NTNU
Norwegian University of
Science and Technology

Department of Mathematical Sciences

# Examination paper for **TMA4140 Discrete Mathematics**

**Academic contact during examination:** Navn Navnesen

**Phone:** +47 XX XX XX XX

**Examination date:** December 2022

**Examination time (from–to):** 00:00 - 23:59

**Permitted examination support material:** Permitted examination aids code C: Specified printed and hand-written support material is allowed. A specific basic calculator is allowed. *We specify that it is allowed to bring a stamped yellow A4 sheet with your own handwritten formulas and notes. The calculators allowed for examination aids code C is listed on the NTNU website.*

!!! Note that this is a mock exam for fall 2022, not the real exam !!!

**Language:** English

**Number of pages:** 14

**Number of pages enclosed:** 0

**Checked by:**

| **Informasjon om trykking av eksamensoppgave** | |
|---|---|
| **Originalen er:** | |
| **1-sidig** ☐ | **2-sidig** ☒ |
| **sort/hvit** ☐ | **farger** ☒ |
| **skal ha flervalgskjema** ☐ | |

Date Signature

This exam has the following structure:

| | | |
|---|---|---|
| Problem 1: | Logic | 10 points |
| Problem 2: | Sets | 10 points |
| Problem 3: | Functions | 10 points |
| Problem 4: | Boolean algebra | 10 points |
| Problem 5: | Relations | 10 points |
| Problem 6: | Induction | 10 points |
| Problem 7: | Combinatorics | 10 points |
| Problem 8: | Graphs and trees | 10 points |
| Problem 9: | Number theory | 10 points |
| Problem 10: | Finite state machines and automata | 10 points |
| **Total:** | | **100 points** |

**The answer to every problem requires a detailed argument/computation.**

## Problem 1 **Logic** (10 points)

a. (3 points) Use truth tables to determine which of the following statements are tautologies and which are contradictions (1 point each):

   i) $q \vee (q \to \neg q)$

   ii) $\neg((\neg r \wedge r) \to s)$

   iii) $((t \to s) \to t) \to t$

b. (7 points) Let $p, q, r, s, t, u$ be primitive statements. Provide a step by step verifications of the inference

$$\Big((\neg p \vee q) \to r\Big) \wedge \Big(r \to (s \vee t)\Big) \wedge \Big(\neg s \wedge \neg u\Big) \wedge \Big(\neg u \to \neg t\Big) \to p$$

**Solution.**

a. i) $q \vee (q \to \neg q)$

| $q$ | $\neg q$ | $(q \to \neg q)$ | $q \vee (q \to \neg q)$ |
|---|---|---|---|
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 |

A tautology.

ii) $\neg((\neg r \wedge r) \to s)$

| $r$ | $\neg r$ | $\neg r \wedge r$ | $s$ | $(\neg r \wedge r) \to s$ | $\neg((\neg r \wedge r) \to s)$ |
|---|---|---|---|---|---|
| 1 | 0 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 0 | 1 | 0 |
| 1 | 0 | 0 | 0 | 1 | 0 |

A contradiction.

iii) $((t \to s) \to t) \to t$

| $t$ | $s$ | $t \to s$ | $(t \to s) \to t$ | $((t \to s) \to t) \to t$ |
|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 | 1 |
| 0 | 1 | 1 | 0 | 1 |
| 0 | 0 | 1 | 0 | 1 |

A tautology.

b. From the laws of inference we have:

| | **Step** | **Reason** |
|---|---|---|
| 1 | $\neg s \wedge \neg u$ | Premise |
| 2 | $\neg u$ | Conjunctive Simplification from (1) |
| 3 | $\neg u \Rightarrow \neg t$ | Premise |
| 4 | $\neg t$ | Modus Ponens from (2) and (3) |
| 5 | $\neg s$ | Conjunctive Simplification from (1) |
| 6 | $\neg s \wedge \neg t$ | Conjunction from (4) and (5) |
| 7 | $\neg(s \vee t)$ | DeMorgan's Law from (6) |
| 8 | $r \Rightarrow (s \vee t)$ | Premise |
| 9 | $\neg r$ | Modus Tollens from (7) and (8) |
| 10 | $(\neg p \vee q) \Rightarrow r$ | Premise |
| 11 | $\neg(\neg p \vee q)$ | Modus Tollens from (9) and (10) |
| 12 | $p \wedge \neg q$ | DeMorgan's Law and Double Negation from (11) |
| 13 | $p$ | Conjunctive Simplification from (12) |

**Problem 2** **Sets** (10 points)

a. (4 points) Let $X, Y$ be arbitrary sets. Use the laws of set theory to show that:

$$\text{If} \quad (X \cup Y) \subseteq (X \cap Y) \quad \text{then} \quad X = Y.$$

b. (6 points) Use the laws of set theory to show that for sets $X, Y, Z$ we have that

$$(Y - Z) \subseteq \overline{X} \text{ if and only if } (X \cap Y) \subseteq Z.$$

**Solution.**

a. By the law of distributivity we have that $((X \cap X) \cup (X \cap Y)) \subseteq (X \cap X \cap Y)$. Simplifying we see that $X \cup (X \cap Y) = X$, then $X \subseteq (X \cap X \cap Y)$ and $X \subseteq (X \cap Y)$. By definition $X \cap Y \subseteq X$. This implies that $X = X \cap Y$. Similarly we have that $Y = Y \cap X$. Then $X = Y$.

b. To prove an if and only if statement we must show that each condition implies the other. We will start by assuming that $(Y - Z) \subseteq \overline{X}$ is true and that $(X \cap Y) \subseteq Z$ follows. Consider the case where $(X \cap Y) \subseteq Z$ is not true i.e. that $(X \cap Y) \nsubseteq Z$. Then $\exists x \in X \cap Y$ such that $x \notin Z$. Because $x \in X \cap Y$ we know that $x \in Y$ and thus $x \in Y - Z$. But $Y - Z \subseteq \overline{X}$ and this implies $x \in \overline{X}$, a contradiction. Then if $(Y - Z) \subseteq \overline{X}$ is true $(X \cap Y) \subseteq Z$ must also be true.

   We now assume that $(X \cap Y) \subseteq Z$ is true and show that $(Y - Z) \subseteq \overline{X}$ follows using the same approach; namely we consider the case where $(X \cap Y) \subseteq Z$ is true and that $(Y - Z) \nsubseteq \overline{X}$ in order to find a contradiction. If $(Y - Z) \nsubseteq \overline{X}$ then $\exists x \in X$ where $x \in Y - Z$ as well. This also implies that $x \in Y$, but if $x \in X$ and $x \in Y$ then $x \in X \cap Y \subseteq Z$, a contradiction. Then if $(X \cap Y) \subseteq Z$ is true $(Y - Z) \subseteq \overline{X}$ must also be true.

**Problem 3** **Functions** (10 points)

a. (5 points) Let $g : A \to B$ and $f : B \to C$ be two functions. Show that if $g$ and $f$ are both injective, then $f \circ g : A \to C$ is injective.

b. (5 points) Let $f : A \to B$ and $g : B \to C$. Show that if $g \circ f : A \to C$ is surjective, then $g$ is surjective.

**Solution.**

a. To show that $f \circ g : A \to C$ is injective we must show that $\forall a, b \in A$ $f(g(a)) = f(g(b)) \implies a = b$. Consider the function $f$, we know that $f$ is injective (that is: $f(a) = f(b) \implies a = b$. Then from this we know that the statement $f(g(a)) = f(g(b)) \implies g(a) = g(b)$, but $g$ is also injective which implies that $a = b$. Then $f \circ g : A \to C$ is injective.

b. We start by assuming that $g \circ f : A \to C$ is surjective and then consider the case where $g$ is not surjective. $g \circ f : A \to C$ is surjective means that $\forall c \in C$, $\exists a \in A$ s.t. $g(f(a)) = c$ where $f(a) \in B$. But if $g$ is not surjective this implies that $\exists c \in C$ s.t. $\neg\exists f(a) \in B$ s.t. $g(f(a)) = c$ which contradicts the surjectivity of $g \circ f : A \to C$. Then if $g \circ f : A \to C$ is surjective $g$ must also be surjective.

**Problem 4** **Boolean algebra** (10 points)

a. (1 point) Let $\mathbb{B}$ be a Boolean algebra. Simplify the following Boolean expression

$$(x \cdot x \cdot x \cdot y \cdot y + \overline{x} \cdot y \cdot y) \cdot \overline{(x \cdot x + x \cdot \overline{y} \cdot \overline{y} \cdot \overline{y})}.$$

b. (3 points) Let $\mathbb{B}$ be a Boolean algebra. Show that $x = 0$ if and only if $y = x\overline{y} + \overline{x}y$ for all $y$.

c. (6 points) Consider the set $X = \{1, 2, 4, 8\}$ and define the binary operations $+ : X \times X \to X$ and $\cdot : X \times X \to X$

$$x + y := \operatorname{lcm}(x, y) \quad \text{resp.} \quad x \cdot y := \gcd(x, y)$$

(recall define the notions of least common multiple (lcm) the greatest common divisor (gcd)) and the unary operation $^{-} : X \to X$, $x \mapsto \overline{x} := 8/x$. Is $(X, +, \cdot, ^{-}, 1, 8)$ a Boolean algebra? Provide a detailed justification for your answer.

**Solution.** Denote the Boolean algebra by $B$. The axioms are the following:

| | |
|---|---|
| Commutativity: | $(\forall x, y \in B)(x + y = y + x \text{ and } x \cdot y = y \cdot x)$ |
| Identity axioms: | $(\forall x \in B)(x + 0 = x \text{ and } x \cdot 1 = x)$ |
| Complement axioms: | $(\forall x \in B)(x + \overline{x} = 1 \text{ and } x \cdot \overline{x} = 0)$ |
| Distributivity of multiplication over addition: | $(\forall x, y, z \in B)(x \cdot (y + z) = x \cdot y + x \cdot z)$ |
| Distributivity of addition over multiplication: | $(\forall x, y, z \in B)(x + y \cdot z = (x + y) \cdot (x + z))$ |

a. We use the laws of boolean variables to simplify:

$$(x \cdot x \cdot x \cdot y \cdot y + \overline{x} \cdot y \cdot y) \cdot \overline{(x \cdot x + x \cdot \overline{y} \cdot \overline{y} \cdot \overline{y})}.$$

$x \cdot x = x$: $(x \cdot y + \overline{x} \cdot y) \cdot \overline{(x + x \cdot \overline{y})}$.

Commutative: $(y \cdot x + y \cdot \overline{x}) \cdot \overline{(x + x \cdot \overline{y})}$.

Distributive and absorption: $y \cdot (x + \overline{x}) \cdot \overline{x}$.

$x + \overline{x} = 1$: $y \cdot (1) \cdot \overline{x}$.

Identity law: $y \cdot \overline{x}$.

b. Assume that $x = 0$. Then $y = 0 \cdot \overline{y} + 1 \cdot y = y$ by dominance and identity laws. Assume that $y = x\overline{y} + \overline{x}y$ $\forall y$ and that $x \neq 0$. For example, set $y = 1$. Then $1 = x \cdot 0 + \bar{x} \cdot 1 = \bar{x}$, which is a contradiction. Thus $x = 0$.

c. In order to determine if $(X, +, \cdot, ^{-}, 1, 8)$ is a Boolean algebra we must make sure it meets the conditions required by the definition. Namely that it satisfies the commutative, distributive, identity, inverse, and inequality of special element laws.

- Commutativity follows from $\text{lcm}(x, y) = \text{lcm}(y, x)$ and $\gcd(x, y) = \gcd(y, x)$.
- Additive identity: $x + 1 = \text{lcm}(x, 1) = x$. Multiplicative identity: $x \cdot 8 = \gcd(x, 8) = x$.
- Additive inverse: We would expect that $x + \overline{x} = 8$, however consider the case where $x = 2$. Then we have that $x + \overline{x} = 4 \neq 8$. Then this is not a Boolean algebra.
- Multiplicative inverse: We would expect that $x \cdot \overline{x} = 1$, however again in the case where $x = 2$ we have that $x \cdot \overline{x} = 2 \neq 1$. Then this is not a Boolean algebra.

- Distributivity: Note that any element in $S$ can be written as $x = 2^i$, with $i \in \{0, 1, 2, 3\}$. Let $x = 2^{i_x}, y = 2^{i_y}, z = 2^{i_z}$, then:

$$\begin{aligned} x(y+z) =& \gcd(x, \operatorname{lcm}(y, z)) \\ =& \gcd(x, 2^{\max(i_y, i_z)}) \\ =& 2^{\min(i_x, \max(i_y, i_z))} \\ =& 2^{\max(\min(i_x, i_y), \min(i_x, i_z))} \\ =& \operatorname{lcm}(\gcd(x, y), \gcd(x, z)) \\ =& xy + xz, \end{aligned}$$

and

$$\begin{aligned} x + yz =& \operatorname{lcm}(x, \gcd(y, z)) \\ =& 2^{\max(i_x, \min(i_y, i_z))} \\ =& 2^{\min(\max(i_x, i_y), \max(i_x, i_z))} \\ =& \gcd(\operatorname{lcm}(x, y), \operatorname{lcm}(x, z)) \\ =& (x+y)(x+z). \end{aligned}$$

From either of the unmet laws (additive or multiplicative inverse) we can conclude that $(X, +, \cdot, ^{-}, 1, 8)$ is not a Boolean algebra.

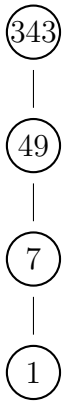
## Problem 5 **Relations** (10 points)

a. (4 points) Draw the Hasse diagram for the divisors of 343.

b. (6 points) Recall that a relation R on a set $A$ is antisymmetric if it does not contain any pair of distinct elements of $A$ each of which is related by $R$ to the other. Prove that the relation $R$ defined on the set $A$ is antisymmetric if and only if $R \cap R^{-1} \subseteq \{(a, a) \mid a \in A\}$.

**Solution.**

a. See diagram:




b. We will start by assuming that R on the set $A$ is antisymmetric and show that $R \cap R^{-1} \subseteq \{(a,a) \mid a \in A\}$. Consider the elements $b, c \in A$ such that $(b,c) \in R \cap R^{-1}$. If $(b,c) \in R^{-1}$ then $(c,b) \in R$. Then we have that $bRc$ and $cRb$ which implies that $b = c$ since R is antisymmetric. Then $(b,c) \in \{(a,a) \mid a \in A\}$ which implies that $R \cap R^{-1} \subseteq \{(a,a) \mid a \in A\}$.

   We now assume $R \cap R^{-1} \subseteq \{(a,a) \mid a \in A\}$ and show that R on the set $A$ must be antisymmetric. Consider if R is not antisymmetric. This means that $\exists (b,c) \in R$ such that $(c,b) \in R$ with $b \neq c$. If $(c,b) \in R$ then $(b,c) \in R^{-1}$ and consequently $(b,c) \in R \cap R^{-1}$. By our assumption $R \cap R^{-1} \subseteq \{(a,a) \mid a \in A\}$, but $(b,c) \in R \cap R^{-1}$ is not in $\{(a,a) \mid a \in A\}$, this is a contradiction. Then R must be antisymmetric.

**Problem 6** **Induction** (10 points)

a. (1 point) Show that for all natural numbers: $4\sum_{k=1}^{n}(k^2+2k)(k+4) = (n^2+n)(n+4)(n+5)$.

b. (3 points) Show that $\sum_{k=1}^{n} k(k!) = (n+1)! - 1$.

c. (6 points)

   i) (2 points) Show that $n^2 \geq 2n+1$ for $n > 2$.

   ii) (4 points) Then determine for which natural numbers we have $2^n \geq n^2$.

**Solution.**

a. For the base case let $n = 1$, then $4\sum_{k=1}^{1}(k^2+2k)(k+4) = (1^2+1)(1+4)(1+5)$ and $4(3)(5) = (2)(5)(6) = 60$.

   Assume this is true up to $n = i$:

   $4\sum_{k=1}^{i}(k^2+2k)(k+4) = (i^2+i)(i+4)(i+5)$.

   We then want to show that this is true for $n = i+1$:

   $4\sum_{k=1}^{(i+1)}(k^2+2k)(k+4) = [(i+1)^2+(i+1)][(i+1)+4][(i+1)+5]$ (Note that the right side of this equation simplifies to $(i+1)(i+2)(i+5)(i+6)$).

   We see that $4\sum_{k=1}^{(i+1)}(k^2+2k)(k+4) = 4\sum_{k=1}^{i}(k^2+2k)(k+4) + 4[(i+1)^2 + 2(i+1)][(i+1)+4]$.
   Using our assumption we can get rid of the summation:
   $4\sum_{k=1}^{i}(k^2+2k)(k+4) + 4[(i+1)^2+2(i+1)][(i+1)+4] = (i^2+i)(i+4)(i+5) + 4[(i+1)^2+2(i+1)][(i+1)+4]$.
   Simplifying by factoring we get $(i+5)(i+1)[i^2+8i+12] = (i+1)(i+2)(i+5)(i+6)$.
   Then it is true for $n = i+1$ and for all natural numbers that $4\sum_{k=1}^{n}(k^2+2k)(k+4) = (n^2+n)(n+4)(n+5)$.

b. For the base case let $n = 1$: $\sum_{k=1}^{1} k(k!) = (1+1)! - 1$, we have that $1(1!) = 2! - 1 = 1$.

   Assume this is true up to $n = i$:

   $\sum_{k=1}^{i} k(k!) = (i+1)! - 1$

   We then want to show that this is true for $n = i+1$:

   $\sum_{k=1}^{i+1} k(k!) = [(i+1)+1]! - 1$.

   We see that $\sum_{k=1}^{i+1} k(k!) = \sum_{k=1}^{i} k(k!) + (i+1)(i+1)! =$
   $(i+1)! - 1 + (i+1)(i+1)! = [(i+1)! + (i+1)(i+1)!] - 1 =$
   $(i+1)![i+2] - 1 = (i+2)! - 1 = [(i+1)+1]! - 1$ which is what we wanted to show. Then $\sum_{k=1}^{n} k(k!) = (n+1)! - 1$.

c. i) For the base case let $n = 3$. Then we have that $9 \geq 7$.

   Assume this is true up to $n = k : k^2 \geq 2k+1$. Then we want to show that this is true for $n = k+1 : (k+1)^2 \geq 2(k+1)+1$.

   We start with our assumption and add $2k+1$ to both sides of the inequality: $k^2+2k+1 \geq 2k+1+(2k+1)$. Note that because $n > 2$ we

have that $2k+1 \geq 7$. This allow us to replace $(2k+1)$ with anything smaller than or equal to 7 to make the equation go up.

Then we factor the left side and replace $(2k+1)$ with 2 on the right side: $(k+1)^2 \geq 2k+3 = 2(k+1)+1$, which is what we wanted to show. Then $n^2 \geq 2n+1$ for $n > 2$.

ii) Testing the natural numbers $n = 1, 2, 3, 4, 5, ...$ we see that $2^n \geq n^2$ does not hold for $n = 3$ but seems to hold beyond that. Then we will use $n = 4$ as our base case and assume $2^n \geq n^2$ holds up to $n = k : 2^k \geq k^2$. We then want to show that this holds for $n = k+1 : 2^{k+1} \geq (k+1)^2$. Starting with our assumption $2^k \geq k^2$ we multiply both sides of the inequality by 2: $2 \cdot 2^k \geq 2 \cdot k^2$ which yields $2^{k+1} \geq k^2 + k^2$. We know from i) that $k^2 \geq 2k+1$ for $k > 2$, so then we can replace $k^2$ with $2k+1$ without affecting the inequality: $2^{k+1} \geq k^2 + 2k + 1 = (k+1)^2$ which is what we wanted to show. Then $2^n \geq n^2$ for $n = 1, 2$ and all $n \geq 4$.

**Problem 7** **Combinatorics** (10 points)

a. (4 points) A string is a palindrome if the string is the same when we read it from the left and from the right, for example: *tacocat*. Let the alphabet be the symbols $\{a, b, c, d, e\}$. How many palindromes of length 11 exists over this alphabet?

b. (6 points) Let $L$ be the language $\{a, b, c\}^*$ consisting of all strings over the alphabet $\{a, b, c\}$. How many

   i) (1 point) strings in $L$ have length 6?

   ii) (2 points) strings in $L$ of length 6 have at least two $a$'s?

   iii) (3 points) strings in $L$ of length 6 are sorted (so that all $a$'s are in front of all $b$'s which are in front of all $c$'s)?

**Solution.**

a. (4 points) Any palindrome of length 11 is of the form $sx\bar{s}$ where $x$ is a single symbol, $s$ is a string of length 5 and $\bar{s}$ is the reversed string of $s$. The palindrome is then uniquely determined of the string $s$ and the symbol $x$. For each symbol in $s$ there are five options, and similarly for $x$. It follows that there are $5^6 = 15625$ different palindromes of length 11.

b. (6 points)

i) (1 point) There are three possible symbols and we are sampling six, so there are $3^6 = 729$ different strings of length six in the language $L$.

ii) (2 points) We have 729 possible strings, and we subtract the strings with none or one $a$. There are $2^6 = 64$ strings that only contains $b$'s and $c$'s. Further, if we have a string with $a$ only in the first position, then there are $2^5$ such strings. The symbol $a$ can be in six different positions, so there are $6 \cdot 2^5 = 192$ strings with exactly one $a$. In conclusion, there are $729 - 64 - 192 = 473$ different strings with at least two $a$'s.

iii) (3 points) This is an unordered sampling with repetition with $n = 3$ symbols and $k = 6$ samples. This can be visualized with 2 walls ($|$), for example as $a$'s$|b$'s$|c$'s, and 6 stars ($*$), and we get samples of the form $* * * * * *|\ |$ or $*|* * * *|*$ and so on. There are $\binom{n+k-1}{k}$ possible outcomes, and we get $\binom{8}{6} = \frac{8!}{6! \cdot 2!} = \frac{8 \cdot 7}{2} = 28$ distinct combinations.

## Problem 8 Graphs and trees (10 points)

a. (4 points) Let $G$ be a graph with vertices $V = \{1, 2, 3, 4, 5, 6\}$. Draw the graph of the following adjacency matrix, where an index $(i, j)$ in the matrix is 0 if there is no edge from vertex $i$ to vertex $j$ and 1 if there is. Is the graph connected? Is the graph complete?

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{bmatrix}$$

b. (6 points) Does the graph have

(a) (1 point) an Euler trail?

(b) (1 point) an Euler circuit?

(c) (2 points) a Hamiltonian path?

(d) (2 points) a Hamiltonian cycle?

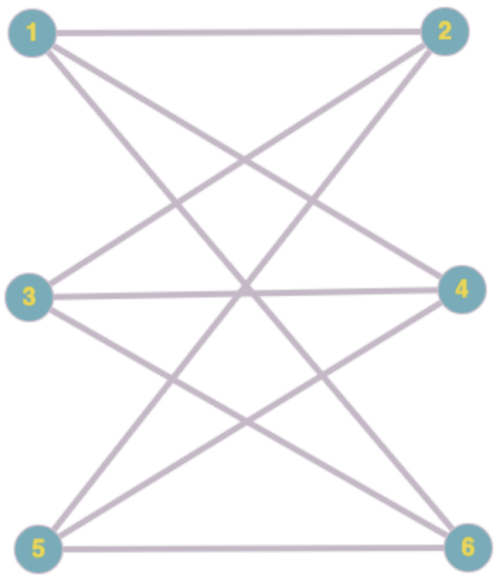



Figure 1: The graph given by the adjacency matrix in problem 8.

**Solution.**

a. (4 points) See drawing in the figure. This is a complete bipartite graph and is denoted $K_{3,3}$. The graph is connected since each vertex in $\{1, 3, 5\}$ is connected to each vertex in $\{2, 4, 6\}$, so there is a path between each pair of vertices in the graph. The graph is not complete since there is no edge between vertices in $\{1, 3, 5\}$ and no edge between vertices in $\{2, 4, 6\}$.

b. (6 points)

   (a) (1 points) More than two vertices has an odd degree, so there can not exist an Euler trail. In this case, every vertex has an odd degree.

   (b) (1 points) It is not the case that all vertices has an even degree, so there can not exist an Euler circuit. This is a necessary requirement.

   (c) (2 points) There are many Hamiltonian paths in this graph. We can choose any starting vertex, and go back and forth between vertices in $\{1, 3, 5\}$ and vertices in $\{2, 4, 6\}$, for example $1 \to 2 \to 3 \to 4 \to 5 \to 6$.

(d) (2 points) Similar to above, choose any starting vertex and go back and forth between the sets, for example $1 \to 2 \to 3 \to 4 \to 5 \to 6 \to 1$.

**Problem 9** **Number theory** (10 points)

a. (4 points) Let $(n, e) = (143, 11)$ be the public key in the RSA cryptosystem. Find the secret key $(p, q, d)$ and decrypt the ciphertext $c = 5$ to find the secret message $m$.

b. (6 points) Find all integer solutions $x$ to the following system of congruences:

$$\begin{aligned} 3x + 2 &\equiv 3 \pmod 7 \\ x - 4 &\equiv 1 \pmod 5 \\ 5x &\equiv 1 \pmod 9 \end{aligned}$$

**Solution.**

a. We have that $n = 143 = 11 \cdot 13 = p \cdot q$ and it follows that $\varphi(n) = (p-1) \cdot (q-1) = 120$. We then find the secret exponent $d$ by solving $e \cdot d \equiv 1 \pmod{\varphi(n)}$. We can compute this using Euclid's extended algorithm, but in this case we note that $11^2 = 121 \equiv 1 \pmod{120}$ and it follows that $d = e = 11$ (this would of course not be secure...). We compute 5 to the following powers of two modulo 143: $5^4 = 25^2 = 625 \equiv 53$ and $5^8 \equiv 53^2 = 2809 \equiv 92$. Then we decrypt the ciphertext by computing $m \equiv c^d = 5^{11} = 5^{1+2+8} = 5 \cdot 25 \cdot 92 \equiv 11500 \equiv 60 \pmod{143}$. In conclusion, we get secret key $(p, q, d) = (11, 13, 11)$ and message $m = 60$.

b. We first note that all moduli are relatively prime and we will then be able to find a unique solution modulo $5 \cdot 7 \cdot 9 = 315$. We then subtract to get $x$ isolated on the left side, and get

$$\begin{aligned} 3x &\equiv 1 \pmod 7 \\ x &\equiv 0 \pmod 5 \\ 5x &\equiv 1 \pmod 9 \end{aligned}$$

Multiply with $3^{-1} \equiv 5 \pmod 7$ in the first row and $5^{-1} \equiv 2 \pmod 9$ in the third row to get

$$\begin{aligned} x &\equiv 5 \pmod 7 \\ x &\equiv 0 \pmod 5 \\ x &\equiv 2 \pmod 9 \end{aligned}$$

The solution is $x \equiv \sum_{i=1}^{r} a_i M_i k_i \pmod M$ where $r$ is the number of congruences of the form $x \equiv a_i \pmod{m_i}$, $M = m_1 \cdot \dots \cdot m_r$ is the product of all individual moduli, $M_i = M/m_i$, and $k_i$ is the inverse of $M_i$ modulo $m_i$. We compute $k_1 \equiv 45^{-1} \equiv 3^{-1} \equiv 5 \pmod 7$ and $k_3 \equiv 35^{-1} \equiv (-1)^{-1} \equiv -1 \pmod 9$. Solution: $x \equiv 5 \cdot 45 \cdot 5 - 2 \cdot 35 = 1055 \equiv 110 \pmod{315}$.

## Problem 10 Finite state machines and automata (10 points)

a. (2 points) Draw the transition diagram of the finite state machine $F$ with input $I = \{a, b\}$, output $O = \{0, 1\}$ and states $S = \{s_0, s_1\}$ (initial state is $s_0$) and the following transition table. What is the output for the input string *abba*?

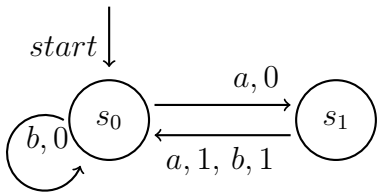
| F | $\eta$ | | $\mu$ | |
|---|---|---|---|---|
| | $a$ | $b$ | $a$ | $b$ |
| $s_0$ | $s_1$ | $s_0$ | 0 | 0 |
| $s_1$ | $s_0$ | $s_0$ | 1 | 1 |

b. (3 points) Draw the transition diagram of a finite state machine with input and output $O = I = \{0, 1\}$, which outputs 1 when it sees the first 0 in the input string and continues outputting 1 until it sees another 0; thereafter it outputs 0. In all other cases it outputs 0.

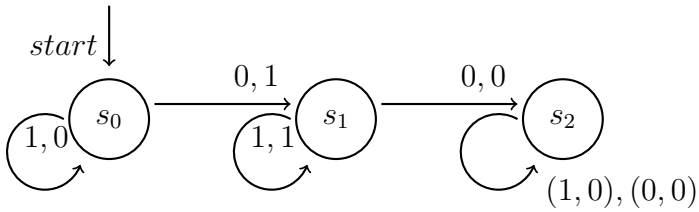
c. (5 points) Draw the transition diagram of a finite state automaton with input $I = \{a, b\}$ that accepts strings with an even number of $a$'s.

**Solution.**

a. The output for the input string *abba* is 0100. See diagram:




b. See diagram:




c. See diagram: