暗号の数理問題解説 #2

河野

演習問題 *1.1　定理 1.2 および定理 1.3 を証明せよ。

最初に定理 1.2 を証明する。最初に定理のような整数 q, r が存在することを示す。

a が 0 以上のとき b を 1 倍，2 倍，3 倍，$\cdots$ としていくといつかは a より大きくなる。よって $k+1$ を $a < (k+1)b$ となる最小の整数とすると，$kb \leqq a < (k+1)b$ が成立する。a が負のとき b を -1 倍，-2 倍，-3 倍，$\cdots$ としていくといつかは a 以下になる。よって k を $kb \leqq a$ となる最大の整数とすると $kb \leqq a < (k+1)b$ が成立する。いずれの場合もある k が存在して

$$kb \leqq a < (k+1)b$$

が成立する。このとき $q = k$，$r = a - qb$ とおき，不等式に代入すると $qb \leqq qb + r < qb + b$ となる。よって

$$0 \leqq r < b$$

が成立する。

次にこのような q, r が一意的であることを示す。そのためには q, r および q', r' が

$$a = qb + r \quad (0 \leq r < b) \qquad a = q'b + r' \quad (0 \leq r' < b)$$

を満たすとき $q = q'$ かつ $r = r'$ が成立することを示せばよい。$q \neq q'$ が成立すると仮定する。$q > q'$ または $q' > q$ が成立するが，$q > q'$ の場合を考える。$qb + r = q'b + r'$ より $(q - q')b = r' - r$ が成立する。$r' < b$ かつ $0leqr$ より $r' - r < b$ が成立する。また $q - q' > 0$ より $q - q' \geq 1$ が成立する。よって

$$b > r' - r = (q - q')b \geq b$$

となり矛盾，よって $q = q'$ である。このとき $r = r'$ となる。$q < q'$ のときも同様に証明できる。

次に定理 1.3 を証明する。最初に存在を示す。即ち命題『 n を 2 以上の自然数とする。素数 $p_1, p_2 \ldots, p_k$ と自然数 $e_1, e_2, \ldots, e_k$ が存在して

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

となる。』を示す。証明は数学的帰納法で行われる。$n = 2$ の場合を考える。2 は素数なので 1 個の積に「分解」しているので成立する。m より小さい自然数 n について命題が成立することを仮定する。このとき $n = m$ に対し命題が成立することを示す。

m が素数の場合と素数でない場合に分ける。m が素数のときは 1 個の積に分解しているので成立している。m が素数でないときを考える。素数ではないので $1, m$ 以外の約数 a が存在する。即ち，1 より大きい自然数 a, b が存在して

$$m = ab$$

と書けている。このとき $a < m$ かつ $b < m$ が成立している。m より小さい自然数に対して命題は成立しているので，a および b は素数の積で表される。即ち素数 $q_1, q_2, \ldots, q_k, q_{k+1}, q_{k+2}, \ldots, q_t$ が存在して

$$a = q_1 q_2 \cdots q_k \qquad b = q_{k+1} q_{k+2} \cdots q_t$$

となっている。このとき

$$m = ab = q_1 q_2 \cdots q_k q_{k+1} q_{k+2} \cdots q_t$$

となっている。同じ素数をひとまとめにしてそれを $p_1, p_2, \ldots, p_k$ とすると

$$m = ab = q_1 q_2 \cdots q_k q_{k+1} q_{k+2} \cdots q_t = p_1^{e_1} p_2^{2_2} \cdots p_k^{e_k}$$

と書ける。よって m のときも命題が成立する。数学的帰納法により証明された。

一意性を証明するため次の命題を使用する。

『p を素数 a, b を自然数とするとき $p|ab \implies p|a$ または $p|b$ が成立する』

この命題が正しくないとすると反例が存在する。a, b がその反例とすると，$a = kp + a', b = k'p + b'$ とおくと a', b' も反例になる。よって最初から $0 < a < p, 0 < b < p$ としてよい。b を固定した中で a が最小になるものを選ぶ。$p = qa + a'$ とする。$a' \neq 0$ なら a', b が反例になり最小性に反する。よって $a' = 0$ である。$p = qa$ なので $a = 1$ または $a = p$ である。$a = p$ なら $0 < a < p$ に反する。$a = 1$ なら $p|ab = b$ なので $0 < b < p$ に反する。いずれにしろ矛盾。よって命題が正しくないとした仮定が間違っているので，命題は証明された。

この命題を用いると一意性が証明させる。

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

が成立しているとする。この等式の左辺は p_1 で割り切れるので右辺も p_1 で割り切れる。命題を繰り返し適用することにより，ある q_i が存在して $p_1|q_i$ が成立する。必要なら積の順序を入れ替えることにより $q_i = q_1$ としてよい。$p_1|q_1$ のとき，p_1, q_1 ともに素数なので $p_1 = q_1$ である。よって両辺を p_1 で割ると

$$p_1^{e_1 - 1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1 - 1} q_2^{f_2} \cdots q_\ell^{f_\ell}$$

が得られる。$e_1 - 1 > 0$ なら同様のことを続けることにより

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

が得られる。この等式の左辺が p_2 で割り切れるので p_1 のときと同様に考えると

$$p_3^{e_3} \cdots p_k^{e_k} = q_1^{f_1 - e_1} p_2^{f_2 - e_2} q_3^{f_3} \cdots q_\ell^{f_\ell}$$

が得られる。このことを p_k まで実行すると

$$1 = q_1^{f_1 - e_1} p_2^{f_2 - e_2} \cdots p_k^{f_k - e_k} q_{k+1}^{f_{k+1}} \cdots q_\ell^{f_\ell}$$

が得られる。この等式が成立するためには $k = el$ かつ $e_1 = f_1, e_2 = f_2, \ldots, e_k = f_k$ が必要である。よって一意性が示された。

演習問題 1.2　命題 1.6 を証明せよ。

定義 1.5 の 3 つの条件が満たされていることを示せばよい。$0 = n \cdot 0$ なので $0 \in n\mathbb{Z}$ である。よって (1) は満たされている。$\forall a, b \in n\mathbb{Z}$ に対し $a = nk, b = n\ell$ $(k, \ell \in \mathbb{Z})$ と表すことができる。$a + b = nk + n\ell = n(k + \ell)$ であり，$k + \ell \in \mathbb{Z}$ なので $a + b \in n\mathbb{Z}$ である。よって (2) も成立する。$\forall a \in n\mathbb{Z}, \forall m \in \mathbb{Z}$ に対し $a = nk$ $(k \in \mathbb{Z})$ と書けるので $ma = m(nk) = n(mk)$ $(mk \in \mathbb{Z})$ となる。よって (3) も成立する。

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) $k_1 79 + k_2 89 = 1$ を満たす k_1, k_2 を 1 組見つけよ。

(1) $1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$ なので，1680 の約数は $2^a 3^b 5^c 7^d$ $(a \leqq 4, b \leqq 1, c \leqq 1, d \leqq 1)$ という形をしている。

$$1, 2, 2^2, 2^3, 2^4, \qquad 1 \cdot 3, 2 \cdot 3, 2^2 \cdot 3, 2^3 \cdot 3, 2^4 \cdot 3$$

$$1 \cdot 5, 2 \cdot 5, 2^2 \cdot 5, 2^3 \cdot 5, 2^4 \cdot 5, \qquad 1 \cdot 7, 2 \cdot 7, 2^2 \cdot 7, 2^3 \cdot 7, 2^4 \cdot 7$$

$$1 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 5, 2^2 \cdot 3 \cdot 5, 2^3 \cdot 3 \cdot 5, 2^4 \cdot 3 \cdot 5 \qquad 1 \cdot 3 \cdot 7, 2 \cdot 3 \cdot 7, 2^2 \cdot 3 \cdot 7, 2^3 \cdot 3 \cdot 7, 2^4 \cdot 3 \cdot 7$$

$$1 \cdot 5 \cdot 7, 2 \cdot 5 \cdot 7, 2^2 \cdot 5 \cdot 7, 2^3 \cdot 5 \cdot 7, 2^4 \cdot 5 \cdot 7 \qquad 1 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7, 2^2 \cdot 3 \cdot 5 \cdot 7, 2^3 \cdot 3 \cdot 5 \cdot 7, 2^4 \cdot 3 \cdot 5 \cdot 7$$

(2) $GCD(240, 360) = 120$

(3) $LCM(240, 360) = 720$ ：$GCD(a, b) \cdot LCM(a, b) = ab$ を知っていれば計算は少し楽かもしれない。

(4) $GCD(589, 703) = 19$ ：2, 3, . . . と順に割り算を実行していってもできるが，「ユークリッドの互除法」を知っていると少し楽かも。$703 = 589 \cdot 1 + 114$ となるので 589 を 114 で割る。$589 = 114 \cdot 5 + 19$ なので 114 を 19 で割る。$114 = 19 \cdot 6$ となるので 19 が最大公約数である。この方法については後のセクションで取り扱う。

(5) $(-9) \cdot 79 + 8 \cdot 89 = 1$ であるが，問題はどうやって見つけるかである。総当たりで考えていってもできるが，数が大きくなると大変である。次の様な方法を考える (これは拡張ユークリッドアルゴリズム呼ばれるもので後で取り扱う)。

$89 = 79 \cdot 1 + 10$ なので

$$79k_1 + 89k_2 = 79k_1 + (79 \cdot 1 + 10)k_2 = 79(k_1 + k_2) + 10k_2$$

となる。ここで $k_3 = k_1 + k_2$ とおくと式は $10k_2 + 79k_3$ となる。$79 = 7 \cdot 10 + 9$ なので

$$10k_2 + 79k_3 = 10k_2 + (7 \cdot 10 + 9)k_3 = 10(7k_3 + k_2) + 9k_3$$

となる。$k_4 = 7k_3 + k_2$ とおくと $9k_3 + 10k_4$ となる。$10 = 9 \cdot 1 + 1$ なので

$$9k_3 + 10k_4 = 9k_3 + (9 \cdot 1 + 1)k_4 = 9(k_3 + k_4) + k_4$$

となる。この式は最初の式と等しいので，これが 1 になるように k_3, k_4 を定めるには $k_4 = 1, k_3 + k_4 = 0$ となるように定めればよい。よって $k_4 = 1, k_3 = -1$ とする。このとき $k_2 = k_4 - 7k_3 = 1 - 7(-1) = 8$ であり，$k_1 = k_3 - k_2 = -1 - 8 = -9$ となる。よって $k_1 = -9, k_2 = 8$ を得る。