

—— オイラーの関数 ——

$\{1, 2, \dots, n\}$ の中で n と互いに素である数の個数を $\phi(n)$ で表し、 ϕ をオイラーの関数という。

例えば、 $\{1, 2, 3, 4, 5, 6\}$ の中で 6 と互いに素なのは 1, 5 の 2 個であるから、 $\phi(6) = 2$ である。また、 $\{1, 2, 3, 4, 5, 6, 7\}$ の中で 7 以外は全て 7 と互いに素だから、 $\phi(7) = 6$ である。

一般に、素数 p に対して、 $\phi(p) = p - 1$ が成り立つ。なぜなら、 $\{1, 2, 3, \dots, p\}$ の中で p 以外は全て p と互いに素であるからである。

また、異なる素数 p, q に対して、 $\phi(pq) = (p - 1)(q - 1)$ が成り立つ。なぜなら、 $\{1, 2, 3, \dots, pq\}$ の中で、 p の倍数は $p, 2p, 3p, \dots, (q - 1)p, qp$ の q 個、 q の倍数は $q, 2q, 3q, \dots, (p - 1)q, pq$ の p 個、 p と q の公倍数は pq の 1 個であるから、 $\phi(pq) = pq - (p \text{ の倍数}) - (q \text{ の倍数}) + (p \text{ と } q \text{ の公倍数}) = pq - q - p + 1 = p(q - 1) - (q - 1) = (p - 1)(q - 1)$ となるからである。

—— RSA 暗号 ——

鍵の生成 自然数 n, e, d を次の (1), (2), (3) をみたすようにとる。

- (1) 異なる素数 p, q により、 $n = pq$
- (2) $\phi(n) = (p - 1)(q - 1)$ と互いに素な e
- (3) $ed \equiv 1 \pmod{\phi(n)}$ となる d

暗号化 自然数に変換した平文 x に対し、 $y \equiv x^e \pmod{n}$ ($0 \leq y < n$) となる暗号文 y を求める。

復号化 暗号文 y に対して、 $z \equiv y^d \pmod{n}$ ($0 \leq z < n$) となる z を求める。 z はもとの平文 x に一致する。

ここで、 n, e は暗号化鍵（公開鍵）で、 d （または p, q ）は複合化鍵（秘密鍵）である。

例えば、 $p = 3, q = 11$ とし、平文 $x = 7 \ 13 \ 17 \ 24$ を RSA 暗号により暗号化してみよう。下記の表は、1 から 32 までの数の、1 から 21 までのべき乗を求め、33 を法として求めたものである。

鍵の生成 自然数 n, e, d を次の (1), (2), (3) をみたすようにとる。

- (1) $n = 3 \times 11 = 33$
- (2) $\phi(3 \times 11) = (3 - 1)(11 - 1) = 20$ と互いに素な e を 3 とする。
- (3) $3d \equiv 1 \pmod{20}$ となる $d = 7$

暗号化 自然数に変換した平文 x に対し、

- $y \equiv 7^3 \equiv 13 \pmod{33}$ ($0 \leq y < 33$)
- $y \equiv 13^3 \equiv 19 \pmod{33}$ ($0 \leq y < 33$)
- $y \equiv 17^3 \equiv 29 \pmod{33}$ ($0 \leq y < 33$)

復号

暗号化

べき乗数

この世界の数

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	2	4	8	16	32	31	29	25	17	1	2	4	8	16	32	31	29	25	17	1	2
3	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3	9	27	15	12	3
4	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4	16	31	25	1	4
5	5	25	26	31	23	16	14	4	20	1	5	25	26	31	23	16	14	4	20	1	5
6	6	3	18	9	21	27	30	15	24	12	6	3	18	9	21	27	30	15	24	12	6
7	7	16	13	25	10	4	28	31	19	1	7	16	13	25	10	4	28	31	19	1	7
8	8	31	17	4	32	25	2	16	29	1	8	31	17	4	32	25	2	16	29	1	8
9	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9	15	3	27	12	9
10	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10	1	10
11	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11	22	11
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
13	13	4	19	16	10	31	7	25	28	1	13	4	19	16	10	31	7	25	28	1	13
14	14	31	5	4	23	25	20	16	26	1	14	31	5	4	23	25	20	16	26	1	14
15	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15	27	9	3	12	15
16	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16	25	4	31	1	16
17	17	25	29	31	32	16	8	4	2	1	17	25	29	31	32	16	8	4	2	1	17
18	18	27	24	3	21	15	6	9	30	12	18	27	24	3	21	15	6	9	30	12	18
19	19	31	28	4	10	25	13	16	7	1	19	31	28	4	10	25	13	16	7	1	19
20	20	4	14	16	23	31	26	25	5	1	20	4	14	16	23	31	26	25	5	1	20
21	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21	12	21
22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22	22
23	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23	1	23
24	24	15	30	27	21	9	18	3	6	12	24	15	30	27	21	9	18	3	6	12	24
25	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25	31	16	4	1	25
26	26	16	20	25	23	4	5	31	14	1	26	16	20	25	23	4	5	31	14	1	26
27	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27	3	15	9	12	27
28	28	25	7	31	10	16	19	4	13	1	28	25	7	31	10	16	19	4	13	1	28
29	29	16	2	25	32	4	17	31	8	1	29	16	2	25	32	4	17	31	8	1	29
30	30	9	6	15	21	3	24	27	18	12	30	9	6	15	21	3	24	27	18	12	30
31	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31	4	25	16	1	31
32	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32	1	32

図 1: RSA 暗号の世界 <http://www.maitou.gr.jp/rsa/rsa10.php> より引用

- $y \equiv 24^3 \equiv 30 \pmod{33} \ (0 \leq y < 33)$

となる暗号文 $y = 13 \ 19 \ 29 \ 30$ を求める。

復号化 暗号文 y に対して、

- $z \equiv 13^7 \equiv 7 \pmod{33} \ (0 \leq z < 33)$
- $z \equiv 19^7 \equiv 13 \pmod{33} \ (0 \leq z < 33)$
- $z \equiv 29^7 \equiv 17 \pmod{33} \ (0 \leq z < 33)$
- $z \equiv 30^7 \equiv 24 \pmod{33} \ (0 \leq z < 33)$

となる $z = 7 \ 13 \ 17 \ 24$ を求める。 z はもとの平文 x に一致する。

ここで、暗号化鍵 $n = 33$ と $e = 3$ のみ公開する。(複合化鍵 $d = 7$ (または、 $p = 3, q = 11$) は秘密にする。)そして、暗号文 $y = 13 \ 19 \ 29 \ 30$ を送信する。複合化鍵 $d = 7$ は相手しか知らないので、他の人は暗号文から平文に複合することはできない。

RSA 暗号は、二つの素数 p, q から $n = pq$ を求めることは易しいが、 n から p, q を求めることは難しいことが、安全性の基となっている。安全性の為に、300 桁以上の n を用いることが推奨されている。

問題

暗号化鍵を $n = 133$, $e = 5$ とする。

暗号文が $y = 44, 13, 91, 13$ のとき、元の平文 z を求めよ。