第三届（2018）全国高校密码数学挑战赛

赛题一

一、赛题名称：序列的有理分数表示

二、赛题描述：

2.1 符号说明

- 同余符号 $\equiv$: 设n是一个正整数. 对任意的整数a和b，有$a \equiv b \bmod n$当且仅当n整除$a-b$.
- 两个整数a和b的最大公因子记为$\gcd(a,b)$.
- 对两个整数a和b，记$\Phi(a,b)=\max\{|a|,|b|\}$.

2.2 基础知识

设$\underline{a}(n)=(a_0,a_1,a_2,\dots,a_{n-1})$是一条有限二元序列，即$a_i \in \{0,1\}, 0 \le i \le n-1$. 若有理分数 $\frac{p}{q}$ 满足q是正奇数，$\gcd(p,q)=1$，并且

$$p \equiv q(a_0+a_1 2+\cdots+a_{n-1}2^{n-1}) \bmod 2^n,$$

则称 $\frac{p}{q}$ 是序列$\underline{a}(n)$的有理分数表示.

2.3 问题描述

已知一条二元序列$\underline{a}(n)=(a_0,a_1,a_2,\cdots,a_{n-1})$. 对$1 \le k \le n$，求有限序列$\underline{a}(k)=(a_0,a_1,a_2,\cdots,a_{k-1})$的有理分数表示. 序列$\underline{a}(n)$请参见附件“sequence.txt”，其中$n=1966000$.

2.4 成绩评判

能正确求解有理分数表示的序列越长（即k越大），得分越高；在k值相等情形下，$\Phi(p,q)$越小，得分越高. 参赛者在论文摘要中应给出所能计算的序列最大长度k和$\underline{a}(k)$的有理分数表示$\frac{p_k}{q_k}$以及$\Phi(p_k,q_k)$，仅需给出一个有理分数表示. 参赛者在论文正文中应详细描述每个有理分数的求取方法.

三、密码学背景及相关问题的研究进展

带进位反馈移位寄存器（简称 FCSR）是由两位美国学者 Klapper 和 Goresky 于 1993 年提出. 与传统的二元域上线性反馈移位寄存器相比, FCSR 通过引入若干进位寄存器, 实现了有理分数2-adic 展开序列的快速生成. 文[1]是关于 FCSR 序列的一个比较全面的综述.

一个 FCSR 由其连接数唯一确定. 一条二元序列$\underline{a}(n)=(a_0,a_1,a_2,\cdots,a_{n-1})$能够由以$q$（$q$为正奇数）为连接数的 FCSR 来生成当且仅当存在整数p满足 $\frac{p}{q}$ 是$\underline{a}(n)$的有理分数表示. 从而若 $\frac{p}{q}$ 是$\underline{a}(n)$的有理分数表示, 则$\log_2 \Phi(p,q)$大致衡量了用以q为连接数的 FCSR 来生成$\underline{a}(n)$所需要的寄存器长度. 若$\Phi(p,q)$在序列$\underline{a}(n)$的全体有理分数表示中达到最小, 则称 $\frac{p}{q}$ 是序列$\underline{a}(n)$的极小有理分数表示, 此时$\log_2 \Phi(p,q)$称为序列$\underline{a}(n)$的2-adic 复杂度, 即生成序列$\underline{a}(n)$所需的最短 FCSR 的寄存器长度. 2-adic 复杂度是衡量一条序列伪随机性的重要指标. 文[1]中给出的有理逼近算法(Rational Approximation Algorithm)是计算序列有理分数表示的有效方法.

四、参考文献

[1] A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. Journal of Cryptology, 1997, 10(2): 111-147. （第 10 节）