RSA 暗号の鍵生成で e から d を求める計算例（教科書 p105）

例として $p = 5, q = 11$ とし，暗号化鍵 $e = 3$ から復号化鍵 d を求める手順を示す．e, d, p, q は

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

を満たす.

$$ed = 1 + k \cdot (p-1)(q-1)$$

だから

$$d \cdot e + j \cdot (p-1)(q-1) = 1$$

つまり，$u = e$, $v = (p-1)(q-1)$ としてをユークリッド互除法を行えばよい．教科書 p.8 では $u > v$ とする，とあるが $u \leq v$ でも正しく動作する．

S1)

$$(u_1, u_2, u_3) = (1, 3, 0), (v_1, v_2, v_3) = (0, 40, 1)$$

S2.1)

$$w = \lfloor u_2/v_2 \rfloor = 0$$

$$(t_1, t_2, t_3) = (u_1, u_2, u_3) - (v_1, v_2, v_3)w = (1, 3, 0)$$

$$(u_1, u_2, u_3) = (v_1, v_2, v_3) = (0, 40, 1)$$

$$(v_1, v_2, v_3) = (t_1, t_2, t_3) = (1, 3, 0)$$

S2.2)

$$w = \lfloor u_2/v_2 \rfloor = 13$$

$$(t_1, t_2, t_3) = (u_1, u_2, u_3) - (v_1, v_2, v_3)w = (-13, 1, 1)$$

$$(u_1, u_2, u_3) = (v_1, v_2, v_3) = (1, 3, 0)$$

$$(v_1, v_2, v_3) = (t_1, t_2, t_3) = (-13, 1, 1)$$

S2.3)

$$w = \lfloor u_2/v_2 \rfloor = 3$$

$$(t_1, t_2, t_3) = (u_1, u_2, u_3) - (v_1, v_2, v_3)w = (40, 0, -3)$$

$$(u_1, u_2, u_3) = (v_1, v_2, v_3) = (-13, 1, 1),$$

$$(v_1, v_2, v_3) = (t_1, t_2, t_3) = (40, 0, -3)$$

S2 の各ステップで

$$u_1 u + u_3 v = u_2, v_1 u + v_3 v = v_2$$

が成立していることを確認すると計算ミスが防げる．

ユークリッド互除法により $gcd(3, 40) = 1$ を得たので最大公約数が 1，すなわち $e = 3$ と $(p-1)(q-1) = 40$ が互いに素であることがわかり，$-13 \cdot 3 + 1 \cdot 40 = 1$ も同時に得られた．

$$-13 \cdot 3 + 1 \cdot 40 = 1$$

$$-13 \cdot 3 = 1 + k \cdot 40 \ (k \text{ は整数})$$

の形なので，$e = 3$, $p = 5$, $q = 11$ のとき

$$ed \equiv 1 \pmod{(p-1)(q-1)}$$

になる整数 d として -13 が得られた（$3 \cdot (-13) = -39 \equiv 1 \pmod{40}$ が成り立つ）が，負の数なのでこのままでは復号鍵として使えない．ユークリッド互除法により得られた

$$-13 \cdot 3 + 1 \cdot 40 = 1$$

の第 1 項に $40 \cdot 3$ を加え，第 2 項から同じ $3 \cdot 40$ を減ずる．

$$27 \cdot 3 - 2 \cdot 40 = 1$$

が成り立つので $e = 3$ のとき $ed \equiv 1 \pmod{(p-1)(q-1)}$ になる数として $d = 27$ が使えることがわかる．これを復号鍵とする．(d を求めるためだけであれば u_3, v_3, t_3 は不要)