T-79.5501 Cryptology Spring 2009

Homework 3

Tutor : Joo Y. Cho
joo.cho@tkk.fi

12th February 2009

Q1. Consider the finite field $\mathbb{F} = \mathbf{Z}_2[x]/(f(x))$, with the polynomial $f(x) = x^5 + x^2 + 1$.

a) Compute $(x^4 + x)(x^3 + x^2 + 1)$.

b) Using the Extended Euclidean Algorithm, compute $(x^3 + x)^{-1}$.

c) Compute x^{35}.

A1-a) Since $x^5 \equiv x^2 + 1$, we get

$$\begin{aligned}(x^4 + x)(x^3 + x^2 + 1) &= x^7 + x^6 + x^3 + x \\ &\equiv x^2(x^2 + 1) + x(x^2 + 1) + x^3 + x \equiv x^4 + x^2\end{aligned}$$

A1-b) Since $r_i = r_{i-2} - q_i r_{i-1}$ and $u_i = u_{i-2} - q_i u_{i-1}$,

i	q_i	r_i	u_i
0		$x^5 + x^2 + 1$	0
1		$x^3 + x$	1
2			
3			
4			

A1-a) Since $x^5 \equiv x^2 + 1$, we get

$$\begin{aligned}(x^4+x)(x^3+x^2+1) &= x^7+x^6+x^3+x \\ &\equiv x^2(x^2+1)+x(x^2+1)+x^3+x \equiv x^4+x^2\end{aligned}$$

A1-b) Since $r_i = r_{i-2} - q_i r_{i-1}$ and $u_i = u_{i-2} - q_i u_{i-1}$,

i	q_i	r_i	u_i
0		x^5+x^2+1	0
1		x^3+x	1
2	x^2+1	x^2+x+1	x^2+1
3			
4			

A1-a) Since $x^5 \equiv x^2 + 1$, we get

$$
\begin{aligned}
(x^4 + x)(x^3 + x^2 + 1) &= x^7 + x^6 + x^3 + x \\
&\equiv x^2(x^2 + 1) + x(x^2 + 1) + x^3 + x \equiv x^4 + x^2
\end{aligned}
$$

A1-b) Since $r_i = r_{i-2} - q_i r_{i-1}$ and $u_i = u_{i-2} - q_i u_{i-1}$,

i	q_i	r_i	u_i
0		$x^5 + x^2 + 1$	0
1		$x^3 + x$	1
2	$x^2 + 1$	$x^2 + x + 1$	$x^2 + 1$
3	$x + 1$	$x + 1$	$x^3 + x^2 + x$
4			

A1-a) Since $x^5 \equiv x^2 + 1$, we get

$$\begin{aligned}(x^4+x)(x^3+x^2+1) &= x^7+x^6+x^3+x \\ &\equiv x^2(x^2+1)+x(x^2+1)+x^3+x \equiv x^4+x^2\end{aligned}$$

A1-b) Since $r_i = r_{i-2} - q_i r_{i-1}$ and $u_i = u_{i-2} - q_i u_{i-1}$,

i	q_i	r_i	u_i
0		x^5+x^2+1	0
1		x^3+x	1
2	x^2+1	x^2+x+1	x^2+1
3	$x+1$	$x+1$	x^3+x^2+x
4	x	1	x^4+x^3+1

$\Rightarrow (x^3+x)^{-1} \bmod x^5+x^2+1 = x^4+x^3+1.$

A1-c) Using $x^5 \equiv x^2 + 1$, we get

$$\begin{aligned} x^{10} &= (x^2+1)^2 \equiv x^4 + 1 \\ x^{20} &= (x^4+1)^2 = x^8 + 1 \equiv x^3(x^2+1) + 1 = x^3 + x^2 \\ x^{30} &= x^{10}x^{20} \equiv (x^4+1)(x^3+x^2) \equiv x^4 + x \end{aligned}$$

Hence,

$$\begin{aligned} x^{35} &= x^{30}x^5 \equiv (x^4+x)(x^2+1) \\ &= x^6 + x^4 + x^3 + x \equiv x^4 \pmod{x^5 + x^2 + 1} \end{aligned}$$

Q2. Let a and b be positive integers where $b > a$. Let r_i, u_i and v_i, $i = 0, 1, \ldots$, be the sequences produced by the Extended Euclidean algorithm. Prove that

1. $r_i = u_i a \bmod b$, and
2. $b = |u_{i+1}| r_i + |u_i| r_{i+1}$,

for all $i = 0, 1, \ldots$.

A2-a) In the Proof of Extended Euclidean Algorithm (see lecture-3 slides), it is proved that $r_i = u_i \cdot a + v_i \cdot b$ for some positive $b > a$ where $i = 0, 1, \ldots$. Hence,

$$r_i = u_i \cdot a \pmod{b}$$

A2-b)
Proof by induction : $u_i \cdot u_{i+1} < 0$ where $i = 1, 2, \ldots$. $i = 1$:

$u_1 \cdot u_2 = u_1 \cdot (u_0 - q_2 \cdot u_1) = -q_2 < 0$.
We assume $u_{i-1} \cdot u_i < 0$.
Then, $u_i \cdot u_{i+1} = u_i \cdot (u_{i-1} - q_{i+1} u_i) = u_i \cdot u_{i-1} - q_{i+1} u_i^2 < 0$.
Hence, the claim holds for i.

A2-b) Prove the main claim by induction.
For $i = 0$, $|u_1|r_0 + |u_0|r_1 = b$.
For $i = 1$, $|u_2|r_1 + |u_1|r_2 = |-q_2| \cdot a + (b - q_2 \cdot a) = b$.
For $i-1$, we assume that $b = |u_i|r_{i-1} + |u_{i-1}|r_i$. Then,

$$\begin{aligned}
|u_{i+1}|r_i &= |u_{i-1}r_i - q_{i+1}u_i|r_i \\
|u_i|r_{i+1} &= |u_i|r_{i-1} - q_{i+1}|u_i|r_i \\
\Rightarrow |u_{i+1}|r_i + |u_i|r_{i+1} &= |u_{i-1}r_i - q_{i+1}u_i|r_i + |u_i|r_{i-1} - q_{i+1}|u_i|r_i
\end{aligned}$$

(1) If $u_{i+1} > 0$, then $u_i < 0$ and $u_{i-1} > 0$

$$\begin{aligned}
u_{i-1}r_i - q_{i+1}u_ir_i + (-u_i)r_{i-1} - q_{i+1}(-u_i)r_i &= u_{i-1}r_i - u_ir_{i-1} \\
&= |u_{i-1}|r_i + |u_i|r_{i-1}
\end{aligned}$$

(2) If $u_{i+1} < 0$, then $u_i > 0$ and $u_{i-1} < 0$.

$$\begin{aligned}
-u_{i-1}r_i + q_{i+1}u_ir_i + u_ir_{i-1} - q_{i+1}u_ir_i &= -u_{i-1}r_i + u_ir_{i-1} \\
&= |u_{i-1}|r_i + |u_i|r_{i-1}
\end{aligned}$$

Hence, the claim holds for i.

Q3. Compute the two least significant decimal digits of the integer 2009^{2009}.

Let p be a prime and t a positive number. Then,

$$\begin{aligned}\phi(p) &= p-1\\ \phi(p^t) &= p^t - p^{t-1}.\end{aligned}$$

A3. The task is to compute $2009^{2009} \pmod{100}$. Since $100 = 2^2 \cdot 5^2$, we compute $x \equiv 2009^{2009} \pmod{100}$ by first solving $x \pmod 4$ and then $x \pmod{25}$. The results are combined by the Chinese Remainder Theorem.

Since $\phi(25) = 5^2 - 5 = 20$, we get

$$\begin{aligned} x &\equiv (2009 \bmod 4)^{2009} = 1 \pmod 4 \\ x &\equiv (2009 \bmod 25)^{100\cdot 20+9} \equiv 9^9 \equiv 14 \pmod{25}. \end{aligned}$$

Using the Extended Euclidean algorithm, we compute $4^{-1} \equiv 19 \pmod{25}$ and $25^{-1} \equiv 1 \pmod 4$. Hence, by Chinese Remainder Theorem, we get

$$x \equiv 1 \cdot 25 \cdot 1 + 14 \cdot 4 \cdot 19 \equiv 89 \quad \pmod{100}.$$

Q4. Consider the finite field $\mathbb{F} = \mathbf{Z}_2[x]/(f(x)) = GF(2^n)$ with polynomial $f(x) = x^4 + x + 1$. Plaintext consists of strings of 4 bits with a single bit `1` and 3 bits `0`. Each such string occur independently and with probability $\frac{1}{4}$. The encryption method is a stream cipher with $\mathcal{P} = \mathcal{C} = \mathcal{K} = \mathbb{F}^*$. Given a key $K = \beta \in \mathbb{F}^*$ and a plaintext sequence x_i, $i = 1, 2, \ldots, n$ the ciphertext sequence is computed as follows

$$y_i = \beta^i x_i,\ i = 1, 2, \ldots, n.$$

It is given that the 3rd and 4th terms of the ciphertext sequence are

$$y_3 = 1100 \text{ and } y_4 = 0111.$$

Then exactly two keys are possible. What are they? (Hint: To facilitate the computations you may represent the elements of $\mathbb{F}^*$ as powers of a primitive element α. For example, if you choose $\alpha = 0010$, then the four possible plaintext terms are 1, α, α^2 or α^3.)

A4. The multiplicative group of all non-zero elements in the Galois field $GF(2^4) = \mathbf{Z}_2[x]/(x^4 + x + 1)$ that are generated by the primitive element $\alpha = x = (0010)$:

k	α^k	k	α^k	k	α^k
1	x	6	$x^6 = x^3 + x^2$	11	$x^{11} = x^3 + x^2 + x$
2	x^2	7	$x^7 = x^3 + x + 1$	12	$x^{12} = x^3 + x^2 + x + 1$
3	x^3	8	$x^8 = x^2 + 1$	13	$x^{13} = x^3 + x^2 + 1$
4	$x^4 = x + 1$	9	$x^9 = x^3 + x$	14	$x^{14} = x^3 + 1$
5	$x^5 = x^2 + x$	10	$x^{10} = x^2 + x + 1$	15	$x^{15} = 1$

The possible plaintexts : $\alpha^0 = (0001)$, $\alpha^1 = (0010)$, $\alpha^2 = (0100)$ and $\alpha^3 = (1000)$.

We put $\beta = x^k$. Then,

$$\alpha^{3k+r} = \alpha^6 \text{ and } \alpha^{4k+s} = \alpha^{10},$$

or what is equivalent

$$\begin{aligned} 3k + r &\equiv 6 \pmod{15} \\ 4k + s &\equiv 10 \pmod{15} \end{aligned}$$

where $r, s \in \{0, 1, 2, 3\}$.
By simple computation, we get $k = 2$ or $k = 6$, and the two possible keys are $\beta = \alpha^2 = 0100$ and $\beta = \alpha^6 = 1100$.

Q5.

Solve the following congruence equations:

a) $5x \equiv 4 \pmod{41}$

b) $35x \equiv 28 \pmod{2009}$

Q5-a) By the Extended Euclidean Algorithm,

i	q_i	r_i	v_i
0		41	0
1		5	1
2	8	1	$-8 \equiv 33$

we get $5^{-1} = 33 \pmod{41}$.
Hence, $x \equiv 5^{-1} \cdot 4 \equiv 9 \pmod{41}$.

Q5-b) Since $GCD(35, 28, 2009) = 7$, the equation is equivalent to $5x \equiv 4 \pmod{287}$. Then, by applying the Extended Euclidean Algorithm,

i	q_i	r_i	v_i
0		287	0
1		5	1
2	57	2	-57
3	2	1	$1 - 2 \cdot -57 \equiv 115$

we get $5^{-1} = 115 \pmod{287}$. Hence, $x \equiv 5^{-1} \cdot 4 \equiv 173 \pmod{287}$. The original equation has now seven solutions modulo 2009:

$$x \equiv 173 + i \cdot 287 \pmod{2009}, \quad i = 0, 1, \ldots, 6.$$

Q6.

Consider a binary LFSR with connection polynomial $x^4 + x^3 + x^2 + x + 1$, that is, $c_0 = c_1 = c_2 = c_3 = 1$ in the recurrence relation (see textbook Section 1.2.5 or the attached slides).

a) Show that the periods of the binary sequences generated by this LFSR are 1 and 5.

b) Consider a stream cipher where the keystream sequence is generated using this LFSR. The ciphertext sequence is
1 1 1 0 1 1 0 1 1 1 1 0 0 0 1 0.
It is given that the 4th and 12th plaintext bits are equal to **0** and the 8th and 16th bits are equal to **1**. Find the initial state of the LFSR, that is, the four first bits of the keystream sequence.

A6-a). By experiment we see that this LFSR generates three cycles of length 5 and the all zero cycle:

0000	0001	0010	0111
	0011	0101	1111
	0110	1010	1110
	1100	0100	1101
	1000	1001	1011

It follows that the periods are 1 and 5.

A6-b)

`1 1 1 0 1 1 0 1 1 1 1 0 0 0 1 0` = ciphertext

`- - - 0 - - - 1 - - - 0 - - - 1` = plaintext

`- - - 0 - - - 0 - - - 0 - - - 1` = keystream

Since $z_i = z_{i+5}$, for all $i = 1, 2, ...$, we know that $z_4 = z_9 = z_{14} = 0$, $z_8 = z_3 = z_{13} = 0$ and so on.

Hence, we can fill in most of the keystream terms to get:

$$\texttt{1000} - \texttt{1000} - \texttt{1000} - \texttt{1} = \textit{keystream}$$

From this we can read the initial state: `1 0 0 0`.