TMA4140
DISKRET MATEMATIKK – DISCRETE MATHEMATICS
NTNU, HØST/FALL2020

Solutions Exercise Set 4

Exercise/Oppgave

1. *Use the rules of inference to show that the following argument is true:*

$$\neg(\neg p \vee q) \wedge (\neg z \to \neg s) \wedge ((p \wedge \neg q) \to s) \wedge (\neg z \vee r) \to r$$

Solution. Using the rules of inference, we have

	Step	Reason
1	$\neg(\neg p \vee q)$	Premise
2	$p \wedge \neg q$	DeMorgan's Law on (1)
3	$(p \wedge \neg q) \to s$	Premise
4	s	Modus Ponens from (2) and (3)
5	$\neg z \to \neg s$	Premise
6	$s \to z$	Contrapositive. Equivalence of (5)
7	z	Modus Ponens from (4) and (6)
8	$\neg z \vee r$	Premise
9	$z \to r$	Equivalence of (8)
10	r	Modus Ponens from (7) and (9)

□

Exercise/Oppgave

2. *Let* $C := \{n \in \mathbb{N} \mid n \text{ is a multiple of } 12\}$ *and*

$$D := \{n \in \mathbb{N} \mid n \text{ is a multiple of } 2 \text{ and } n \text{ is a multiple of } 6\}.$$

Which of the statements is true: $C \subset D$, $D \subset C$, $C = D$. *Provide a detailed answer.*

Proof. We will prove that $C \subset D$. Let $n \in C$. By definition of being a multiple, we have that $n = 12m$ for a $m \in \mathbb{N}$. Note that $n = 12m = 6(2m) = 2(6m)$. In particular, we have that there exist two $s, t \in \mathbb{N}$ such that $n = 6s$ and $n = 2t$. We conclude that n is both a multiple of 2 and of 6, and so $n \in D$.

On the other hand, $D \not\subset C$. Indeed, it is clear that $6 \in D$ but 6 is not a multiple of 12. □

Exercise/Oppgave

3. *Let* x *and* y *be positive integers. Define the function* F *recursively:*

$$F(x,y) = \begin{cases} 0, & x < y \\ F(x-y, y) + 1, & y \leq x \end{cases}$$

Date: September 14, 2020.

Compute explicitly $F(2,3), F(3,2), F(23,6), F(14,3), F(15,3)$. *Is* F *injective? Justify your answer.*

Proof. Solution By definition of F, we have

(1) $F(2,3) = 0$ since $2 < 3$.
(2) $F(3,2) = F(3-2,3) + 1 = F(1,3) + 1 = 1$.
(3) $F(23,6) = F(17,6) + 1 = F(11,6) + 2 = F(5,6) + 3 = 3$.
(4) $F(14,3) = F(11,3) + 1 = F(8,3) + 2 = F(5,3) + 3 = F(2,3) + 4 = 4$.
(5) $F(15,3) = F(12,3) + 1 = F(9,3) + 2 = F(6,3) + 3 = F(3,3) + 4 = F(0,3) + 5 = 5$.

We have that F is not injective, since $F(1,2) = 0 = F(2,3)$, and $(1,2) \neq (2,3)$. □

Exercise/Oppgave
4. Section/Sektion 4.1: *6, 17d, 18d, 39b, 44*

Proof. Solution

- 4.1.6. Assume that $a|c$ and $b|d$. By definition, this means that there exist integers x, y such that $ax = c$ and $by = d$. Multiplying these two equations, we get that $axby = cd$. This is equivalent to say that $ab(xy) = cd$. Since we have found an integer xy such that $ab(xy) = cd$, we conclude that $ab|cd$.
- 4.1.17d. Assume that $a \equiv 4 \pmod{13}$ and $b \equiv 9 \pmod{13}$. Then $2a \equiv 8 \pmod{13}$ and $3b \equiv 27 \pmod{13}$, and hence $2a + 3b \equiv 35 \pmod{13}$. Noticing that $35 \equiv 9 \pmod{13}$, then if $c = 9$, we have that $c = 2a + 3b \pmod{13}$.
- 4.1.18d. Assume that $a \equiv 11 \pmod{19}$ and $b \equiv 3 \pmod{19}$. Then $7a \equiv 77 \pmod{19}$ and $3b \equiv 9 \pmod{19}$, and hence $7a + 3b \equiv 86 \pmod{19}$. Noticing that $86 \equiv 10 \pmod{19}$, then if $c = 10$, we have that $c = 7a + 3b \pmod{19}$.
- 4.1.39b. Note that

$$\begin{aligned} (3^4 \pmod{17})^2 \pmod{11} &\Leftrightarrow (81 \pmod{17})^2 \pmod{11} \\ &\Leftrightarrow 13^2 \pmod{11} \\ &\Leftrightarrow 2^2 \pmod{11} \\ &\Leftrightarrow 4. \end{aligned}$$

- 4.1.44. Assume that n is an integer. We know that we have that $n \equiv a \pmod 4$, for $0 \leq a \leq 3$. This implies that $n^2 \equiv a^2 \pmod 4$. Note that
  - If $a = 0$, then $a^2 \equiv 0 \pmod 4$.
  - If $a = 1$, then $a^2 \equiv 1 \pmod 4$.
  - If $a = 2$, then $a^2 \equiv 0 \pmod 4$.
  - If $a = 3$, then $a^2 \equiv 1 \pmod 4$.

  Since these are all the cases, we conclude that if n is an integer then $n^2 \equiv 0$ or $1 \pmod 4$.

□

Exercise/Oppgave
5. Section/Sektion 4.2: *3b, 7b, 24a*

Solution.

- 4.2.3b. We will convert $(1000000001)_2$ to a decimal expansion. We have that

$$(1000000001)_2 = 1 \cdot 2^9 + 1 \cdot 2^0 = 513.$$

- 4.2.7b. We will convert $(135\text{AB})_{16}$ to a binary expansion. We replace each hexadecimal digit by a block of four binary digits. Then

$$(135\text{AB})_{16} = (000100011010110101011)_2.$$

- 4.2.24a. For the sum, we have

$$\begin{array}{rccc} & 1 & A & E \\ + & B & B & C \\ \hline & D & 6 & A \end{array}$$

For the case of the product, we first convert to decimal expansion:

$$(1AE)_{16} \cdot (BBC)_{16} = (430)_{10} \cdot (3004)_{10} = (1291720)_{10} = (13B5C8)_{16}.$$

□

Exercise/Oppgave

6. Section/Sektion 4.3: *6, 12, 33c, d, 39e, 49*

Solution.

- 4.3.6. Since there are less factors 5 in 100! compared with the factors 2, the number of zeros at the end of 100! is given by the number of 5 factors in 100!. The factors 5 will appear in the integers 5, 10, 15,..., 95, 100. However, the integers 25, 50, 75 and 100 will give us an additional factor 5 since those integers are divisible by $25 = 5^2$. Since no integer will give a contribution of three factors since $5^3 = 125$, then the number of 5 factors in 100! is equal to $20 + 4 = 24$.
- 4.3.12. Let n be a positive integer. Consider the sequence of n consecutive numbers given by

$$(n+1)! + 2, (n+1)! + 3, \ldots, (n+1)! + (n+1).$$

Note that the terms of the sequence are of the form $(n+1)! + k$, where $2 \leq k \leq n+1$. In particular, for $2 \leq k \leq n+1$, it is clear that $k|(n+1)!$ and $k|k$. Hence $k|(n+1)! + k$. We conclude that $(n+1)! + k$ is composite for all $2 \leq k \leq n+1$.

- 4.3.33c. We will use the Euclid's algorithm in order to find $\gcd(1001, 1331)$. We have that

$$\begin{aligned} 1331 &= 1 \cdot 1001 + 330 \\ 1001 &= 3 \cdot 330 + 11 \\ 330 &= 30 \cdot 11 + 0 \end{aligned}$$

Hence $\gcd(1001, 1331) = 11$.

- 4.3.33d. We will use the Euclid's algorithm in order to find $\gcd(12345, 54321)$. We have that

$$\begin{aligned} 54321 &= 4 \cdot 12345 + 4941 \\ 12345 &= 2 \cdot 4941 + 2463 \\ 4941 &= 2 \cdot 2463 + 15 \\ 2463 &= 164 \cdot 15 + 3 \\ 15 &= 5 \cdot 3 + 0 \end{aligned}$$

Hence $\gcd(12345, 54321) = 3$.

- 4.3.39e. e) 117,213 First, we use the Euclid's algorithm in order to find the greatest common divisor. We have

$$\begin{aligned} 213 &= 1 \cdot 117 + 96 \\ 117 &= 1 \cdot 96 + 21 \\ 96 &= 4 \cdot 21 + 12 \\ 21 &= 1 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0. \end{aligned}$$

  Hence $\gcd(213, 117) = 3$. Reversing the algorithm, we have that

$$\begin{aligned} 3 &= 12 - 1 \cdot 9 \\ &= 12 - 1 \cdot (21 - 1 \cdot 12) \\ &= 2 \cdot 12 + (-1) \cdot 21 \\ &= 2 \cdot (96 - 4 \cdot 21) + (-1) \cdot 21 \\ &= (-9) \cdot 21 + 2 \cdot 96 \\ &= (-9) \cdot (117 - 1 \cdot 96) + 2 \cdot 96 \\ &= 11 \cdot 96 + (-9) \cdot 117 \\ &= 11 \cdot (213 - 1 \cdot 117) + (-9) \cdot 117 \\ &= 11 \cdot 213 + (-20) \cdot 117. \end{aligned}$$

  Hence $3 = 11 \cdot 213 + (-20) \cdot 117$.
- 4.3.49. Consider the product of three consecutive integers. This integer can be written as $n(n+1)(n+2)$. It is clear that at least one of n, $n+1$ and $n+2$ must be divisible by 2. On the other hand, it is also clear that exactly one of n, $n+1$ and $n+2$ must be divisible by 3. Since 2 and 3 are prime factors of $n(n+1)(n+2)$, then we conclude that $n(n+1)(n+2)$ is divisible by $2 \cdot 3 = 6$.

□

Exercise/Oppgave
7. Section/Sektion 4.4: *5b, c, 8, 11a, b*

Solution.
- 4.4.5b. Using Euclid's algorithm, we have

$$\begin{aligned} 141 &= 7 \cdot 19 + 8 \\ 19 &= 2 \cdot 8 + 3 \\ 8 &= 2 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1. \end{aligned}$$

Going backwards, we get that 1 can be written as a linear combination as follows:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - 1 \cdot (8 - 2 \cdot 3) \\ &= 3 \cdot 3 + (-1) \cdot 8 \\ &= 3 \cdot (19 - 2 \cdot 8) + (-1) \cdot 8 \\ &= (-7) \cdot 8 + 3 \cdot 19 \\ &= (-7) \cdot (141 - 7 \cdot 19) + 3 \cdot 19 \\ &= (-7) \cdot 141 + 52 \cdot 19. \end{aligned}$$

Hence $1 = (-7) \cdot 141 + 52 \cdot 19$. We conclude that the inverse of 19 modulo 141 is 52.

- 4.4.5c. Using Euclid's algorithm, we have

$$\begin{aligned} 89 &= 1 \cdot 55 + 34 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

Going backwards, we get that 1 can be written as a linear combination as follows:

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - (5 - 1 \cdot 3) \\ &= 2 \cdot 3 + (-1) \cdot 5 \\ &= 2 \cdot (8 - 1 \cdot 5) + (-1) \cdot 5 \\ &= (-3) \cdot 5 + 2 \cdot 8 \\ &= (-3) \cdot (13 - 1 \cdot 8) + 2 \cdot 8 \\ &= (-3) \cdot 13 + 5 \cdot 8 \\ &= (-3) \cdot 13 + 5 \cdot (21 - 1 \cdot 13) \\ &= (-8) \cdot 13 + 5 \cdot 21 \\ &= (-8) \cdot (34 - 1 \cdot 21) + 5 \cdot 21 \\ &= (-8) \cdot 34 + 13 \cdot 21 \\ &= (-8) \cdot 34 + 13 \cdot (55 - 1 \cdot 34) \\ &= (-21) \cdot 34 + 13 \cdot 55 \\ &= (-21) \cdot (89 - 1 \cdot 55) + 1355 \\ &= (-21) \cdot 89 + 34 \cdot 55. \end{aligned}$$

Hence $1 = (-21) \cdot 89 + 34 \cdot 55$. We conclude that the inverse of 55 modulo 89 is 34.

- 4.4.8. Assume that $d := \gcd(a, m) > 1$. We will show that the inverse of a modulo m does not exist. We proceed by contradiction assuming that such inverse exists. This means that there is an integer r such that $ar \equiv 1 \pmod{m}$. This is equivalent to say that $m|ar - 1$, i.e., there exists $t \in \mathbb{Z}$ such that $mt = ar - 1$. Now, using that d is a common divisor of a and m, we have that d also divides mt and ar. This implies that d divides $1 = ar - mt$ and hence $d = 1$. This contradicts that $d > 1$. Then our initial assumption is not true. We conclude that a does not have an inverse modulo m.
- 4.4.11a. We will solve $19x \equiv 4 \pmod{141}$. Since 52 is the inverse of 19 modulo 141 we have

$$x \equiv 52 \cdot 19x \equiv 52 \cdot 4 \equiv 208 \equiv 67 \pmod{141}.$$

  The solution is given by all the integers x such that $x \equiv 67 \pmod{141}$.
- 4.4.11b. We will solve $55x \equiv 34 \pmod{89}$. Since 34 is the inverse of 55 modulo 89, we have

$$x \equiv 34 \cdot 55x \equiv 34 \cdot 34 \equiv 1156 \equiv 88 \pmod{89}.$$

  The solution is given by all the integers x such that $x \equiv 88 \pmod{89}$.

□