Algebraic Structures in Cryptography

Exercises IV 7.10.2015

1. Prove (iii) of Lemma 2 on page 22 of the lecture notes.

2. Calculate $|121/122|_2$, $|45/999|_3$, and $|833/111|_7$.

3. Let $S_n = 1 \cdot 5^0 + 2 \cdot 5^1 + 1 \cdot 5^2 + 2 \cdot 5^3 + 1 \cdot 5^4 + 2 \cdot 5^5 + \cdots + 1 \cdot 5^{2n} + 2 \cdot 5^{2n+1}$. Show that the sequence $(S_n)$ approaches $-11/24$ in the 5-adic sense, that is, $\lim_{n \to \infty} |S_n + 11/24|_5 = 0$.

4. A binary Galois FCSR with 6 cells has feedback to the second, third and sixth cell, counting from the right to the left (shift is towards right). The initial state is 000001 with zeros in carries. Find the connection integer and the initial state integer. Use either Theorem 5 or the formulas after Example 33 to compute the eight first output bits.

5. A binary Fibonacci FCSR with only 3 cells has feedback from the first and the second cell, counting from the right to the left (shift is towards right). The initial state is 001 with zero in carry. Find the connection integer and the initial state integer. Use Theorem 6 to compute the eight first output bits.

6. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points on the elliptic curve $E$. Show that $P \neq Q \neq -P$ implies $x_2 \neq x_1$ when

   (a) $p > 3$,
   (b) $p = 2$.

7. In the case of Example 36 (lecture notes, p. 31–32):

   (a) compute $(t^4, t^3) + (t^6, t^6)$,
   (b) find a natural number $k$ such that $(t^6, t^6) = k(t, t^5)$. 