T-79.503 Foundations of Cryptology
Exam
January 11 2005

SOLUTIONS

1. The first output sequence is `1 1 1 1 ...` of period length 1, and it can also be generated using an LFSR of length 1 with polynomial $x+1$ which is a divisor of polynomial $f(x) = x^3+x^2+x+1 = (x+1)^3$. The second output sequence is `0 1 0 1 1 1 1 0 0 0 1 0 0 1 1 | 0 1 0...` of period length 15. It follows that the sum sequence can be generated with an LFSR of length 5 with feedback polynomial $\mathrm{lcm}(x+1, g(x)) = (x+1)(x^4+x+1) = x^5+x^4+x^2+1$. This is the shortest length, because the sum sequence has 4 consecutive zeros. The feedback polynomial of degree 5 is uniquely determined as soon as at least 10 terms of the sequence are given.

2. (a) For $a' = 010$, we get

x	$x+a'$	$t(x)$	$t(x+a')$	$t(x+a')+t(x)$
000	010	0	0	0
001	011	0	1	1
010	000	0	0	0
011	001	1	0	1
100	110	0	1	1
101	111	1	1	0
110	100	1	0	1
111	101	1	1	0

It follows that $N_D(010, b') = 4$, for $b' = 0$ or $b' = 1$.
For $a' = 111$, we get

x	$x+a'$	$t(x)$	$t(x+a')$	$t(x+a')+t(x)$
000	111	0	1	1
001	110	0	1	1
010	101	0	1	1
011	100	1	0	1
100	011	0	1	1
101	010	1	0	1
110	001	1	0	1
111	000	1	0	1

It follows that $N_D(111, b') = 8$, for $b' = 1$, and $N_D(111, b') = 0$, or $b' = 0$.

(b) An intrepretation of the result $N_D(111, 1) = 8$ is that output is complemented as all input bits are complemented. See also the table for $a' = 111$.

3. We have $1000 = 2^3 5^3 = 8 \cdot 125$. We compute $\phi(8) = \phi(2^3) = 2^3(1-1/2) = 4$ and $\phi(125) = \phi(5^3) = 5^3(1-1/5) = 100$.

To compute $x = 2005^{2005}$ modulo 1000, we compute it first modulo 8 and then modulo 125, and combine the results using the Chinese Remainder Theorem. As $2005 \equiv 1 \bmod \phi(8)$ we get

$$2005^{2005} \equiv 5^1 \equiv 5 (\text{mod} 8).$$

Since $\phi(125) = 100$, we get

$$2005^{2005} \equiv 5^5 = 125 \cdot 25 \equiv 0 (\text{mod} 125).$$

So we have

$$\begin{aligned} x &\equiv 0 (\text{mod} 125) \\ x &\equiv 5 (\text{mod} 8). \end{aligned}$$

Since $125 \equiv 5 (\text{mod} 8)$ it follows that $x = 125$.

An alternative solution is obtained by observing that, for $n \geq 3$, we have $5^n \bmod 1000 = 625$, if n is even, and $5^n \bmod 1000 = 125$, if n is odd.

4. (a)

$$\left(\frac{801}{2005}\right) = \left(\frac{2005}{801}\right) = \left(\frac{403}{801}\right) = \left(\frac{801}{403}\right) = \left(\frac{398}{403}\right) = \left(\frac{2}{403}\right)\left(\frac{199}{403}\right) = -\left(\frac{199}{403}\right)$$
$$= \left(\frac{403}{199}\right) = \left(\frac{5}{199}\right) = \left(\frac{199}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1$$

using the properties of the Jacobi symbol.

(b) $\frac{n-1}{2} = 1002 = 2 \cdot 501$. We get

$$801^{1002} = (801^2)^{501} = (1)^{501} = 1 \,(\text{mod}\, 2005).$$

By (a) we have

$$\left(\frac{801}{2005}\right) = 1 = 801^{\frac{2005-1}{2}}$$

and hence 2005 is an Euler pseudo prime to the base 801.

5. Running Wiener's algorithm we get:

j	r_j	q_j	c_j	d_j	n'
0	117353	-	1	0	-
1	400271	0	0	1	-
2	117353	3	1	3	352058
3	48212	2	2	7	410735
4	20929	2	5	17	399000
5	6354	⋮	⋮	⋮	⋮

For each j the test value n' is computed as $n' = (d_j b - 1)/c_j$. For $j = 4$ the candidate value $n' = 399000$. Substituting the values $n = 400271$ and $n' = 399000$ to the equation $x^2 - (n - n' + 1)x + n = 0$ we get

$$x^2 - 1272x + 400271 = 0,$$

from where the solutions (= values of p and q) are $x = 636 \pm 65$. The value of the private exponent is $a = 17$. We also see that $\phi(n) = n' = 399000$.