詳細解答

STEP III 1987，第 5 題

純數學 • 模算術密碼

> **STEP III 1987，第 5 題**
>
> 繼續閱讀之前，請先看題目（原題為英文）。題目載於 STEP Support Programme 的試題資料庫：
>
> step.maths.org/questions/87-s3-q5

關鍵思路

這套密碼其實是兩個獨立的移位密碼（shift cipher）：偶數位置用一個（密鑰為 n_0），奇數位置用另一個（密鑰為 n_1），兩者都再加上額外的移位 j。先把已知的移位 j 除去。餘下的，就是信息的兩半各自移了一個未知常數；而模（modulo）50 的移位是雙射（bijection），所以相等的數仍然相等，不同的數仍然不同。那三個 43 正是洩露 n_0 的指紋。之後，取一個模 50 的和，便可確定 n_1。

解答

只有 n_0 和 n_1 模 50 的值才有關係，所以我們取 $0 \le n_0, n_1 \le 49$。每個 a_k 都介乎 0 與 49 之間，所以只要知道 a_k 模 50 的剩餘（residue），它的值便確定了。

除去已知的移位

對於偶數位置，設 $c_j = b_{2j} - j$，其中 $j = 1, \ldots, 6$。對於奇數位置，設 $d_j = b_{2j+1} - j$，其中 $j = 0, \ldots, 5$。於是

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

由加密後的信息可得：

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 之下減去一個固定的 n，是一對一（one-to-one）的運算。所以，奇偶性（parity）相同的兩個位置上的 a 相等，當且僅當它們對應的 c（或 d）相等。

> **想一想** 那三個 43 可以放在哪裏？

六個 d_j 各不相同，所以奇數位置上是六個不同的數，其中最多只有一個 43。因此最少有兩個 43 在偶數位置。在 c_j 當中，唯一重複的是 32，它恰好出現兩次（$j = 3, 5$），不多也不少。所以偶數位置上恰好有兩個相等的數，而它們必定就是那兩個 43，因為 43 是信息中唯一出現多於一次的數。因此

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

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

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

這是因為 $42 + 11 = 53 \equiv 3$。這六個數全部都在信息之中，這是必然的。

求 n_1

從信息中取走這六個數，餘下的就是奇數位置上的數

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

所以 $\{d_j - n_1\}$ 在模 50 之下必須等於 S。

> **想一想** 怎樣才可以不必把五十個值逐一嘗試，就求出 n_1？

把兩邊分別加起來。如果兩個集合相同，它們的和在模 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（它同時整除模數），得 $3n_1 \equiv 11 \pmod{25}$。由於 $3 \times 17 = 51 \equiv 1$，我們得到 $n_1 \equiv 11 \times 17 = 187 \equiv 12 \pmod{25}$。所以 $n_1 = 12$ 或 $n_1 = 37$。

和的條件只是必要條件（necessary condition），並非充分條件（sufficient condition），所以兩個值都要檢驗。若 $n_1 = 37$，則 $d_0 - 37 = -2 \equiv 48$，而這個數不在信息之中，所以 $n_1 = 37$ 不成立。若 $n_1 = 12$，則

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

這正好就是 S。所以 $n_1 = 12$。

信息

把兩半交錯排列，原來的信息是

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

其中 $n_0 \equiv 39$ 及 $n_1 \equiv 12 \pmod{50}$。以上論證顯示這是唯一的答案：n_0 的值別無選擇，而 n_1 的兩個候選值中只有一個可行。

驗算

把答案重新加密。例如 $b_{12} \equiv a_{12} + 39 + 6 = 48$ 及 $b_7 \equiv a_7 + 12 + 3 = 58 \equiv 8$，兩者都正確。用電腦把全部 2500 對 (n_0, n_1) 逐一嘗試，會發現恰好只有一對，即 $(39, 12)$，能解密出題目所給的那組數，而且得出的正是上面的信息。

常見錯誤

- 弄錯下標。奇數位置由 b_1 開始，對應 $j = 0$；但偶數位置由 b_2 開始，對應 $j = 1$。
- 把 $6n_1 \equiv 22 \pmod{50}$ 除以 6，彷彿 6 是可逆（invertible）的。其實不然，因為 $\gcd(6, 50) = 2$，而這個同餘式在模 50 之下有兩個解。
- 找到一個可行的 n_1 值，卻沒有說明其他值都不可行。題目要求你解釋所用的方法，所以唯一性需要論證。

STEP 之外

這是凱撒（Caesar）密碼，亦即移位密碼，而這裏的破解方法是頻率分析（frequency analysis）的一個小例子：移位會保留字母重複出現的規律。在大學的入門課程中，由 $6n \equiv 22$ 得出兩個解的那一步，屬於線性同餘式（linear congruence）$ax \equiv b \pmod{m}$ 的理論：這類同餘式有解，當且僅當 $\gcd(a, m)$ 整除 b。仿射密碼（affine cipher）$x \mapsto ax + b$，以及其後的 RSA，都是建基於同樣的想法。Davenport 的 *The Higher Arithmetic* 對同餘的講解十分精彩。

Beyond STEP 詳細解答：https://beyondstep.keithmcnulty.org/zh-hant/。解答文字採用 CC0 1.0；題目本身版權屬 Cambridge University Press & Assessment 所有（©），本文件不予轉載。由機器從英文翻譯而成；尚未經審閱。