暗号の数理問題解説 #6

河野

演習問題 3.1　a, b を正の整数とする。このとき最大公約数と最小公倍数の積は ab である事，即ち $(a,b)\cdot[a,b] = a\cdot b$ が成立することを示せ。

ここでは素因数分解の存在と一意性 (自然数が素数の積に一通りに分解される) は認めることとする。a と b が互いに素であるとき，最小公倍数が ab になることは素因数分解の一意性より従う。

a と b の最大公約数を x とすると，自然数 a_1, b_1 が存在して $a = xa_1$，$b = xb_1$ と書ける。a_1 と b_1 の最大公約数が 1 より大きいならば x が最大公約数ということに反する。よって a_1 と b_1 は互いに素である。y を a と b の最小公倍数とすると，y は x で割り切れる。$y_1 = \dfrac{y}{x}$ とおくと y_1 は a_1 と b_1 の公倍数であり，しかも最小公倍数であり，$y_1 = a_1b_1$ となる。よって

$$xy = x x\frac{y}{x} = xxy_1 = xxa_1b_1 = xa_1\cdot xb_1 = ab$$

となる

演習問題 3.2

(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)　1 を約数に入れないなら $2, 3, 5, 7$ である。
(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)　$GCD(589, 703) = 19$：$2, 3, \ldots$ 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。