Problem 1

p	q	$\neg(p \rightarrow q)$
T	T	F
T	F	T
F	T	F
F	F	F

p	q	$\neg q$	$(p \vee q)$	$\neg q \wedge (p \vee q)$
T	T	F	T	F
T	F	T	T	T
F	T	F	T	F
F	F	T	F	F

They are the same

Problem 2

i) $f: \mathbb{N} \to \mathbb{N}, \quad n \to n+1$

Proof: injective

$f(n_1) = f(n_2)$

$n_1 + 1 = n_2 + 1$

$n_1 = n_2$

injective

Proof: Surjective

$f(n) = n + 1 = y$

$n = y - 1$

Let $y \in \mathbb{N}$, there is no $n \in \mathbb{N}$ such that

$n = y - 1 = 1 - 1 = 0$

$f(n)$ is injective, not surjective

Problem 2

ii) $g: \mathbb{R} \to \mathbb{R}_{\geq 0},\ x \to x^2 - 4x + 4$

Proof: injective

$g(0) = 0^2 - 4 \cdot 0 + 4 = 4$

$g(4) = 4^2 - 4 \cdot 4 + 4 = 4$

but $0 \neq 4$

not injective

Proof: Surjective

$g(x) = x^2 - 4x + 4 = (x-2)^2$

$(x-2)^2 = y$

$x - 2 = \sqrt{y}$

$x = \sqrt{y} + 2$

Let $y \in \mathbb{R}_{\geq 0}$, ~~for~~ $\forall y$ there $\exists x \in \mathbb{R}$. Surjective

$g(x)$ is not injective, surjective

Problem 2

iii) $h: \mathbb{Z} \to \mathbb{N}_0, \quad n \to n^4$

Proof: injective

$h(n_1) = h(n_2)$

$n_1^4 = n_2^4$

$\sqrt[4]{n_1^4} = \sqrt[4]{n_2^4}$

$\pm n_1 \neq \pm n_2$

not injective

Proof: surjective

$h(n) = n^4 = y$

$n = \sqrt[4]{y}$

Let $y \in \mathbb{N}_0$, there is no $n \in \mathbb{Z}$ such that $n = \sqrt[4]{y} = \sqrt[4]{2}$

not surjective

$h(n)$ is not injective, not surjective

Problem 2

iv) $P: \mathbb{Z} \to \mathbb{N}_0, \; k \to 2|k| - \frac{k-|k|}{2}$

Proof: injective

$$P(k_1) = P(k_2)$$

$$2|k_1| - \frac{k_1 - |k_1|}{2} = 2|k_2| - \frac{k_2 - |k_2|}{2}$$

$$\frac{4|k_1|}{2} - \frac{k_1 - |k_1|}{2} = \frac{4|k_2|}{2} - \frac{k_2 - |k_2|}{2}$$

$$\frac{5|k_1| - k_1}{2} = \frac{5|k_2| - k_2}{2}$$

$$5|k_1| - k_1 = 5|k_2| - k_2$$

Case 1: $k > 0$

$$5|k_1| - k_1 = 5|k_2| - k_2$$

$$4|k_1| = 4|k_2|$$

$$|k_1| = |k_2|$$

Case 2: $k \leq 0$

$$5|k_1| - k_1 = 5|k_2| - k_2$$

$$5|k_1| - (-k_1) = 5|k_2| - (-k_2)$$

$$6|k_1| = 6|k_2|$$

$$|k_1| = |k_2|$$

injective

Problem 2

iv) $P: \mathbb{Z} \to \mathbb{N}_0, k \to 2|k| - \frac{k-|k|}{2}$

Proof: surjective

case 1: $k > 0$

$$P(k) = 2|k| - \frac{k-|k|}{2} = y$$

$$2k - \frac{k-k}{2} = y$$

$$2k = y$$

$$k = \frac{y}{2}$$

case 2: $k \leq 0$

$$P(k) = 2|k| - \frac{k-|k|}{2} = y$$

$$2k - \frac{-k-k}{2} = y$$

$$2k - \frac{-2k}{2} = y$$

$$2k + k = y$$

$$k = \frac{y}{3}$$

let $y \in \mathbb{N}_0$, there is no $k \in \mathbb{Z}$ such that $k = \frac{y}{2} = \frac{1}{2}$, and $k = \frac{y}{3} = \frac{1}{3}$

not surjective

$P(k)$ is injective, not surjective

Problem 4

let $p = 47$, $q = 61$, $e = 17$

a) $\gcd((p-1)(q-1), e)$

$\gcd((47-1)(61-1), 17)$

$\gcd(2760, 17)$

$2760 = 17 \cdot 162 + 6$

$\gcd(17, 6)$

$17 = 6 \cdot 2 + 5$

$\gcd(6, 5)$

$6 = 5 \cdot 1 + 1$

$\gcd(5, 1) = \underline{\underline{1}}$

Problem 4

b) Let $p = 47$, $q = 61$, $e = 17$

Public key: $(p \cdot q, e) \rightarrow (2867, 17)$

Padding scheme: Position in alphabet: A → 00, B → 01

GOOD → 0614, 1403

Encryption: $M^e \bmod n$

(We use fast modular exponentiation)

$0614^{17} \bmod 2867 = 0472$

$1403^{17} \bmod 2867 = 0793$

Problem 4

c) let $p = 47$, $q = 61$, $e = 17$

$d \cdot e = \gcd((p-1)(q-1)) \bmod (p-1)(q-1)$

$17d = 1 \bmod 2760$

* this means that $17d + 2760k = 1$ for integers d, k

* Express 1 as a linear composition of 17 and 2760

$1 = 6 - 5 \cdot 1$

$1 = 6 - (17 - 6 \cdot 2)$

$1 = 3 \cdot 6 - 17$

$1 = 3 \cdot (2760 - 17 \cdot 162) - 17$

$1 = 3 \cdot 2760 - 487 \cdot 17$

this means that $k = 3$, $d = -487$

So $d \equiv -487 \equiv 2273 \bmod 2760$

Problem 4

d) Let $p = 47$, $q = 61$, $e = 17$, $d = 2273$

Massage: 2741 2504 $\quad n = p \cdot q = 2867$

decryption: $M^d \bmod n$

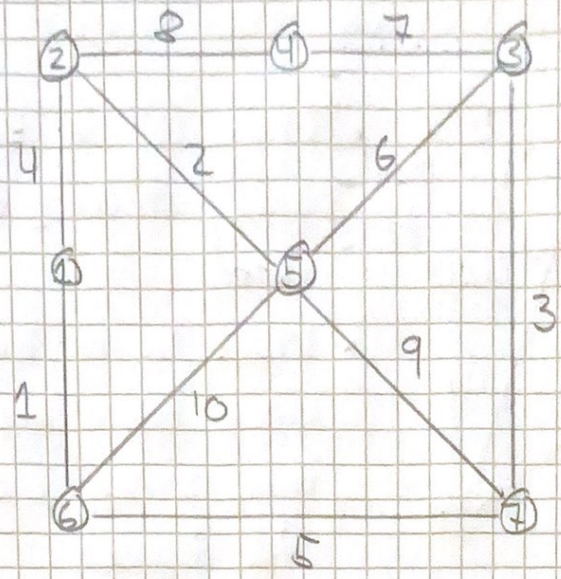
$2741^{2273} \bmod 2867 = 1120$

$2504^{2273} \bmod 2867 = 0210$

decrypted:

11	20	02	10
↓	↓	↓	↓
L	U	C	K

Problem 6



a) Shortest path between 2 and 7

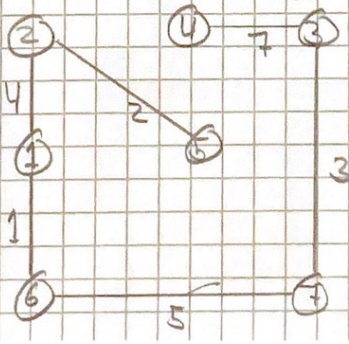
	V_2	V_4	V_1	V_5	V_6	V_3	V_7
$\emptyset$	0	∞	∞	∞	∞	∞	∞
V_2	0	8	4	2	–	–	–
$V_2V_4V_1V_5$	0	8	4	2	5	8	11
$V_2V_4V_1V_5V_6V_3$	0	8	4	2	5	8	10

Shortest path: $V_2 \rightarrow V_1 \rightarrow V_6 \rightarrow V_7 = 10$

b) minimum spanningtree: $V_2 \rightarrow V_5 \rightarrow V_1 \rightarrow V_6 \rightarrow V_7 \rightarrow V_3 \rightarrow V_4$

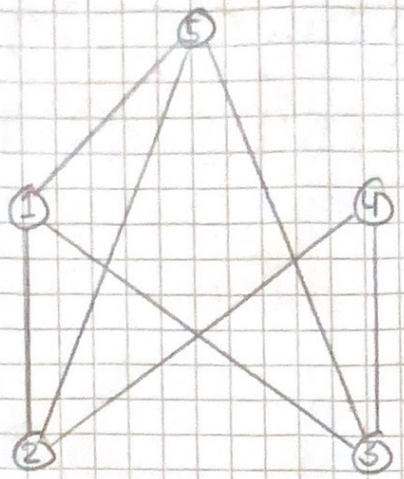
$0 + 2 + 4 + 1 + 5 + 3 + 7$

$= 22$



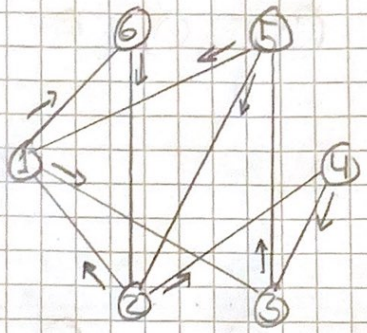
Problem 7

a) $G = (V, E)$



* There is no Euler circuit since not every degree is even
* There is no Euler path since there are more than 2 vertices with odd degree.

b) $G' = (V', E')$



* There are no Euler circuit since not every degree is even
* Euler Path:
  5, 1, 6, 2, 1, 3, 5, 2, 4, 3

Problem 8

- Let event A be that a person selected at random is allergic to coffee
- Let event B be that the test result is positive

$$P(A) = \frac{1}{2000} \qquad P(\bar{A}) = \frac{1999}{2000}$$

$$P(B|A) = \frac{92}{100} \qquad P(B|\bar{A}) = \frac{7}{100}$$

$$P(B) = P(B|A) \cdot P(A) + P(B|\bar{A}) \cdot P(\bar{A}) \quad \text{(Law of total probability)}$$

$$= \frac{92}{100} \cdot \frac{1}{2000} + \frac{7}{100} \cdot \frac{1999}{2000}$$

$$= \frac{2817}{40\,000}$$

$$P(A|B) = \frac{P(B|A) \cdot P(A)}{P(B)} \quad \text{(Bayes theorem)}$$

$$= \frac{\frac{92}{100} \cdot \frac{1}{2000}}{\frac{2817}{40\,000}}$$

$$= \frac{92}{14085}$$

$$\approx 0{,}65\,\%$$

Problem 9

Let $n \in \mathbb{N}$ and X_n be the random variable that equals the number of tails minus the number of heads, when n fair coins tossed

T_n = number of tails

H_n = number of heads

$E(T_n) = E(H_n)$ → since it is a fair coin

$E(X_n) = E(T_n) - E(H_n)$

$\underline{\underline{E(X_n) = 0}}$