できる。$I = \{\, n_1p_1 + n_2p_2 \mid n_1, n_2 \in \mathbb{Z} \,\}$ とおくとき，I がイデアルであることを示す。$n_1 = 1, n_2 = 0$ とすると $p_1 = 1 \cdot p_1 + 0 \cdot p_2 = n_1p_1 + n_2p_2 \in I$ なので $I \neq \emptyset$ となりイデアルの性質 (1) を満たす。$a \in I$ とすると整数 n_1, n_2 が存在して $a = n_1p_1 + n_2p_2$ と書ける。$b \in I$ とすると整数 m_1, m_2 が存在して $b = m_1p_1 + m_2p_2$ と書ける。$a + b = (n_1 + m_1)p_1 + (n_2 + m_2)p_2$ となるので $a + b \in I$ となりイデアルの性質 (2) も

満たす。$a = n_1p_1 + n_2p_2 \in I$，$m \in \mathbb{Z}$ とすると $ma = (mn_1)p_1 + (mn_2)p_2$ となるので $ma \in I$ となりイデアルの性質 (3) も満たす。よって I はイデアルである。命題 1.7 よりある整数 d を用いて $I = d\mathbb{Z}$ と書けている。負だったら $-d$ をとることにより，$d > 0$ としてよい。$d = 1$ のとき $1 \in I$ よりある整数 k_1, k_2 を用いて $1 = k_1p_1 + k_2p_2$ と書けるので証明が終わる。よって $d > 1$ を仮定する。$p_1 \in I$ より $p_1 \in d\mathbb{Z}$ となるので，p_1 は d の倍数である。$p_2 \in I$ より $p_2 \in d\mathbb{Z}$ となるので，p_2 は d の倍数である。d は p_1 と p_2 の公約数になるが，これは互いに素ということに矛盾する。この場合はないので証明が終わる。 ∎

定理 1.4 を用いると次が証明できる。

定理 1.8 最大公約数が d であるような整数 a, b に対し，

$$k_1a + k_2b = d$$

を満たす整数 k_1, k_2 が存在する。

証明　d を a, b の最大公約数とすると，$a = a_1d, b = b_1d$ となる整数 a_1, b_1 が存在する。a_1, b_1 が互いに素でなければ，さらに約数が存在して d が最大公約数ということに反するので，a_1 と a_2 は互いに素である。a_1 と b_1 に定理 1.4 を適用すると，整数 k_1, k_2 が存在して $k_1a_1 + k_2b_1 = 1$ となる。よって

$$k_1a + k_2b = k_1a_1d + k_2b_1d = (k_1a_1 + k_2b_1)d = 1 \cdot d = d$$

となり証明される。 ∎

定理 1.4 は 2 個以上の場合にも成立する。

定理 1.9 $p_1, \cdots, p_n$ を 1 と 0 ではない整数とし，1 以外の共通の約数を持たないとする。すなわち，ある 0, 1 ではない整数 d で $d|p_1, \cdots, d|p_n$ となるようなものは存在しないとする。

この時，ある整数 $k_1, \cdots, k_n$ が存在して，

$$k_1p_1 + \cdots + k_np_n = 1$$

となる。

証明

$$H = \{\ m_1p_1 + \cdots + m_np_n \mid m_i \in \mathbb{Z}\ (i = 1, \cdots, n)\ \}$$

とおく。すなわち，これは $p_1, \cdots, p_n$ の整数倍の和を全て集めたもので，前と同様にイデアルになることが分かる。

命題 1.7 より，ある正の整数 m があって，$H = m\mathbb{Z}$ となっている。

これは，H の全ての元は m の整数倍になるということを意味している。すなわち，$p_1, \cdots, p_n$ は全て m の整数倍となる。仮定より，$p_1, \cdots, p_n$ は 1 以外の共通の約数を持たないので，$m = 1$ でなければならない。

$H = \mathbb{Z}$ となるので，$1 \in H$ である。すなわち，$k_1p_1 + \cdots + k_np_n = 1$ となるような整数 $k_1, \cdots, k_n$ が存在する。 ∎

注意： $k_1p_1 + k_2p_2 = 1$ を満たす整数 k_1, k_2 は，一意的に決まるわけではない。例えば，m を任意の整数とした時，

$$1 = k_1p_1 + k_2p_2 = k_1p_1 + k_2p_2 + mp_1p_2 - mp_1p_2 = (k_1 + mp_2)p_1 + (k_2 - mp_1)p_2$$

である。すなわち，

$$k_1' = k_1 + mp_2 \qquad k_2' = k_2 - mp_1$$

も同じ性質を持つ。

逆に，$k_1p_1 + k_2p_2 = 1$, $k_1'p_1 + k_2'p_2 = 1$ を満たす整数 k_1, k_2, k_1', k_2' があったとすると，$(k_1' - k_1)p_1 + (k_2' - k_2)p_2 = 0$ であるから，

$$(k_1' - k_1)p_1 = -(k_2' - k_2)p_2$$

である。p_1 と p_2 は互いに素であるから，$p_2|(k_1' - k_1)$, $p_1|(k_2' - k_2)$ でなければならない。すなわち，ある整数 m_1, m_2 があって，$k_1' - k_1 = m_1p_2$, $k_2' - k_2 = m_2p_1$ となっている。

$$(k_1 + m_1p_2)p_1 + (k_2 + m_2p_1)p_2 = 1$$

であるが，$k_1p_1 + k_2p_2 = 1$ より，$m_1p_2p_1 + m_2p_1p_2 = (m_1 + m_2)p_1p_2 = 0$ であるから，$m_1 = -m_2$ でなければならない。

以上から，次のことがわかった。

命題 1.10 p_1, p_2 を互いに素な２つの整数とし，k_1, k_2 を

$$k_1p_1 + k_2p_2 = 1$$

を満たす整数とする。ある整数 k_1', k_2' で $k_1'p_1 + k_2'p_2 = 1$ となるならば，ある整数 m があって，

$$k_1' = k_1 + mp_2 \qquad k_2' = k_2 - mp_1$$

となっている。

演習問題 1.3

(1) 1680 の正の約数をすべて求めよ。　(2) 240 と 360 の最大公約数を求めよ。
(3) 240 と 360 の最小公倍数を求めよ。　(4) 589 と 703 の最大公約数を求めよ。
(5) $k_1179 + k_289 = 1$ を満たす k_1, k_2 を 1 組見つけよ。