第六届（2021）全国高校密码数学挑战赛
赛题一

一、赛题名称

环上序列的截位还原

二、赛题描述

2.1 基本概念

设 $m>1$ 是正整数，m 元整数集 $\{0,1,\dots,m-1\}$ 在模 m 的加法和乘法下构成一个环，称为整数模 m 剩余类环，并记为 $\mathbb{Z}/(m)$. 若 $2^{k-1}\le m<2^k$，则称 m 的比特长度为 k，例如 $34=2^5+2$，则 34 的比特长度为 6.

设 $c_0,c_1,\dots,c_{n-1}\in\mathbb{Z}/(m)$,

$$f(x)=x^n-(c_{n-1}x^{n-1}+\cdots+c_1x+c_0)\in\mathbb{Z}/(m)\,[x]$$

是 $\mathbb{Z}/(m)$ 上的 n 次首一多项式. 当 c_0 是 $\mathbb{Z}/(m)$ 中的可逆元时，即 $\gcd(c_0,m)=1$ 时，存在整数 $T>0$，使得 $f(x)\mid x^T-1$. 称这样最小的正整数 T 为 $f(x)$ 的周期，并记为 $\mathrm{per}(f(x),m)$. 当 m 是素数方幂时，不妨设 $m=p^e$，其中 p 是素数，$e\ge 1$ 是整数，易知

$$\mathrm{per}(f(x),m)\le p^{e-1}(p^n-1).$$

若 $\mathrm{per}(f(x),m)=p^{e-1}(p^n-1)$，则称 $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的 n 次本原多项式.

注 1： 当 $f(x)$ 是 $\mathbb{Z}/(p^e)$ 上的 n 次本原多项式时，对任意的

$1 \le j \le e$，$f(x) \bmod p^j$ 是 $\mathbb{Z}/(p^j)$ 上的 n 次本原多项式.

一般地，设 $m = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ 是 m 的标准分解，其中 $p_1, p_2, \dots, p_r$ 是互不相同的素数，$e_1, e_2, \dots, e_r$ 是正整数，若对任意的 $1 \le i \le r$，$f(x) \bmod p_i^{e_i}$ 是 $\mathbb{Z}/(p_i^{e_i})$ 上的 n 次本原多项式，则称 $f(x)$ 是 $\mathbb{Z}/(m)$ 上的 n 次本原多项式.

设 $\underline{a} = (a_t)_{t\ge 0}$ 是 $\mathbb{Z}/(m)$ 上的一条序列，即 $a_t \in \mathbb{Z}/(m)$，$t \ge 0$，若 $\underline{a}$ 满足如下 n 级线性递归关系式

$$a_{t+n} = c_{n-1} a_{t+n-1} + \cdots + c_1 a_{t+1} + c_0 a_t \mod \mathrm{m},\ t \ge 0,$$

其中 $c_0, c_1, \dots, c_{n-1} \in \mathbb{Z}/(m)$ 是递归系数，则称 $\underline{a}$ 是 $\mathbb{Z}/(m)$ 上由

$$f(x) = x^n - (c_{n-1} x^{n-1} + \cdots + c_1 x + c_0)$$

生成的 n 级线性递归序列，称 $f(x)$ 为序列 $\underline{a}$ 的一个特征多项式，并称 n 维向量 $(a_0, a_1, \dots, a_{n-1})$ 为序列 $\underline{a}$ 的初态．进一步，若 $f(x)$ 是 $\mathbb{Z}/(m)$ 上的 n 次本原多项式，$\underline{a}$ 是 $\mathbb{Z}/(m)$ 上由 $f(x)$ 生成的 n 级线性递归序列，若对任意的 $1 \le i \le r$，

$$\left([a_0]_{\bmod p_i}, [a_1]_{\bmod p_i}, \dots, [a_{n-1}]_{\bmod p_i}\right) \ne (0,0,\dots,0),$$

其中 $[a_t]_{\bmod p_i}$ 表示最小的非负整数，使得 $a_t \equiv [a_t]_{\bmod p_i} \bmod p_i$，则称 $\underline{a}$ 是 $\mathbb{Z}/(m)$ 上由 $f(x)$ 生成的 n 级本原序列.

2.2 问题描述

设 $f(x) = x^n - (c_{n-1} x^{n-1} + \cdots + c_1 x + c_0)$ 是 $\mathbb{Z}/(m)$ 上的 n 次本原多项式，$\underline{a} = (a_t)_{t\ge 0}$ 是 $\mathbb{Z}/(m)$ 上由 $f(x)$ 生成的 n 级本原序列，$\underline{a}^L = (a_0, a_1, \dots, a_{L-1})$ 是 $\underline{a}$ 的前 L 长有限序列，其中 $L > n$．将每个 a_t 进行二进制展开

$$a_t = a_{t,k-1} \cdot 2^{k-1} + a_{t,k-2} \cdot 2^{k-2} + \cdots + a_{t,0},\ 0 \le t \le L-1,$$

其中 $k = \lfloor \log_2(m-1) \rfloor + 1, a_{t,i} \in \{0,1\},\ 0 \le i < k$. 设 l 是正整数满足 $1 \le l \le k$，令 $\mathrm{MSB}_l(a_t)$ 表示 a_t 的高 l 比特构成的整数，即

$$\mathrm{MSB}_l(a_t) = \left\lfloor \frac{a_t}{2^{k-l}} \right\rfloor = a_{t,k-1} \cdot 2^{l-1} + a_{t,k-1} \cdot 2^{l-2} + \cdots + a_{t,k-l} \cdot 2^0.$$

例如：$\mathrm{MSB}_3(34) = 4$. 令 $\mathrm{MSB}_l(\underline{a}^L)$ 表示 $\underline{a}^L$ 的高 l 比特构成的有限序列，也即

$$\mathrm{MSB}_l(\underline{a}^L) = \left(\mathrm{MSB}_l(a_0), \mathrm{MSB}_l(a_1), \dots, \mathrm{MSB}_l(a_{L-1})\right).$$

本赛题共包含三类挑战，每类挑战分为 9 级，从第 1 级到第 9 级，难度逐级加大.

第一类挑战：在模数 m、本原多项式 $f(x)$ 均已知的条件下，利用已知的 $\mathrm{MSB}_l(\underline{a}^L)$ 还原出未知的初态 $(a_0, a_1, \dots, a_{n-1})$，具体数据见附件.

第二类挑战：在级数 n、模数 m 均已知的条件下，利用已知的 $\mathrm{MSB}_l(\underline{a}^L)$ 还原出未知的本原多项式 $f(x)$ 和初态 $(a_0, a_1, \dots, a_{n-1})$，具体数据见附件.

第三类挑战：在级数 n 和模数 m 的比特长度均已知的条件下，利用已知的 $\mathrm{MSB}_l(\underline{a}^L)$ 还原出未知的模数 m、本原多项式 $f(x)$ 和初态 $(a_0, a_1, \dots, a_{n-1})$，具体数据见附件.

2.3 成绩评判

（1）本次赛题三类挑战中各级挑战的具体分值如表 1 所示.

表 1 三类挑战各级分值对应表

分 值	第一类	第二类	第三类
第 1 级	10 分	10 分	10 分
第 2 级	20 分	20 分	20 分
第 3 级	40 分	40 分	40 分
第 4 级	80 分	80 分	80 分
第 5 级	160 分	160 分	160 分
第 6 级	320 分	320 分	320 分
第 7 级	640 分	640 分	640 分
第 8 级	1280 分	1280 分	1280 分
第 9 级	2560 分	2560 分	2560 分

(2) 第一类挑战中成功求取某级相应初态 $(a_0, a_1, \dots, a_{n-1})$ 视为该级挑战成功，并按表 1 获得该级相应得分. 各级得分的最大值为第一类的得分. 例如 A 团队成功挑战了第一类中的第 1，2，3，5，6，7 级，但未能成功挑战第 8，9 级，则 A 团队在第一类的得分为 640 分.

(3) 第二类挑战中成功求取各级相应本原多项式 $f(x)$ 和初态 $(a_0, a_1, \dots, a_{n-1})$ 视为该级挑战成功，并按表 1 获得该级相应得分；若只成功求取本原多项式，而未能成功求取初态，则该级得分为本级总分的 60%. 各级得分的最大值为第二类的得分. 例如 A 团队成功挑战了第二类中的第 1，2，3，4，5，6 级，第 7 级只成功求取本原多项式 $f(x)$，但未能成功求取初态，第 8，9 级均未能给出正确的本

原多项式和初态，则 A 团队在第二类的得分为 384 分.

（4）第三类挑战中成功求取各级相应模数 m，本原多项式 $f(x)$ 和初态 $(a_0, a_1, \dots, a_{n-1})$ 视为该级挑战成功，并按表 1 获得该级相应得分；若只成功求取模数，而未能给出本原多项式和初态，则该级得分为本级总分的60%；若只成功求取模数和本原多项式，而未能给出初态，则该级得分为本级总分的80%. 各级得分的最大值为第三类的得分. 例如 A 团队成功挑战了第三类中的第 1，2，3，4，5，6 级，第 7 级成功求取模数 m 和本原多项式 $f(x)$，但未能成功求取初态，第 8，9 级均未能给出正确的模数，本原多项式和初态，则 A 团队在第三类的得分为 512 分.

（5）本赛题的总得分为三类挑战得分之和，例如，上述 A 团队的总得分为 $640 + 384 + 512 = 1536$ 分.

（6）三类挑战中每级挑战结果，均需给出计算平台和计算结果，并简述求解原理、步骤、时间和空间复杂度等，程序代码以附件形式附到作品报告中以验证正确性.

（7）方法有创新者，时间和空间复杂度有优势者可酌情加分.

三、密码学背景及相关问题的研究进展

由于进位运算的作用，整数的加法运算在比特层面蕴含丰富的非线性结构，因此整数剩余类环上的线性递归序列（简称环上序列）是一类天然蕴含丰富非线性结构的序列，在序列密码、伪随机数发生器等领域均有重要的应用. 例如，3GPP 移动通信加密算法国际标准

——ZUC 算法中采用 $\mathbb{Z}/(2^{31}-1)$ 上的 16 级本原序列作为驱动序列.

1985 年, Reeds 和 Sloane 将有限域上的 Berlekamp-Massey 算法推广到整数剩余类环上，可有效求取有限序列的最短线性递归关系式，从而有效预测环上序列的输出. 为了增强抗预测性，通常将环上序列进行截位输出，例如截取高 l 位进行输出. 在模数 m 和本原多项式均已知的条件下，杨建斌等[1]将还原序列初态的问题转化为求解模 m 上线性同余方程组的小整数解问题，然后基于 Frieze 等人[2]所给出的格方法对线性同余方程组进行“脱模”处理，进一步转化为整数环上的线性方程组，从而求解相应初态. 最近，孙宏宇等[3]将未知参数条件下线性同余发生器的还原理论拓展到一般环上序列，从而在模数 m 和递归关系式均未知的条件下，给出了由部分截高 $l>1$ 序列还原未知模数，递归系数和初态的方法. 对于模数 m 已知，而递归关系式未知情形，基于文献[3]的工作，通过求解关于未知递归系数的非线性方程组，可有效降低对数据量的要求。

四、参考文献

[1] 杨建斌，朱宣勇. 整数剩余类环上的截位序列还原研究[J]. 密码学报，2017，4(2)：133-150.

[2] A.M. Frieze, J. Hastad, R. Kannan, J.C. Lagarias and A. Shamir. Reconstructing truncated integer variables satisfying linear congruences[J]. SIAM Journal on Computing, 1988, 17(2): 262-280.

[3] H.Y. Sun, X.Y. Zhu and Q.X. Zheng. Predicting truncated multiple recursive generators with unknown parameters[J]. Designs, Codes and Cryptography, 2020, 88: 1083-1102. https://doi.org/10.1007/s10623-020-00729-8.