Quiz 10

(1) For the pairs of integers \(a, b\) given below, find the integers \(q\) and \(r\) such that \(a = qb + r\) and \(0 \leq r < b\).

- \(a = 24,\ b = 5\).
  
  Since \(a > 0\), and we have \(\frac{24}{5} = 4\) remainder, thus
  
  \[q = 4\text{ and } r = 24 - 4 \cdot 5 = 4.\]

- \(a = -100,\ b = 3\).
  
  Since \(a < 0\), and we have \(\frac{-100}{3} = -33\) remainder, thus
  
  \[q = -33 - 1 = -34\text{ and } r = -100 - (-24) \cdot 3 = 2.\]

(2) Pick one pair \((a, b)\) from (1) and prove that there is only one pair \((q, r)\) that satisfies conditions \(a = qb + r\) and \(0 \leq r < b\).

Proof for \(a = 24\) and \(b = 5\). For \(q = 4\) and \(r = 4\), we have \(24 = 4 \cdot 5 + 4\) and \(0 \leq r < 5\).

Assume there is a pair \((q, r)\) of integers such that \(24 = q \cdot 5 + r\) and \(0 \leq r < 5\) (thus \(r \in \{0, 1, 2, 3, 4\}\)). (We have to show \(q = 4\) and \(r = 4\).)

\[
\begin{align*}
4 \cdot 5 + 4 &= q \cdot 5 + r \\
\quad &\implies 4 \cdot 5 - q \cdot 5 = r - 4 \\
\quad &\implies (4 - q) \cdot 5 = r - 4 \in \{-4, -3, -2, -1, 0\}, \\
\quad &\text{because by the assumption } r \in \{0, 1, 2, 3, 4\} \\
\quad &\implies (4 - q) \cdot 5 = r - 4 = 0, \\
\quad &\text{because 0 is the only element in } \{-4, -3, -2, -1, 0\}, \\
\quad &\text{that is a multiple of 5,} \\
\quad &\implies r = 4, \text{ and } (4 - q) \cdot 5 = 0 \implies 4 - q = 0, \\
\quad &\implies r = 4 \text{ and } q = 4.
\end{align*}
\]

Alternative proof for \(a = 24\) and \(b = 5\). Assume there is a pair \((q, r)\) of integers such that \(24 = q \cdot 5 + r\) and \(0 \leq r < 5\) (We have to show \(q = 4\) and \(r = 4\)).

Since \(r \in \{0, 1, 2, 3, 4\}\) we have:

- If \(r = 0\), then \(24 = q \cdot 5\). Since \(24\) is not divisible by \(5\), this is not possible case.
• If \( r = 1 \), then \( 24 = q \cdot 5 + 1 \) implies \( 23 = q \cdot 5 \). Since 23 is not divisible by 5, this is not possible case.
• If \( r = 2 \), then \( 24 = q \cdot 5 + 2 \) implies \( 22 = q \cdot 5 \). Since 22 is not divisible by 5, this is not possible case.
• If \( r = 3 \), then \( 24 = q \cdot 5 + 3 \) implies \( 21 = q \cdot 5 \). Since 21 is not divisible by 5, this is not possible case.
• If \( r = 4 \), then \( 24 = q \cdot 5 + 4 \) implies \( 20 = q \cdot 5 \). In this case we have \( r = 4 \) and \( q = 4 \).

Proof for \( a = -100 \) and \( b = 3 \). For \( q = -34 \) and \( r = 2 \), we have \(-100 = q3 + r\) and \(0 \leq r < 3\).
Assume there is a pair \((q, r)\) of integers such that \(-100 = q \cdot 3 + r\) and \(0 \leq r < 3\) (thus \( r \in \{0, 1, 2\}\)). (We have to show \( q = -34 \) and \( r = 2 \).)

\[
\begin{align*}
\frac{-34 \cdot 3 + 2}{-100} = \frac{q \cdot 3 + r}{-100} & \implies (-34) \cdot 3 - q \cdot 3 = r - 2 \\
\implies (-34 - q) \cdot 3 = r - 2 \in \{-2, -1, 0\}, & \text{because by the assumption } r \in \{0, 1, 2\} \\
\implies (-34 - q) \cdot 3 = r - 2 = 0, & \text{because 0 is the only element in } \{-2, -1, 0\}, \\
\implies r = 2, & \text{that is a multiple of 3}, \\
\implies r = 2 \text{ and } (-34 - q) \cdot 3 = 0 & \implies -34 - q = 0, \\
\implies r = 2 \text{ and } q = -34. &
\end{align*}
\]

Alternative proof for \( a = -100 \) and \( b = 3 \). Assume there is a pair \((q, r)\) of integers such that \(-100 = q \cdot 3 + r\) and \(0 \leq r < 3\) (We have to show \( q = -34 \) and \( r = 2 \).)
Since \( r \in \{0, 1, 2\} \) we have:
• If \( r = 0 \), then \(-100 = q \cdot 3\). Since \(-100\) is not divisible by 3, this is not possible case.
• If \( r = 1 \), then \(-100 = q \cdot 3 + 1\) implies \(-101 = q \cdot 3\). Since \(-101\) is not divisible by 3, this is not possible case.
• If \( r = 2 \), then \(-100 = q \cdot 3 + 2\) implies \( q = -34 \).
(1) Let $a, b$ be positive integers.

(a) For $a = 24$ and $b = 5$ we have

\[
\begin{align*}
24 &= 4 \cdot 5 + 4, & 5 &= 0 \cdot 24 + 5, & 5 &= 1 \cdot 5 + 0, \\
0 &\leq 4 < 5, & 0 &\leq 5 < 24, & 0 &\leq 0 < 5
\end{align*}
\]

By the definition of mod and div we have
\[
\begin{align*}
& \bullet 24 = 4 \div 5 \cdot 5 + 4, \\
& \bullet 5 = 0 \div 24 + 5, \\
& \bullet 5 = 1 \div 5 + 0.
\end{align*}
\]

Therefore
\[
\begin{align*}
& \bullet a \mod b = 4, \quad b \mod a = 5, \\
& \bullet a \div b = 4, \quad b \div a = 0, \\
& \bullet a \mod a = 0, \quad a \div a = 1.
\end{align*}
\]

(b) Prove the following statements:

- If $a < b$, then $a \div b \neq b \div a$.

Since $a, b$ are positive integers and $a < b$, we have

\[
0 \leq \frac{a}{b} < 1, \quad \text{and} \quad \frac{b}{a} > 1.
\]

($b$ can be written as $b = a + (b-a)$, thus \[ \frac{b}{a} = \frac{a+\left(b-a\right)}{a} = \frac{a}{a} + \frac{b-a}{a} = \]

\[ 1 + x, \text{where} \ x = \frac{b-a}{a} \text{is a positive real number} \].

Therefore \[ \frac{a}{b} = 0.\text{[remainder]}, \quad \text{and} \quad \frac{b}{a} = n.\text{[remainder]}, \]

where $n \geq 1$ imply

\[
\begin{align*}
a &= 0 \div b + a, & b &= n \div a + r < a
\end{align*}
\]

Therefore $a \div b \neq b \div a$.

- If $a > b$, then $a \div b \neq b \div a$.

Since $a, b$ are positive integers and $a > b$, we have
\[
\frac{a}{b} > 1, \quad \text{and} \quad 0 \leq \frac{b}{a} < 1
\]

(a can be written as \( a = b + (a - b) \), thus \( \frac{a}{b} = \frac{b + (a - b)}{b} = \frac{b}{b} + \frac{a - b}{b} = 1 + x \), where \( x = \frac{a - b}{b} \) is a positive real number).

\[
\frac{a}{b} = n \quad \text{remainder} \quad \text{where} \quad n \geq 1 \quad \text{and} \quad \frac{b}{a} = 0 \quad \text{remainder}
\]

imply

\[
a = n \cdot b + r, \quad \text{and} \quad b = 0 \cdot a + b
\]

Therefore \( a \div b \neq b \div a \).

• Using the last two statements show that

\( a \neq b \) if and only if \( a \div b \neq b \div a \)

We have to show two statements:

I. If \( a \neq b \), then \( a \div b \neq b \div a \).

II. If \( a \div b \neq b \div a \), then \( a \neq b \).

Proof of I. Assume \( a \neq b \), then either \( a < b \) or \( a > b \).

If \( a < b \), then the first of the last two statements implies \( a \div b \neq b \div a \).

If \( a > b \), then the second of the last two statements implies \( a \div b \neq b \div a \).

Therefore any time \( a \neq b \), we have \( a \div b \neq b \div a \).

Proof of II. (Recall that the proof of the statement of the form ”If \( X \), then \( Y \)” is logically equivalent to the proof of the statement ”If \( \neg Y \), then \( \neg X \”).

In order to prove the statement

”If \( a \div b \neq b \div a \), then \( a \neq b \)”,

it is enough to prove the statement

”If \( a = b \), then \( a \div b = b \div a \)”

Assume \( a = b \), then obviously \( a \div b = b \div a \), because \( a \div a = a \div a \).

(2) (Using Euclidean algorithm) find \( \gcd(97, 17) \).
\[ \begin{align*}
97 &= 5 \cdot 17 + 12 \quad \implies \quad \gcd(97, 17) = \gcd(17, 12) \\
17 &= 1 \cdot 12 + 5 \quad \implies \quad \gcd(17, 12) = \gcd(12, 5) \\
12 &= 2 \cdot 5 + 2 \quad \implies \quad \gcd(12, 5) = \gcd(5, 2) \\
5 &= 2 \cdot 2 + 1 \quad \implies \quad \gcd(5, 2) = \gcd(2, 1) = 1
\end{align*} \]

Therefore

\[ \gcd(97, 17) = 1 \]