

Øving 5 - Løsningsforslag

Oppgave 4.7 (for \mathbb{Z}_7) s. 135

Skal finne den multiplikative inversen til hvert av elementene i \mathbb{Z}_7 . Gitt et element a , så er b en invers til a i \mathbb{Z}_p , hvis $ab \equiv 1 \pmod{p}$, der p er et primtall.

En måte å finne inversene på er å skrive opp multiplikasjonstabellen for \mathbb{Z}_7 og lokalisere alle elementer som er lik 1.

\times	1	2	3	4	5	6
1	1*	2	3	4	5	6
2	2	4	6	1*	3	5
3	3	6	2	5	1*	4
4	4	1*	5	2	6	3
5	5	3	1*	6	4	2
6	6	5	4	3	2	1*

Tabell 1: Multiplikasjon modulo 7

der elementene lik 1 er merket med en stjerne. Kan dermed lese ut fra tabellen følgende:

$$1 \cdot 1 \equiv 1 \pmod{7} \quad (1)$$

$$2 \cdot 4 \equiv 1 \pmod{7} \quad (2)$$

$$3 \cdot 5 \equiv 1 \pmod{7} \quad (3)$$

$$4 \cdot 2 \equiv 1 \pmod{7} \quad (4)$$

$$5 \cdot 3 \equiv 1 \pmod{7} \quad (5)$$

$$6 \cdot 6 \equiv 1 \pmod{7} \quad (6)$$

Dette gir følgende inverser:

$$1^{-1} \equiv 1 \pmod{7} \quad (7)$$

$$2^{-1} \equiv 4 \pmod{7} \quad (8)$$

$$3^{-1} \equiv 5 \pmod{7} \quad (9)$$

$$4^{-1} \equiv 2 \pmod{7} \quad (10)$$

$$5^{-1} \equiv 3 \pmod{7} \quad (11)$$

$$6^{-1} \equiv 6 \pmod{7} \quad (12)$$

Oppgave 4.9 s. 136

For å finne største fellese divisor (gcd) brukes Euklids algoritme (s. 116-117 i Stallings). Algoritmen terminerer når 'resten' i divisjonen er null. Da er største felles divisor lik forrige rundes rest.

a) Skal finne $\gcd(24140, 16762)$.

$$24140 = 16762 \cdot 1 + 7378$$

$$16762 = 7378 \cdot 2 + 2006$$

$$7378 = 2006 \cdot 3 + 1360$$

$$2006 = 1360 \cdot 1 + 646$$

$$1360 = 646 \cdot 2 + 68$$

$$646 = 68 \cdot 9 + 34$$

$$68 = 34 \cdot 2 + 0$$

Dermed er $\gcd(24140, 16762) = \gcd(16762, 7378) = \gcd(7378, 2006) = \gcd(2006, 1360) = \gcd(1360, 646) = \gcd(646, 68) = \gcd(68, 34) = 34$.

b) Skal finne $\gcd(4655, 12075)$.

$$12075 = 4655 \cdot 2 + 2765$$

$$4655 = 2765 \cdot 1 + 1890$$

$$2765 = 1890 \cdot 1 + 875$$

$$1890 = 875 \cdot 2 + 140$$

$$875 = 140 \cdot 6 + 35$$

$$140 = 35 \cdot 4 + 0$$

Dermed er $\gcd(4655, 12075) = \gcd(4655, 2765) = \gcd(2765, 1890) = \gcd(1890, 875) = \gcd(875, 140) = \gcd(140, 35) = 35$

Oppgave 4.13 a) s. 136

Her skal Euklids utvidede algoritme (s. 119-120 i Stallings) brukes til å finne inversen av de gitte tallene. Tabell 2 viser at $\gcd(1234, 4321) = 1$, og at den

Q	A1	A2	A3	B1	B2	B3
-	1	0	4321	0	1	1234
3	0	1	1234	1	-3	619
1	1	-3	619	*	4	615
1	*	4	615	*	-7	4
153	*	-7	4	*	1075	3
1	*	1075	3	*	-1082	1

Tabell 2: Finne inversen til 1234 modulo 4321

multiplikative inversen til 1234 modulo 4321 er -1082, dvs.

$$1234^{-1} \equiv -1082 \equiv 3239 \pmod{4321} \quad (13)$$

Elementene A1 og B1 trengs ikke for å finne inversen, og er derfor erstattet med stjerne. Oppgave b) og c) løses helt tilsvarende.

Oppgave 4.16 s. 136

Polynomaritmetikk i \mathbf{Z}_{10} :

a) $(7x + 2) - (x^2 + 5) = -x^2 + 7x - 3 = 9x^2 + 7x + 7$

b) Utfører polynommultiplikasjonen og reduserer koeffisientene modulo 10:

$$\begin{aligned}(6x^2 + x + 3) \times (5x^2 + 2) &= 30x^4 + 12x^2 + 5x^3 + 2x + 15x^2 + 6 \\ &= (0 + 3 \cdot 10)x^4 + 5x^3 + (7 + 2 \cdot 10)x^2 + 2x + 6 \\ &= 5x^3 + 7x^2 + 2x + 6\end{aligned}$$

Oppgave 4.19 s.137

Når vi skal finne den multiplikative inversen til $x^3 + x + 1$ i $\text{GF}(2^4)$ med $m(x) = x^4 + x + 1$ må vi bruke Euklids utvidede algoritme for polynomer (s.130 i Stallings).

Initialisering

$$\begin{aligned}A1(x) &= 1, A2(x) = 0, A3(x) = x^4 + x + 1 \\ B1(x) &= 0, B2(x) = 1, B3(x) = x^3 + x + 1\end{aligned}$$

Iterasjon 1

$$\begin{aligned}Q(x) &= \text{kvotienten til } \frac{A3(x)}{B3(x)} = x \\ \text{siden } \frac{A3(x)}{B3(x)} &= \frac{x^4 + x + 1}{x^3 + x + 1} = x + \frac{x^2 + 1}{x^3 + x + 1} \\ A1(x) &= 0, A2(x) = 1, A3(x) = x^3 + x + 1 \\ B1(x) &= 1, B2(x) = x, B3(x) = x^2 + 1\end{aligned}$$

Iterasjon 2

$$\begin{aligned}Q(x) &= \text{kvotienten til } \frac{A3(x)}{B3(x)} = x \\ \text{siden } \frac{A3(x)}{B3(x)} &= \frac{x^3 + x + 1}{x^2 + 1} = x + \frac{1}{x^2 + 1} \\ A1(x) &= 1, A2(x) = x, A3(x) = x^2 + 1 \\ B1(x) &= x, B2(x) = x^2 + 1, B3(x) = 1\end{aligned}$$

Algoritmen terminerer når $B3(x)=1$, og da er $B2(x)$ lik inversen:

$$(x^2 + x + 1)^{-1} \pmod{(x^4 + x + 1)} = x^2 + 1.$$

Løsning til oppgave 5.1 og 5.2

5.1 We want to show that $d(x) = a(x) \times b(x) \bmod (x^4 + 1) = 1$. Substituting into Equation (5.1) in Appendix 5A, we have:

$$\begin{bmatrix} d_0 \\ d_1 \\ d_2 \\ d_3 \end{bmatrix} = \begin{bmatrix} a_0 & a_3 & a_2 & a_1 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_1 & a_0 & a_3 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 0E \\ 09 \\ 0D \\ 0B \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

But this is the same set of equations discussed in the subsection on the MixColumn transformation:

$$\begin{aligned} (\{0E\} \cdot \{02\}) \oplus \{0B\} \oplus \{0D\} \oplus (\{09\} \cdot \{03\}) &= \{01\} \\ (\{09\} \cdot \{02\}) \oplus \{0E\} \oplus \{0B\} \oplus (\{0D\} \cdot \{03\}) &= \{00\} \\ (\{0D\} \cdot \{02\}) \oplus \{09\} \oplus \{0E\} \oplus (\{0B\} \cdot \{03\}) &= \{00\} \\ (\{0B\} \cdot \{02\}) \oplus \{0D\} \oplus \{09\} \oplus (\{0E\} \cdot \{03\}) &= \{00\} \end{aligned}$$

The first equation is verified in the text. For the second equation, we have $\{09\} \cdot \{02\} = 00010010$; and $\{0D\} \cdot \{03\} = \{0D\} \oplus (\{0D\} \cdot \{02\}) = 00001101 \oplus 00011010 = 00010111$. Then

$$\begin{aligned} \{09\} \cdot \{02\} &= 00010010 \\ \{0E\} &= 00001110 \\ \{0B\} &= 00001011 \\ \{0D\} \cdot \{03\} &= \underline{00010111} \\ &00000000 \end{aligned}$$

For the third equation, we have $\{0D\} \cdot \{02\} = 00011010$; and $\{0B\} \cdot \{03\} = \{0B\} \oplus (\{0B\} \cdot \{02\}) = 00001011 \oplus 00010110 = 00011101$. Then

$$\begin{aligned} \{0D\} \cdot \{02\} &= 00011010 \\ \{09\} &= 00001001 \\ \{0E\} &= 00001110 \\ \{0B\} \cdot \{03\} &= \underline{00011101} \\ &00000000 \end{aligned}$$

For the fourth equation, we have $\{0B\} \cdot \{02\} = 00010110$; and $\{0E\} \cdot \{03\} = \{0E\} \oplus (\{0E\} \cdot \{02\}) = 00001110 \oplus 00011100 = 00010010$. Then

$$\{0B\} \cdot \{02\} = 00010110$$

$$\begin{array}{rcl}
\{0D\} & = & 00001101 \\
\{09\} & = & 00001001 \\
\{0E\} \cdot \{03\} & = & \underline{00010010} \\
& & 00000000
\end{array}$$

5.2 a. {01}

b. We need to show that the transformation defined by Equation 5.2, when applied to $\{01\}^{-1}$, produces the correct entry in the S-box. We have

$$\begin{array}{c}
\left[\begin{array}{cccccccc|c}
1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0
\end{array} \right] \oplus \left[\begin{array}{c} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{array} \right] = \left[\begin{array}{c} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{array} \right] \oplus \left[\begin{array}{c} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{array} \right] = \left[\begin{array}{c} 0 \\ 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{array} \right]
\end{array}$$

The result is {7C}, which is the same as the value for {01} in the S-box (Table 5.4a).