MysteryTwister C3

Modular Sequences

Author: Chaoyun Li, ECRYPT-NET, KU Leuven

August 2018

Modular Fibonacci Sequences

You are familiar with the Fibonacci sequence:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \cdots$$

If the numbers are taken modulo 2, then the sequence would be

$$0, 1, 1, 0, 1, 1, 0, 1, 1, \cdots$$

which is a periodic binary sequence with minimal period 3.

Problem 1: *What is the sequence modulo 3? modulo 5?*

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Binary Sequences

Consider the class of recurrence sequences modulo 2. The sequence s_i is determined by the following recurrence relation:

$$s_{i+6} = s_i + s_{i+5} \pmod 2, i \geqslant 0, \tag{1}$$

where the initial values $s_0, s_1, s_2, s_3, s_4, s_5$ are given integers. For instance, if we have $s_0 = s_1 = s_2 = s_3 = s_4 = s_5 = 0$, then it's the all zero binary sequence, which trivially has minimal period 1.

Problem 2: *What is the minimal period of the resulting sequence for arbitrary initial values $s_0, s_1, s_2, s_3, s_4, s_5$?*

Binary Sequences – Hints

- It suffices to consider binary initial values due to the mod 2 operation.
- Consider the vectors $(s_i, s_{i+1}, \cdots, s_{i+5})$ for $i \geqslant 0$.

Challenge

Your task is to solve the problems 1 and 2.

Please enter the solution without any spaces in the following way:
sequencemod3sequencemod5minimalperiod

Example:
sequence mod 3: 1234
sequence mod 5: 12345
minimal period: 20
$\rightarrow$ solution: 12341234520

MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST