MATHEMATISCHES INSTITUT
DER UNIVERSITÄT MÜNCHEN
Prof. Otto Forster

SS 2007
May 16, 2007

Cryptography

Problem Sheet #5

Problem 17

For a positive integer m let $N_m := \{x \in \mathbb{Z} : 0 \le x < m\}$.

a) Define the function $F : N_{32} \to N_{32}$ as follows: For $x \in N_{32}$ let $(b_0, b_1, \ldots, b_9) \in \{0,1\}^{10}$ be given by the relation

$$x(x+1) = \sum_{i=0}^{9} b_i\, 2^i,\ b_i \in \{0,\, 1\}.$$

Then set

$$F(x) := \sum_{i=0}^{4} b_{i+2}\, 2^i \in N_{32}.$$

A *cycle* of length r of F is an r-element subset $C = \{x_0, x_1, \ldots, x_{r-1}\} \subset N_{32}$ such that

$$F(x_{i-1}) = x_i \quad \text{for} \quad 1 \le i < r \quad \text{and} \quad F(x_{r-1}) = x_0.$$

(A cycle of length 1 consists of a single fixpoint of F). The *domain of attraction* (G. *Einzugsbereich*) of C is the set

$$A(C) := \{x \in N_{32} : F^k(x) \in C \text{ for some integer } k \ge 0\}.$$

Determine all cycles and fixpoints of F and their domains of attraction. Display the result in a graph.

b) Find the largest cycle of the map $G : N_{100} \to N_{100}$, defined as follows: For $x \in N_{100}$ let

$$x^2 = \sum_{i=0}^{3} c_i\, 10^i,\ c_i \in \{0, 1, \ldots, 9\}.$$

Then $G(x) := c_1 + 10c_2$.

Problem 18

The sequence $(x_0,\, x_1,\, x_2,\, x_3,\, x_4) = (11,\, 30,\, 229,\, 8,\, 267)$ was generated by a linear congruential generator $x_{i+1} = (ax_i + b) \bmod m$, $i \ge 0$. Determine a, b, m and compute the values $x_5, \ldots, x_9$.

---

p.t.o.

Problem 19

a) Prove that the polynomial $F(T) := T^7 + T + 1 \in \mathbb{F}_2[T]$ is irreducible.

b) Show that for every initial vector $v = (b_0, b_1, \ldots, b_6) \in \mathbb{F}_2^7 \smallsetminus \{\vec{0}\}$ the LFSR sequence defined by

$$b_{k+7} = b_{k+1} + b_k$$

has period length 127.

Problem 20

Use the sequence (b_i) of 19b) to "shrink" the sequence (x_i) of problem 18 as follows: Define $z_i := x_{k_i}$, where k_i is the position of the i-th '1' in the sequence (b_i) (all counts are 0-based).

What is the period of the shrunk sequence (z_i) for the initial vector

$$v = (b_0, \ldots, b_6) = (1, 1, \ldots, 1).$$

What about other initial vectors?

Due: Wednesday, May 23, 2007, 14:10 h

Solutions should be returned in the Cryptography letter box in the first floor of the Institute in front of the library.