解答例

STEP III 1987、第 5 問

純粋数学 ・ 合同算術による暗号

> **STEP III 1987、問 5**
>
> 先に進む前に、まず問題を読んでおこう。問題は STEP Support Programme の問題データベースにある：
>
> step.maths.org/questions/87-s3-q5

鍵となる考え方

この暗号は 2 つの独立したシフト暗号（shift cipher）からなる。偶数番目の位置に対するもの（鍵 n_0）と奇数番目の位置に対するもの（鍵 n_1）であり、どちらにもさらに j だけのずらしが加わっている。まず既知のずらし j を取り除く。すると残るのは、メッセージのそれぞれの半分が 1 つの未知の定数だけずらされたものである。法 50 でのずらしは全単射（bijection）なので、等しい数は等しいまま、異なる数は異なるままに保たれる。3 つある 43 が手がかりとなって n_0 が判明する。その後、法 50 での和をとることで n_1 が定まる。

解答

n_0 と n_1 は法 50 での値だけが意味をもつので、$0 \le n_0, n_1 \le 49$ とする。各 a_k は 0 以上 49 以下であるから、法 50 での剰余（residue）がわかれば a_k は一意に定まる。

既知のずらしを取り除く

偶数番目の位置について、$j = 1, \ldots, 6$ に対して $c_j = b_{2j} - j$ とおく。奇数番目の位置について、$j = 0, \ldots, 5$ に対して $d_j = b_{2j+1} - j$ とおく。このとき

$$a_{2j} \equiv c_j - n_0, \qquad a_{2j+1} \equiv d_j - n_1 \pmod{50}.$$

暗号化されたメッセージから次が得られる。

j	1	2	3	4	5	6
b_{2j}	27	36	35	40	37	48
c_j	26	34	32	36	32	42

j	0	1	2	3	4	5
b_{2j+1}	35	2	15	8	40	24
d_j	35	1	13	5	36	19

n_0 を求める

法 50 で一定の n を引く操作は一対一（one-to-one）である。したがって、偶奇が同じ 2 つの位置の a が等しいのは、対応する c（または d）が等しいとき、かつそのときに限る。

考えてみよう 3 つの 43 はどの位置に入りうるか。

6 個の d_j はすべて異なるので、奇数番目の位置には 6 個の異なる数が入り、そのうち 43 は高々 1 個である。よって少なくとも 2 個の 43 は偶数番目の位置にある。c_j の中で重複しているのは 32 だけであり、それはちょうど 2 回（$j = 3, 5$）現れる。したがって偶数番目の位置にはちょうど 2 個の等しい数が入り、メッセージ中で 2 回以上現れる数は 43 だけなので、それらは 2 個の 43 でなければならない。ゆえに

$$32 - n_0 \equiv 43 \pmod{50} \quad \Longrightarrow \quad n_0 \equiv -11 \equiv 39 \pmod{50}.$$

すると $a_{2j} \equiv c_j - 39 \equiv c_j + 11$ であり、$42 + 11 = 53 \equiv 3$ であるから

$$(a_2, a_4, a_6, a_8, a_{10}, a_{12}) = (37, 45, 43, 47, 43, 3),$$

が得られる。6 個とも、当然そうあるべきとおり、メッセージ中に含まれている。

n_1 を求める

メッセージからこれら 6 個の数を取り除くと、奇数番目の位置の数

$$S = \{1, 7, 23, 24, 39, 43\},$$

が残る。よって $\{d_j - n_1\}$ は法 50 で S に一致しなければならない。

考えてみよう 50 通りの値をすべて試さずに n_1 を求めるにはどうすればよいか。

両辺の総和をとる。2 つの集合が一致するなら、その和は法 50 で一致する。

$$\sum d_j - 6n_1 \equiv \sum_{s \in S} s \pmod{50}, \qquad \text{すなわち} \qquad 109 - 6n_1 \equiv 137.$$

よって $6n_1 \equiv -28 \equiv 22 \pmod{50}$ である。法も割り切る 2 で全体を割ると $3n_1 \equiv 11 \pmod{25}$ となる。$3 \times 17 = 51 \equiv 1$ であるから、$n_1 \equiv 11 \times 17 = 187 \equiv 12 \pmod{25}$ を得る。したがって $n_1 = 12$ または $n_1 = 37$ である。

和の条件は必要条件であるが十分条件ではないので、両方の値を確かめる。$n_1 = 37$ のとき $d_0 - 37 = -2 \equiv 48$ となり、これはメッセージに含まれないので $n_1 = 37$ は不

適である。$n_1 = 12$ のとき

$$(a_1, a_3, a_5, a_7, a_9, a_{11}) \equiv (23,\ -11,\ 1,\ -7,\ 24,\ 7) \equiv (23,\ 39,\ 1,\ 43,\ 24,\ 7),$$

となり、これはちょうど S である。よって $n_1 = 12$ である。

メッセージ

2 つの半分を交互に並べると、元のメッセージは

$$23,\ 37,\ 39,\ 45,\ 1,\ 43,\ 43,\ 47,\ 24,\ 43,\ 7,\ 3,$$

であり、$n_0 \equiv 39$、$n_1 \equiv 12 \pmod{50}$ である。以上の議論から、この答えが唯一であることがわかる。n_0 は必然的に定まり、n_1 の 2 つの候補のうち条件を満たすのは 1 つだけだったからである。

検算

答えを再び暗号化してみる。たとえば $b_{12} \equiv a_{12} + 39 + 6 = 48$、$b_7 \equiv a_7 + 12 + 3 = 58 \equiv 8$ であり、どちらも正しい。コンピュータで 2500 通りの組 (n_0, n_1) をすべて試すと、与えられた数の集まりに復号される組はちょうど 1 つ $(39, 12)$ だけであり、それが上のメッセージを与えることが確かめられる。

よくある間違い

- 添字を取り違える。奇数番目の位置は b_1 から $j = 0$ で始まるが、偶数番目の位置は b_2 から $j = 1$ で始まる。
- $6n_1 \equiv 22 \pmod{50}$ を、6 が逆元をもつかのように 6 で割ってしまう。$\gcd(6, 50) = 2$ なので 6 は逆元をもたず、この合同式（congruence）は法 50 で 2 つの解をもつ。
- 条件を満たす n_1 の値を見つけただけで、他の値が条件を満たさないことを示さない。問題は方法の説明を求めているので、一意性には論証が必要である。

STEP のその先へ

これはカエサル暗号（Caesar cipher、シフト暗号）であり、ここでの解読法は頻度分析（frequency analysis）の小さな例である。ずらしの操作は、文字の重複のパターンを保つのである。大学の最初の講義では、$6n \equiv 22$ から 2 つの解を得る段階は、線形合同式（linear congruence）$ax \equiv b \pmod{m}$ の理論にあたる。この合同式は、$\gcd(a, m)$

が b を割り切るとき、かつそのときに限り解をもつ。アフィン暗号（affine cipher）$x \mapsto ax + b$ や、さらに進んだ RSA 暗号も同じ考え方の上に築かれている。Davenport の *The Higher Arithmetic*（高等整数論入門）は合同式を見事に解説している。

Beyond STEP 解答集：https://beyondstep.keithmcnulty.org/ja/。解答本文は CC0 1.0 である。問題そのものは © Cambridge University Press & Assessment に帰属し、ここには掲載していない。英語版から機械翻訳したものであり、まだ校閲を経ていない。