

# 数学アラカルト(問題解答)

## 第2回 公開鍵暗号の仕組み

問題 1. (1) 2 (2) 4 (3) 6 (4) 2

問題 2. (1) 6 個, 和 3 (2) 8 個, 和 4 (3) 10 個, 和 5 (4) 12 個, 和 6

問題 3. (1)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(2)

×	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

(3)

×	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

×	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

問題 4. (1)  $d = 61$  (2)  $d = 35$  (3)  $d = 103, q = 29$  (4)  $d = 185$

((3), (4)で  $L = \text{lcm}(22, 28) = 308$ )

問題 5. (1) 暗号文  $b = 175$  (2) 暗号文  $b = 109$  (3) 秘密鍵  $d = 7$ , 平文  $a = 147$  ( $L = \text{lcm}(10, 16) = 80$ )