TMA4140
DISKRET MATEMATIKK – DISCRETE MATHEMATICS
NTNU, HØST/FALL2020

Exercise Set 5 / Øving 5

The solutions must be submitted via OVSYS (to the assigned group/TA).
Løsningene må sendes inn via OVSYS (til den tildelte gruppen/TA).

Deadline for submission:	**Wednesday, 30 September, 1:00pm**
Innleveringsfrist:	**Onsdag, 30. September, kl. 13:00**

Textbook: K. H. Rosen, *Discrete Mathematics and Its Applications*, 8. edition

Exercise/Oppgave

1. *A* fundamental product *of the sets* $A_1, A_2, \dots, A_n$ *is defined to be a set of the form* $A_1^{\epsilon_1} \cap A_2^{\epsilon_2} \cap \cdots \cap A_n^{\epsilon_n}$, *where* $A_i^{\epsilon_i}$ *is either the set* A_i *or its complement* $\overline{A_i}$.

i) *List all fundamental products of three sets* A_1, A_2, A_3

ii) *Find the number of fundamental products of* n *sets* $A_1, A_2, \dots, A_n$

Solution. i) Note that for each ϵ_i, we have two choices: either taking the complement or just the set. Then the fundamental products of A_1, A_2, A_3 are the following eight sets:

$$A_1 \cap A_2 \cap A_3,\ A_1 \cap A_2 \cap \overline{A_3},\ A_1 \cap \overline{A_2} \cap A_3,\ A_1 \cap \overline{A_2} \cap \overline{A_3},$$
$$\overline{A_1} \cap A_2 \cap A_3,\ \overline{A_1} \cap A_2 \cap \overline{A_3},\ \overline{A_1} \cap \overline{A_2} \cap A_3,\ \overline{A_1} \cap \overline{A_2} \cap \overline{A_3}.$$

ii) Now consider n sets $A_1, \dots, A_n$. Note that a fundamental product is determined by the n-tuple $(\epsilon_1, \dots, \epsilon_n)$, where ϵ_i establishes if we take the set A_i of its complement in order to give a fundamental product. Since ϵ_i has two possible options for $i = 1, \dots, n$, then the number of fundamental products of n sets is given by 2^n. We can check that the number of fundamental products of three sets is $2^3 = 8$ as we obtained in part i). □

Exercise/Oppgave

2. *Show that the function* h *is surjective if and only if the following holds: for every two functions* g_1 *and* g_2 *with domain of* g_1 *equal to the domain of* g_2 *equal to the codomain of* h, *the following right cancellation is satisfied: if* $g_1h = g_2h$ *then* $g_1 = g_2$.

Solution. ⇒) Assume that $h : A \to B$ is surjective. Consider two functions $g_1, g_2 : B \to C$ such that $g_1 \circ h = g_2 \circ h$. Take $b \in B$. Since h is surjective, there is $a \in A$ such that $h(a) = b$. By hypothesis, we have that $(g_1 \circ h)(a) = (g_2 \circ h)(a)$. By definition of composition of functions, we have that $(g_1 \circ h)(a) = g_1(h(a)) = g_1(b)$ and $(g_2 \circ h)(a) = g_2(b)$. Hence $g_1(b) = g_2(b)$. Since this holds for any $b \in B$, we conclude that $g_1 = g_2$.

Date: September 20, 2020.

$\Leftarrow$) Assume that any two functions $g_1, g_2 : B \to C$ such that $g_1 \circ h = g_2 \circ h$ imply that $g_1 = g_2$. We shall prove that $h : A \to B$ is surjective. Proceed by contradiction. Assume that h is not surjective, i.e., there exists $b_0 \in B$ such that there is no $a \in A$ such that $h(a) = b_0$. Consider the particular case that $B = C$, $g_1 = \mathrm{id}_B$, and $g_2 : B \to B$ is a function such that $g_2(b) = b$ for any $b \in B$ and $b \neq b_0$, and $g(b_0)$ is defined to be any other element of B different from b_0. This is possible in the case that B has more than one element (if $|B| = 1$ then obviously any non-empty function h is surjective and the result follows). It is clear that $g_1(b) = g_2(b)$ for $b \neq b_0$. Now, since $h(a) \neq b_0$ for any $a \in A$, we then have that $g_1(h(a)) = g_2(h(a))$, for any $a \in A$. Now, by assumption, this implies that $g_1 = g_2$ but this is a contradiction since $g_1(b_0) = b_0 \neq g_2(b_0)$. We conclude that our assumption is false. Therefore h is surjective.

□

Exercise/Oppgave

3. *Show that the function $f(n) = 5n^3 + 7n^2 - n + 7 \in O(n^3)$.*

Solution. Using the definition, we say that $f(n)$ is $O(n^3)$ if there are constants C and k such that $|f(n)| \leq Cn^3$ whenever $x > k$. We will give these constants. Take $k = 7$. Now, if $n > 7$, by triangular inequality and using that $n^3 > n$, we have

$$|f(n)| \leq 5n^3 + 7n^2 + n + 7 \leq 5n^3 + n^3 + n^3 + n^3 = 8n^3.$$

Taking $C = 8$, we have that $|f(n)| \leq Cn^3$ when $n > 7$. We conclude that $f(n)$ is $O(n^3)$ as we wanted to show. □

Exercise/Oppgave

4. Section/Sektion 4.4: *5b, c, 8, 11a, b, 21, 33, 37a*

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 $x \equiv 88 \pmod{89}$.
- 4.4.21. We will find the solution for the system
$$x \equiv 1 \pmod{2}, \quad x \equiv 2 \pmod{3}, \quad x \equiv 3 \pmod{5}, \quad x \equiv 4 \pmod{11}.$$
According to the proof of the Chinese Remainder Theorem, we set
$$\begin{aligned} a_1 &= 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_4 = 4 \\ m_1 &= 2, \quad m_2 = 3, \quad m_3 = 5, \quad m_4 = 11 \\ m &= 2 \cdot 3 \cdot 5 \cdot 11 = 330 \\ M_1 &= 330/2 = 165, \quad M_2 = 330/3 = 110, \quad M_3 = 330/5 = 66, \quad M_4 = 330/11 = 30 \end{aligned}$$
Since $\gcd(m_i, M_i) = 1$ for $i = 1, 2, 3, 4$, we can find the inverse $y_i \mod m_i$, i.e. y_i is an integer such that $M_i y_i \equiv 1 \pmod{m_i}$, for $i = 1, 2, 3, 4$.
  - $i = 1$: $165y_1 \equiv y_1 \equiv 1 \pmod{2}$. Then we can take $y_1 = 1$.
  - $i = 2$: $110y_2 \equiv 2y_2 \equiv 1 \pmod{3}$. We can easily see that 2 is the inverse mod 3 of 2. Multiplying by 2 we have $2(2y_2) \equiv 4y_2 \equiv y_2 \equiv 2 \pmod{3}$. So, we can take $y_2 = 2$.
  - $i = 3$: $66y_3 \equiv y_3 \equiv 1 \pmod{5}$. So, we can take $y_3 = 1$.
  - $i = 4$: $30y_4 \equiv 8y_4 \equiv 1 \pmod{11}$. We can easily see that 7 is the inverse mod 11 of 8 since $7 \cdot 8 \equiv 56 \equiv 1 \pmod{11}$. Then we have $7(8y_4) \equiv y_4 \equiv 7 \pmod{3}$. So, we can take $y_4 = 7$.

  Finally, the solutions to the system are those x such that
$$\begin{aligned} x &\equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4 \\ &\equiv 1 \cdot 165 \cdot 1 + 2 \cdot 110 \cdot 2 + 3 \cdot 66 \cdot 1 + 4 \cdot 30 \cdot 7 \\ &\equiv 1643 \equiv 323 \pmod{330}. \end{aligned}$$
- 4.4.33. Note that 13 is a primer number such that $\gcd(7, 13) = 1$. By the Fermat's little theorem, we have that $7^{12} \equiv 1 \pmod{13}$. Taking 10th-power, we have
$$(7^{12})^{10} \equiv 7^{12 \cdot 10} = 7^{120} \equiv 1^{10} \equiv 1 \pmod{13}.$$
Finally, multiplying by 7 we conclude that
$$7^{121} = 7 \cdot 7^{120} \equiv 7 \cdot 1 \equiv 7 \pmod{13}.$$
Hence $7^{121} \bmod 13$ is equal to 7.
- 4.4.37a. Note that 11 is a primer number such that $\gcd(2, 11) = 1$. By the Fermat's little theorem, we have that $2^{10} \equiv 1 \pmod{11}$. Since $2^{340} = (2^{10})^{34}$, we have that
$$2^{340} \equiv (2^{10})^{34} \equiv 1^{34} \equiv 1 \pmod{11}.$$

□

Exercise/Oppgave

5. Section/Sektion 4.5: *12*

Solution. The power generator is a method for generating pseudorandom numbers. To use the power generator, parameters p and d are specified, where p is a prime, d is a positive integer such that $p \not| d$, and a seed x_0 is specified. The pseudorandom numbers $x_1, x_2, \ldots$ are generated using the recursive definition $x_{n+1} \equiv x_n^d \pmod{p}$. We give the the sequence of pseudorandom numbers generated by the power generator with $p = 11$, $d = 2$, and seed $x_0 = 3$.

$$\begin{aligned} x_1 &\equiv 3^2 \equiv 9 \pmod{11}, \\ x_2 &\equiv 9^2 \equiv 81 \equiv 4 \pmod{11}, \\ x_3 &\equiv 4^2 \equiv 16 \equiv 5 \pmod{11}, \\ x_4 &\equiv 5^2 \equiv 25 \equiv 3 \pmod{11}. \end{aligned}$$

Hence $x_0 = x_4$ and the sequence is periodic. □

Exercise/Oppgave
6. Section/Sektion 4.6: *26*

Solution. We first find the decryption exponent d, which is the inverse of $e = 17$ modulo $52 \cdot 60 = 3120$. Using Euclid's algorithm, we find that $2 \cdot 3120 - 367 \cdot 17 = 1$, and our decryption exponent, the inverse of e, is given by

$$d \equiv -367 \equiv 2753 \pmod{3120}.$$

Consequently, to decrypt a block c, we compute $m \equiv c^d \pmod{3233}$. Using computational aid, we have

$$\begin{aligned} 3185^{2753} &\equiv 1816 \pmod{3233}, \\ 2038^{2753} &\equiv 2008 \pmod{3233}, \\ 2460^{2753} &\equiv 1717 \pmod{3233}, \\ 2550^{2753} &\equiv 0411 \pmod{3233}, \end{aligned}$$

Hence, the decrypted message is 1816 2008 1717 0411. The translation is SQUIRREL. □

Exercise/Oppgave
7. Section/Sektion 6.1: *27, 46*

Solution.

- 6.1.27. Note that, for each state, the representative can be chosen by one of the governor and the two senators. This mean that for each state, we have 3 options. Since this applies to each of the 50 states and the choice of each state is independent of the other states, the number of ways that the committee can be formed is equal to 3^{50}.
- 6.1.46. We count the possible linear order and then we divide by the number of times that each linear order (i.e. not taking into account that the table is circular) is considered. One notes that, there are 10 possibilities for the first chair; 9 possibilities for the second chair, 8 possibilities for the third chair, and 7 possibilities for the last chair. Then the number of linear order is $10 \cdot 9 \cdot 8 \cdot 7$. Finally, since the table has four chairs, then every linear order is counted 4 times. Hence the number of ways to seat the people is

$$\frac{10 \cdot 9 \cdot 8 \cdot 7}{4} = 1260.$$

□

Exercise/Oppgave

8. Section/Sektion 6.2: *13, 18, 20*

Solution.

- 6.2.13. Recall that if $(a, b, c), (x, y, z) \in \mathbb{R}^3$, then the coordinates of the midpoint of the segment defined by the two points is given by

  $$\left(\frac{a+x}{2}, \frac{b+y}{2}, \frac{c+z}{2}\right).$$

  Then, two points with integer coordinates will have a midpoint with integer coordinates if and only if, each pair of components, $(a, x), (b, y), (c, z)$ has the same parity.

  Take one of the given nine points in $\mathbb{R}^3$ with integer coordinates (x, y, z). Look at the first coordinate of the remaining eight points. By the pigeonhole principle, there are at least four of such points with the same parity that of x. If there are five of more of such points, take a subset of five points and forget of the other points; if there are exactly four points, take the set of the original point (x, y, z) and the four such points. In any case, we have a subset of five points such that their first coordinate has the same parity that the first coordinate of the other points. Doing this, we will assure that the first coordinate of the midpoint of any pair of points will be an integer.

  We repeat the argument with the second coordinate. Take any point belonging to the subset of five points considered above. By the pigeonhole principle, there are at least two points of the other four points such that the second coordinate of each point has the same parity that the first point. Again, if there three of more of such points, we take a subset of three points and forget of the other points; if there are exactly two of such points, take the set of the first point and the two such points. In any case, we have a subset of three points such that all the first coordinates have the same parity, and all the second coordinates have the same parity. Then, the midpoint of any pair of points in this new subset will have integer coordinates on the first and second components.

  Finally, repeating the above argument, by the pigeonhole principle, there are at least two points such that their third component has the same parity. Since these points are chosen such that their first coordinates have the same parity, and their second coordinates have also the same parity, we conclude that the midpoint of these two points will have integer coordinates, as we wanted to show.
- 6.2.18. The answer is 5. Note that we can divide the set in the integers $A = \{1, 3, 5, 7\}$ and $B = \{9, 11, 13, 15\}$. Note that for each element in the first set, there exists a unique element in the second set such that the sum of the two elements is 16. Choosing four elements, it is possible that our choice is the set A and this subset does not satisfy the desired property. Now, note that we can divide our set in four subsets:

  $$A_1 = \{1, 15\}, A_2 = \{3, 13\}, A_3 = \{5, 11\}, A_4 = \{7, 9\}.$$

  If we choose a subset C of size 5, by the pigeonhole principle, there exists $i \in \{1, 2, 3, 4\}$ such that $A_i \subset C$. We conclude that any C of size 5 will have a pair of elements such that their sum is equal to 16.
- 6.2.20. a) By contradiction. Assume that there are at most four male students and at most four female students. This implies that there are at most eight students in the discrete mathematics class. However, this contradicts that the class has nine students. Hence, our initial assumption must be false and its negation must be true. Such negation is precisely

that there are at least five male students or at least five female students. This argument is similar to the proof of the pigeonhole principle.

b) By contradiction. Assume that there are at most two male students and at most six female students. This implies that there are at most eight students in the discrete mathematics class. However, this contradicts that the class has nine students. Hence, our initial assumption must be false and its negation must be true. Such negation is precisely that there are at least three male students or at least seven female students.

□