详细解答

STEP III 1987，第 5 题

纯数学 · 模算术密码

> **STEP III 1987，第 5 题**
>
> 继续阅读之前，请先看题目（原题为英文）。题目载于 STEP Support Programme 的试题资料库：
>
> step.maths.org/questions/87-s3-q5

关键思路

这套密码其实是两个独立的移位密码（shift cipher）：偶数位置用一个（密钥为 n_0），奇数位置用另一个（密钥为 n_1），两者都再加上额外的移位 j。先把已知的移位 j 除去。余下的，就是信息的两半各自移了一个未知常数；而模（modulo）50 的移位是双射（bijection），所以相等的数仍然相等，不同的数仍然不同。那三个 43 正是泄露 n_0 的指纹。之后，取一个模 50 的和，便可确定 n_1。

解答

只有 n_0 和 n_1 模 50 的值才有关系，所以我们取 $0 \le n_0, n_1 \le 49$。每个 a_k 都介乎 0 与 49 之间，所以只要知道 a_k 模 50 的剩余（residue），它的值便确定了。

除去已知的移位

对于偶数位置，设 $c_j = b_{2j} - j$，其中 $j = 1, \ldots, 6$。对于奇数位置，设 $d_j = b_{2j+1} - j$，其中 $j = 0, \ldots, 5$。于是

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

由加密后的信息可得：

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

求 n_0

在模 50 之下减去一个固定的 n，是一对一（one-to-one）的运算。所以，奇偶性（parity）相同的两个位置上的 a 相等，当且仅当它们对应的 c（或 d）相等。

> ? **想一想** 那三个 43 可以放在哪里?

六个 d_j 各不相同，所以奇数位置上是六个不同的数，其中最多只有一个 43。因此最少有两个 43 在偶数位置。在 c_j 当中，唯一重复的是 32，它恰好出现两次（$j = 3, 5$），不多也不少。所以偶数位置上恰好有两个相等的数，而它们必定就是那两个 43，因为 43 是信息中唯一出现多于一次的数。因此

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

现在 $a_{2j} \equiv c_j - 39 \equiv c_j + 11$，由此得

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

这是因为 $42 + 11 = 53 \equiv 3$。这六个数全部都在信息之中，这是必然的。

求 n_1

从信息中取走这六个数，余下的就是奇数位置上的数

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

所以 $\{d_j - n_1\}$ 在模 50 之下必须等于 S。

> ? **想一想** 怎样才可以不必把五十个值逐一尝试，就求出 n_1?

把两边分别加起来。如果两个集合相同，它们的和在模 50 之下也相同：

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

所以 $6n_1 \equiv -28 \equiv 22 \pmod{50}$。全式除以 2（它同时整除模数），得 $3n_1 \equiv 11 \pmod{25}$。由于 $3 \times 17 = 51 \equiv 1$，我们得到 $n_1 \equiv 11 \times 17 = 187 \equiv 12 \pmod{25}$。所以 $n_1 = 12$ 或 $n_1 = 37$。

和的条件只是必要条件（necessary condition），并非充分条件（sufficient condition），所以两个值都要检验。若 $n_1 = 37$，则 $d_0 - 37 = -2 \equiv 48$，而这个数不在信息之中，所以 $n_1 = 37$ 不成立。若 $n_1 = 12$，则

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

这正好就是 S。所以 $n_1 = 12$。

信息

把两半交错排列，原来的信息是

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

其中 $n_0 \equiv 39$ 及 $n_1 \equiv 12 \pmod{50}$。以上论证显示这是唯一的答案：n_0 的值别无选择，而 n_1 的两个候选值中只有一个可行。

验算

把答案重新加密。例如 $b_{12} \equiv a_{12} + 39 + 6 = 48$ 及 $b_7 \equiv a_7 + 12 + 3 = 58 \equiv 8$，两者都正确。用电脑把全部 2500 对 (n_0, n_1) 逐一尝试，会发现恰好只有一对，即 $(39, 12)$，能解密出题目所给的那组数，而且得出的正是上面的信息。

常见错误

- 弄错下标。奇数位置由 b_1 开始，对应 $j = 0$；但偶数位置由 b_2 开始，对应 $j = 1$。
- 把 $6n_1 \equiv 22 \pmod{50}$ 除以 6，仿佛 6 是可逆（invertible）的。其实不然，因为 $\gcd(6, 50) = 2$，而这个同余式在模 50 之下有两个解。
- 找到一个可行的 n_1 值，却没有说明其他值都不可行。题目要求你解释所用的方法，所以唯一性需要论证。

STEP 之外

这是凯撒（Caesar）密码，亦即移位密码，而这里的破解方法是频率分析（frequency analysis）的一个小例子：移位会保留字母重复出现的规律。在大学的入门课程中，由 $6n \equiv 22$ 得出两个解的那一步，属于线性同余式（linear congruence）$ax \equiv b \pmod{m}$ 的理论：这类同余式有解，当且仅当 $\gcd(a, m)$ 整除 b。仿射密码（affine cipher）$x \mapsto ax + b$，以及其后的 RSA，都是建基于同样的想法。Davenport 的 *The Higher Arithmetic* 对同余的讲解十分精彩。

Beyond STEP 详细解答：https://beyondstep.keithmcnulty.org/zh-hans/。解答文字采用 CC0 1.0；题目本身版权属 Cambridge University Press & Assessment 所有（©），本文件不予转载。由机器从英文翻译而成；尚未经审阅。