演習問題

$p = 7,\ q = 13$と、相異なる素数をとり、 $n = pq = 91$で RSA 暗号を考える。
以下の問に答えよ。

1. $(n, e) = (91, 5)$は公開鍵となることを示せ。
2. 上で示した公開鍵(n, e)に対する秘密鍵dを決定せよ。

解答 ：

解答例:

1.

$e = 5$が、$(p-1)(q-1) = 6 \times 12 = 72$と互いに素であればよい。

両者の最大公約数は 1 より、互いに素。

よって、(n, e)は公開鍵となる。

2.

$n_0 = (p-1)(q-1) = 72,\ n_1 = e = 5$として拡張ユークリッド互除法を適用すると

i	n_i	q_i	x_i	y_i
0	72		1	0
1	5	14	0	1
2	2	2	$x_0 - q_1 x_1 = 1$	$y_0 - q_1 y_1 = -14$
3	1	2	$x_1 - q_2 x_2 = -2$	$y_1 - q_2 y_2 = 29$
4	0			

となり、$i = 3$の行に着目して

$$1 = (-2) \times 72 + 29 \times 5$$

式変形すると

$$5 \times 29 = 2 \times 72 + 1$$

これより、

$$5 \times 29 \equiv 1 \ (mod\ 72)$$

求めるべきは、$ed \equiv 1 \left(mod\ (p-1)(q-1)\right)$ を満たすdであるから、

秘密鍵dは、$d = 29$とすればよい。