T-79.5501 Cryptology
Homework 4
October 13& 14, 2005

1. Consider two binary linear feedback shift registers with polynomials $f(x) = x^3 + x^2 + x + 1$ and $g(x) = x^4 + x + 1$. Initialize the first register with 111, and the second one with 0101 (the registers are shifted to the left). Generate the two output sequences and take their xor-sum sequence. Determine the unique shortest linear feedback shift register that generates the sum-sequence.

2. Prove Corollary 2 of Lecture 4: If $f(x)$ divides $h(x)$ then $\Omega(f) \subset \Omega(h)$.

3. Let e be the exponent of $f(x)$. Show that then there is a sequence $S \in \Omega(f)$ such that the period of S is equal to e.

4. Determine the exponent of the polynomial $f(x) = x^5 + x^4 + x^3 + x^2 + x + 1$.

5. Another Fact: An irreducible polynomial $f(x)$ is primitive if and only if $x = 00\ldots010$ is a primitive element in the field $\mathbb{Z}_2[x]/(f(x))$.

   We know that the polynomial $x^4 + x^3 + x^2 + x + 1$ is irreducible but not primitive, since its exponent is 5. Find a primitive element in the field $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$.

6. Let S be a sequence of bits with linear complexity L. Its complemented sequence $\bar{S}$ is the sequence obtained from S by complementing its bits, that is, by adding 1 *modulo* 2 to each bit.

   a) Show that $LC(\bar{S}) \leq L + 1$.
   b) Show that $LC(\bar{S}) = L - 1,$ or $L,$ or $L + 1.$

7. Let us play with the set of integers $\{0, 1, 2, ..., 9\}$. Given two integers from this set, generate a new number by computing the sum of the two previous numbers. If the sum is a one-digit number then the new term is equal to the sum. If the sum is a two digit number then the new term is equal to the sum of the two digits. For example, if the previous numbers are 2 and 5, then the new number is 7. And if the previous numbers are 7 and 9, the new term is $1 + 6 = 7$. Describe this procedure in terms of a linear recursion over a finite ring. Show that the period of any sequence of integers generated in this manner is a divisor of 24.