Problem 1. Give, if it exists, a solution $(u, v) \in \mathbb{Z}^2$ to the following equations. Explain your work to get full credit.

I. $4u + 37v = 1$.
II. $3u + 9v = 5$.

I) Such a solution does exist because $4$ and $37$ are coprime.

$37 = 4 \times 9 + 1$

$1 = 37 \times 1 - 4 \times 9$

$v = 1$ and $u = -9$ work.

II) If such a $(u, v)$ exists, then

$5 = 2u + 9v$

So 3 divides 5. Impossible.

So there is no solution.
Problem 2. You know the following theorems:
- let \((u_n)_{n \in \mathbb{N}}\) and \((v_n)_{n \in \mathbb{N}}\) be two sequences of real numbers. We suppose that they both have a limit which we call \(u\) and \(v\) respectively. If \(u_n \leq v_n\) for all \(n \in \mathbb{N}\), then \(u \leq v\).
- the squeeze theorem.
- a non decreasing sequence that is bounded above has a limit.
- a non increasing sequence that is bounded below has a limit.

0. Let \((u_n)_{n \in \mathbb{N}}\) be a sequence of real numbers. Give a precise definition of what it means for the sequence to have limit \(\ell\) (using \(\varepsilon\)).

\[ \forall \varepsilon > 0 \quad \exists \, m_0 \quad \forall \, m \geq m_0 \quad |u_m - \ell| < \varepsilon. \]

***

For \(n \in \mathbb{N},\ n \geq 1\), set\[ S_n := \sum_{k=1}^{n} \frac{(-1)^k}{\pi^k}. \]

We want to prove that the sequence \((S_n)_{n \geq 1}\) has a limit.

I. Give the expression of \(S_1, S_2, S_3, S_4\). Compare \(S_1\) and \(S_3\). Compare \(S_2\) and \(S_4\) (comparing two real numbers \(x\) and \(y\) means saying if \(x \leq y\) or \(y \leq x\).)

\[ S_1 = \frac{-1}{\pi} \]
\[ S_2 = \frac{-1}{\pi} + \frac{1}{\pi^2} \]
\[ S_3 = -\frac{1}{\pi} + \frac{1}{\pi^2} - \frac{1}{\pi^3} \]
\[ S_4 = -\frac{1}{\pi} + \frac{1}{\pi^2} - \frac{1}{\pi^3} + \frac{1}{\pi^4} \]
\[ S_3 - S_1 = \frac{1}{\pi^2} \left( \frac{1}{\pi} \right) \]
\[ \geq 0 \]
\[ \implies S_3 \geq S_1 \]
\[ S_4 - S_2 = \frac{1}{\pi^3} \left( -\frac{1}{\pi} + \frac{1}{\pi^4} \right) \]
\[ \leq 0 \]
\[ \implies S_4 \leq S_2. \]
II. For $p \in \mathbb{N}$, $p \geq 1$ set $U_p := S_{2p}$. Prove that the sequence $(U_p)_{p\geq 1}$ is non increasing that is to say $U_{p+1} \leq U_p$ for all $p \geq 1$.

Let $p \in \mathbb{N}$, $p \geq 1$

\[ U_{p+1} - U_p = S_{2p+2} - S_{2p} = \frac{1}{q^{2p+2}} - \frac{1}{q^{2p+1}} = \frac{1}{q^{2p+1}} \left( \frac{1}{q^2} - 1 \right) \leq 0 \]

So $U_{p+1} \leq U_p$.

III. For $p \in \mathbb{N}$, $p \geq 1$ set $V_p := S_{2p+1}$. Prove that the sequence $(V_p)_{p\geq 1}$ is non decreasing that is to say $V_p \leq V_{p+1}$ for all $p \geq 1$.

Let $p \in \mathbb{N}$, $p \geq 1$

\[ V_{p+1} - V_p = S_{2p+3} - S_{2p+1} = -\frac{1}{q^{2p+3}} + \frac{1}{q^{2p+2}} = \frac{1}{q^{2p+2}} \left( 1 - \frac{1}{q^2} \right) \geq 0 \]

So $V_{p+1} \geq V_p$.

IV. For $p \geq 1$, compute $U_p - V_p$ and compare $U_p$ and $V_p$.

Let $p \geq 1$

\[ U_p - V_p = S_{2p} - S_{2p+1} = \frac{1}{q^{2p+1}} \geq 0 \]

So $U_p \geq V_p$. 
V. Deduce that \((U_p)_{p \geq 1}\) is bounded below by \(V_1\) and likewise, that \((V_p)_{p \geq 1}\) is bounded above by \(U_1\).

By IV, we have \(U_p \geq V_p\) \(\forall p \geq 1\).

By III we have \(V_1 \leq V_2 \leq \ldots \leq V_p\) \(\forall p \geq 1\).

So \(U_p \geq V_1\) \(\forall p \geq 1\).

Likewise, \(V_p \leq U_p\) and \(U_p \leq U_{p-1} \leq \ldots \leq U_1\).

So \(V_p \leq U_p\).

VI. Using the two previous questions, prove that
- \((U_p)_{p \geq 1}\) has a limit \(u \in \mathbb{R}\)
- \((V_p)_{p \geq 1}\) has a limit \(v \in \mathbb{R}\),
- and that \(u = v\).

\((U_p)_{p \geq 1}\) is bounded below and non-increasing \(\implies\) it has a limit \(u\).

\((V_p)_{p \geq 1}\) is bounded above and non-decreasing \(\implies\) it has a limit \(v\).

Moreover \(\frac{U_p - V_p}{p^{2p+1}} = \frac{1}{p^{2p+1}}\) has limit \(u - v\) and \(\frac{1}{p^{2p+1}}\) has limit 0.

\[ \implies u = v \]

VII. Bonus 1 Prove carefully, using the previous question, that \((S_n)_{n \geq 1}\) has a limit equal to \(u = v\).
(You can use the definition of a limit with the \(\varepsilon\)'s...)

Let \(\varepsilon > 0\). From \(U_p \geq p\) \(\forall p \geq p_0\), \(|U_p - u| = |S_{2p} - u| < \varepsilon\)
we know \(V_p \geq q\) \(\forall p \geq q_0\), \(|V_p - u| = |S_{2q} - u| < \varepsilon\)

So let \(n_0 = \max(p_0, q_0 + 1)\) and let \(n \geq n_0\).
If \( n \) is even, there is \( p \in \mathbb{N}, p \geq 1 \) such that \( n = 2p \) and \( p \geq p_0 \) because \( n \geq 2p_0 \).

So \( |S_n - u| = |S_{2p} - u| < \epsilon \).

If \( n \) is odd, there is \( p \in \mathbb{N}, p \geq 1 \) such that \( n = 2p + 1 \) and \( p \geq p_0 \) because \( n \geq 2p + 1 \).

So \( |S_n - u| = |S_{2p+1} - u| < \epsilon \).

We have proved that given \( \epsilon > 0 \) there is \( p \in \mathbb{N} \) such that \( n \geq n_0 \) implies \( |S_n - u| < \epsilon \).

\( (S_n) \) has limit \( u \).
VIII. **Bonus 2** Give the general theorem about sequences of the form

\[ S_n = \sum_{k=1}^{n} a_k \]

(where \((a_k)_{k \geq 1}\) is a sequence of real numbers with certain properties you need to specify) that we can prove by the method above.

Let \((a_k)_{k \geq 1}\) be a sequence of real numbers of the form

\[ a_k = (-1)^k |a_k| \]

Suppose that

\[ |a_{k+1}| \leq |a_k| \quad \forall \ k \geq 1 \]

\[ \lim_{k \to \infty} a_k = 0 \]

Then \((S_n)_{n \in \mathbb{N}}\) has a limit.
**Problem 3 (True/False).** Justify your answer to get full credit. When you think it is true, give your argument. When you think it is false, give a counter example, or an argument to prove that the negation of the statement is true.

I. \((\mathbb{Z}/7\mathbb{Z}, \times)\) is a group.

*FALSE*

\[ \text{No because } [0] \in \mathbb{Z}/7\mathbb{Z} \text{ does not have an inverse for } \times \]

II. There is an element \([x]_{24} \in \mathbb{Z}/24\mathbb{Z}\) such that \([x]_{24} \times [8]_{24} = [1]_{24}\).

*FALSE*

\[ \text{If that was the case, there would be } x \in \mathbb{Z}/24 \text{ such that } 8x \equiv 1 \pmod{24} \]
\[ \Rightarrow \text{ there would be } y \in \mathbb{Z}/24 \text{ such that } 8x - 24y = 1 \]
\[ \text{Impossible because } 2 \text{ divides } 8x - 24y \]

III. The polynomial \(X - 2\) divides \(X^4 + X^2 - X + 8\).

*FALSE* because \(2^4 + 2^2 - 2 + 8 \neq 0\).

\[ X^2 - 3X + 2 \]

IV. The polynomial \((X - 2)(X - 1)\) divides \(X^4 - 2X^3 - X + 2\).

*TRUE* because 1 and 2 are roots of this polynomial.

\[ \frac{X^2 + X + 1}{X^4 - 2X^3 - X + 2} \]

V. The set \([0, 1]\) as a maximum element and a minimum element.

*It has no maximum element because it does not contain its least upper bound 1.*
VI. Let $(u_n)_{n \in \mathbb{N}}$ be the sequence defined by

$$u_n = 1 + \frac{1}{n}.$$ 

i. The set $\{u_n, \, n \in \mathbb{N}\}$ has a least upper bound.

Yes, because it is not empty and $u_n \leq 2, \, \forall \, m \in \mathbb{N}, \, n \geq 1$. So it is also bounded above.

ii. The sequence $(u_n)_{n \in \mathbb{N}}$ has a limit equal to the least upper bound of the set $\{u_n, \, n \in \mathbb{N}\}$.  

\underline{FALSE}: It has limit 1 which is not an upper bound for the set.

VII. There is a non empty subset of $\mathbb{R}$ that does not contain any element of $\mathbb{Q}$.

\underline{TRUE}: $\exists x \in \sqrt{2}$?

VIII. The least upper bound of $\mathbb{Q} \cap \{x \in \mathbb{R}, x^2 \geq 2\}$ is $\sqrt{2}$.

\underline{FALSE}: this set is not bounded above.

IX. A sequence $(u_n)_{n \in \mathbb{N}}$ that has a limit $u \in \mathbb{R}$ is necessarily bounded below.

Likewise, $(u_n)_{n}$ is bounded below by $\text{Min}(u_0, \ldots, u_{(n-0-1)}, u-1)$.

\underline{TRUE}: Let $\varepsilon = 1$

\exists m_0 \mid \forall n \geq m_0 \quad u_n < u + \varepsilon

So $(u_n)_{n \in \mathbb{N}}$ is bounded above by $\text{MAX}(u_0, \ldots, u_{(n-0-1)}, u+1)$.
Problem 4. Recall that given a group \((G, \circ)\) with unit \(e\), we say that \((H, \circ)\) is a subgroup of \((G, \circ)\) if \(H\) is a subset of \(G\) satisfying:

- The subset \(H\) contains \(e\).
- For any \(h_1, h_2 \in H\), the element \(h_1 \circ h_2\) also belongs to \(H\).
- For any \(h \in H\), the symmetric \(h'\) of \(h\) in \((G, \circ)\) belongs to the subset \(H\).

Recall also that given a prime number \(p\), the set \((\mathbb{Z}/p\mathbb{Z})^* = \mathbb{Z}/p\mathbb{Z} - \{[0]_p\}\) is a group for the multiplication \(\times\).

Justify your answers:

I. What is the subgroup of \(((\mathbb{Z}/23\mathbb{Z})^*, \times)\) with smallest possible cardinality that contains the class of 1?

It is \([1]_{23}\).

II. What is the subgroup of \(((\mathbb{Z}/11\mathbb{Z})^*, \times)\) with smallest possible cardinality that contains the class of \(2\)?

If a subgroup \(H\) of \((\mathbb{Z}/11\mathbb{Z})^*\) contains \([2]_{11}\), then it contains:

\[
\]

\[
[2]^6 = [2][-1] = [-2] = [9], \quad [2]^7 = [2][9] = [18] = [7],
\]

\[
\]

III. What are the subgroups of \((\mathbb{R}^*, \times)\) with cardinality 2?

Such a subgroup contains 1 and another element \(x\).

We have \(x^2 \in \{1, x\}\) so

\(x = 1\) (impossible) or \(x = -1\).

So it is \((\mathbb{Z}/11\mathbb{Z})^*\) it itself.
So the only possibility is
\[(1, -17, x)\]
and one checks indeed that this is a subgroup of \((\mathbb{R}^*, \times)\).
IV. What are the subgroups of \((\mathbb{R}^*, \times)\) with cardinality 3?

Such a subgroup \(H\) has the form \(H = \{1, x, y\}\) with \(x \neq 1, y \neq 1, x \neq y \).

We have \(xy = \frac{1}{x}y \neq 1\) and the only possibility is \(xy = 1\) so \(y = \frac{1}{x}\).

We also have \(x^2 = \frac{1}{x}x = 1\) which gives a contradiction.

Because: 1) \(x^2 = 1 \Rightarrow x = \frac{1}{x} = y\) 2) \(x^2 = x\) \(\Rightarrow x = x\) 3) \(x^2 = \frac{1}{x}\)

\(\Rightarrow x = 1\)

V. What are the subgroups of \((\mathbb{R}, +)\) with cardinality 2?

Such a subgroup \(H\) has the form \(H = \{0, x\}\) with \(x \neq 0\).

Put \(dx \in H\) so \(dx = 0\) or \(dx = x\)

Which implies \(x = 0\).

\(\text{There is no such group}\)

VI. Bonus Let \(a, n \in \mathbb{N}, a, n \geq 1\). Prove that

the smallest subgroup of \((\mathbb{Z}/n\mathbb{Z}, +)\) containing \([a]_n\) is \((\mathbb{Z}/n\mathbb{Z}, +)\) itself

if and only if

\(a\) and \(n\) are coprime.

1) If \(a\) and \(n\) are coprime, \(\exists u, v \in \mathbb{Z}\)

\(au + vn = 1\)

So \(au = 1 \mod n\)

So \(u \cdot [a]_n = [1]_n\)

\(\text{if } u \geq 0 \text{ this is } [a]_n + \ldots + [a]_n\)

\(\text{m times}\)

\(\text{if } u \leq 0 \text{ this is } -([a]_n + \ldots + [a]_n)\)

\(\text{m times}\)
In both cases

\[ a \mathbb{Z}_m \text{ is contained in any subgroup of } (\mathbb{Z}/m\mathbb{Z}, +) \text{ that contains } [a \mathbb{Z}_m]. \]

So \([1]_m\) is contained in such a subgroup.

But then also

\[ [1]_m + [1]_m \]

\[ [1]_m + [1]_m + [1]_m \]

\[ \cdots \]

\[ \underbrace{[1]_m + [1]_m + \cdots + [1]_m}_{n-1 \text{ times}} \]

so all the elements of \(\mathbb{Z}/m\mathbb{Z}\) are contained in a subgroup containing \([a \mathbb{Z}_m]\).
2) Suppose that \( a \) and \( n \) are not coprime:

\[ \text{If } m \in \mathbb{N} \text{ and } m \geq 1, \text{ then } m \mid a \]

\[ m \mid n \]

Let \( H = \{ [x]_m \mid \text{for all } x \in \mathbb{Z} \text{ such that } m \mid x \} \)

- \( H \) contains \([0]_m\)
- Let \([x]_m \in H\) then \(m \mid x\)
  - \([y]_m \in H\) and \(m \mid y\)
  - So \(m \mid x + y\)
  - Therefore \([x]_m + [y]_m = [x+y]_m \leq m \in H\)

- Let \([x]_m \in H\) then \(m \mid x\) so \(m \mid -x\)
  - Therefore \([-x]_m = -[x]_m \in H\)

So \((H, +)\) is a subgroup of \((\mathbb{Z}/n\mathbb{Z}, +)\)
It contains \([a]_n\) because \(m/a\).

It is not equal to \((\mathbb{Z}/n\mathbb{Z}, +)\) because for example, it does not contain \([1]_n\).