Quiz

Remarks

- Time: 11 am - 12:30pm
- Do not use "písané písmo" but "paličkové".
- Write down the answers on the papers given to you, more can be provided upon request - full name should be written on each page of the answer sheet.
- Detailed computation steps are required. 0 mark will be given if only a final answer is provided.

Question 1. (2 marks)

1. Find $\gcd(120, 35)$ using the Euclidean algorithm
2. Find $21^{-1} \bmod 160$ using the extended Euclidean algorithm

Solution. 1. By the Euclidean algorithm

$$\begin{array}{ll} 120 = 35 \times 3 + 15 & \gcd(120,35) = \gcd(35,15) \\ 35 = 15 \times 2 + 5 & \gcd(35,15) = \gcd(15,5) \\ 15 = 5 \times 3 & \gcd(15,5) = 5 \end{array}$$

We have, $\gcd(120, 35) = 5$.
2. By the Euclidean algorithm:

$$\begin{array}{ll} 160 = 21 \times 7 + 13 & 21 = 13 \times 1 + 8 \\ 13 = 8 \times 1 + 5 & 8 = 5 \times 1 + 3 \\ 5 = 3 \times 1 + 2 & 3 = 2 \times 1 + 1 \end{array}$$

By the extended Euclidean algorithm:

$$\begin{array}{ll} 1 = 3 - 2, & 2 = 5 - 3 \\ 3 = 8 - 5, & 5 = 13 - 8 \\ 8 = 21 - 13, & 13 = 160 - 21 \times 7 \end{array}$$

$$\begin{aligned} 1 &= 3 - (5 - 3) = 3 \times 2 - 5 = 8 \times 2 - 5 \times 3 = 8 \times 2 - (13 - 8) \times 3 \\ &= 8 \times 5 - 13 \times 3 = 21 \times 5 - 13 \times 8 = 21 \times 5 - (160 - 21 \times 7) \times 8 \\ &= 21 \times 61 - 160 \times 8 \end{aligned}$$

Thus $21^{-1} \bmod 160 = 61$

Question 2. (2 marks) Solve the following system of simultaneous linear congruences

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 7 \\ x &\equiv ? \bmod 105 \end{aligned}$$

Solution. With the formula we have seen in the lecture

$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7, \quad a_1 = 2, \quad a_2 = 3, \quad a_3 = 2,$$
$$m = 3 \times 5 \times 7 = 105, \quad M_1 = 35, \quad M_2 = 21, \quad M_3 = 15.$$

Then

$$M_1 \equiv 35 \equiv 2 \bmod 3, \quad M_2 \equiv 21 \equiv 1 \bmod 5, \quad M_3 \equiv 15 \equiv 1 \bmod 7.$$

Using the extended Euclidean algorithm, we can find

$$y_1 = M_1^{-1} \bmod 3 = 2, \quad y_2 = M_2^{-1} \bmod 5 = 1, \quad y_3 = M_3^{-1} \bmod 7 = 1.$$

And

$$\begin{aligned} x &= \sum_{i=1}^{3} a_i y_i M_i \bmod m = 2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15 \bmod 105 \\ &= 233 \bmod 105 = 23 \bmod 105. \end{aligned}$$

Question 3. (2 marks) Let $f(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{F}_2[x]$. The set of congruence classes modulo $f(x)$ is a field, in particular:

$$\mathbb{F}_2[x]/(f(x)) = \left\{ \sum_{i=0}^{7} b_i x^i \;\middle|\; b_i \in \mathbb{F}_2 \ \forall i \right\} \cong \mathbb{F}_{2^8}$$

Define φ:

$$\begin{aligned} \varphi : \mathbb{F}_2[x]/(f(x)) &\to \mathbb{F}_2^8 \\ b_7x^7 + b_6x^6 + b_5x^5 + b_4x^4 + b_3x^3 + b_2x^2 + b_1x + b_0 &\mapsto b_7b_6b_5b_4b_3b_2b_1b_0 \end{aligned}$$

Then we have a 1-1 correspondence between elements in $\mathbb{F}_2[x]/(f(x))$ and binary string of length 8, or bytes. During the lecture, we have discussed that with addition and multiplication modulo $f(x)$ in $\mathbb{F}_2[x]/(f(x))$, we can define the corresponding addition and multiplication between bytes. We have also seen that the multiplicative inverse of $g(x) \in \mathbb{F}_2[x]/(f(x))$ can be found using the extended Euclidean algorithm. Consequently, we can find the inverse of a byte as an element in $\mathbb{F}_2[x]/(f(x))$.

Find inverse of $\texttt{5B}_{16} = 01011011_2$ as an element in $\mathbb{F}_2[x]/(f(x))$. Write the final answer in **hexadecimal** format.

Solution. By the Euclidean algorithm

$$\begin{aligned} f(x) &= (x^2+1)(x^6+x^4+x^3+x+1) + (x^5+x^3+x^2), \\ x^6+x^4+x^3+x+1 &= x(x^5+x^3+x^2) + (x+1), \\ x^5+x^3+x^2 &= (x^4+x^3+x+1)(x+1) + 1. \end{aligned}$$

By the extended Euclidean algorithm

$$\begin{aligned} 1 &= (x^5+x^3+x^2) + (x^4+x^3+x+1)(x+1) \\ &= (x^5+x^3+x^2) + (x^4+x^3+x+1)((x^6+x^4+x^3+x+1) + x(x^5+x^3+x^2)) \\ &= (x^4+x^3+x+1)(x^6+x^4+x^3+x+1) + (x^5+x^4+x^2+x+1)(x^5+x^3+x^2) \\ &= (x^4+x^3+x+1)(x^6+x^4+x^3+x+1) \\ &\quad +(x^5+x^4+x^2+x+1)(f(x) + (x^2+1)(x^6+x^4+x^3+x+1)) \\ &= (x^5+x^4+x^2+x+1)f(x) + (x^7+x^6+x^5+x^4)(x^6+x^4+x^3+x+1). \end{aligned}$$

We have

$$
\begin{aligned}
(x^6+x^4+x^3+x+1)^{-1} \bmod f(x) &= x^7+x^6+x^5+x^4 = 11110000_2 \\
&= \texttt{F0}.
\end{aligned}
$$

Question 4. (4 marks) We have learned that

Theorem 1. Every Boolean function $\varphi : \mathbb{F}_2^n \to \mathbb{F}_2$ has a unique algebraic normal form representation

$$
\varphi(\mathbf{x}) = \sum_{\mathbf{v}\in\mathbb{F}_2^n} \left(\lambda_{\mathbf{v}} \prod_{i=0}^{n-1} x_i^{v_i} \right),
$$

the coefficients $\lambda_{\mathbf{v}} \in \mathbb{F}_2$ are given by

$$
\lambda_{\mathbf{v}} = \sum_{\mathbf{w}\leq\mathbf{v}} \varphi(\mathbf{w}),
$$

where $\mathbf{w} \leq \mathbf{v}$ means that $w_i \leq v_i$ for all $0 \leq i \leq n-1$.

The 1**st bit** of PRESENT Sbox output is a Boolean function $\varphi_1 : \mathbb{F}_2^4 \to \mathbb{F}_2$, find the algebraic normal form for φ_1.

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Table 1: PRESENT Sbox

Solution. We can construct the following truth table:

$\mathbf{x}$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x_3	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
x_2	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
x_1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
x_0	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
$\mathrm{SB}_{\mathrm{PRESENT}}(\mathbf{x})$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2
$\varphi_1(\mathbf{x})$	0	0	1	1	0	0	1	0	1	1	1	0	0	1	0	1
$\lambda_{\mathbf{x}}$	0	0	1	0	0	0	0	1	1	0	1	1	1	1	0	0

The algebraic normal form of φ_1 is then given by

$$
\begin{aligned}
\varphi_1(\mathbf{x}) &= \sum_{\mathbf{v}\in\mathbb{F}_2^n} \left(\lambda_{\mathbf{v}} \prod_{i=0}^{n-1} x_i^{v_i} \right) = \lambda_{0010}x_1 + \lambda_{0111}x_2x_1x_0 + \lambda_{1000}x_3 + \lambda_{1010}x_3x_1 \\
&\quad +\lambda_{1011}x_3x_1x_0 + \lambda_{1100}x_3x_2 + \lambda_{1101}x_3x_2x_0 \\
&= x_1 + x_3 + x_1x_3 + x_2x_3 + x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3
\end{aligned}
$$