I non-conditional statements

Biconditional statements on that line.

Proposition \( P \iff Q \)

proof

\( P \implies Q \)

\( Q \implies P \)

Proposition: Suppose \( a \) and \( b \) are integers. Thus \( a \equiv b \pmod{6} \) if and only if \( a \equiv b \pmod{2} \) and \( a \equiv b \pmod{3} \).

Proof: Assume \( a \equiv b \pmod{6} \) that is \( 6 \mid a-b \), so we can write \( a-b=6n \) for some \( n \in \mathbb{Z} \)

but \( a-b=6n \) is equivalent to \( a-b \equiv 0 \pmod{2} \) and \( a-b \equiv 0 \pmod{3} \), so we have \( a \equiv b \pmod{2} \) and \( a \equiv b \pmod{3} \).

\( a-b=2x \quad a-b=3z \) for some \( x, z \in \mathbb{Z} \)

\( 2x=3z \)

3z is even, \( x \) is even

\( x=2m \) for some \( m \in \mathbb{Z} \)

\( a-b=3(2m)=6m \)

\( 6\mid a-b \)

\( a \equiv b \pmod{6} \)
Dividing non-conditional statements

II Equivalent Statements (Examples are on page 123)

The following are equivalent (TFAE)

Proof \( a \div b = c \quad a \div b = c \)
\[ \begin{align*}
& a \leq b \leq c \\
& b \leq a \leq c \\
& c \leq b \leq a \\
& d \leq e \leq d \\
& f \leq e \leq f
\end{align*} \]

III Existence & Uniqueness proofs

\[ A = ax + by, \quad x, y \in \mathbb{Z} \]

(on page 126) We need to show \( \text{dla and dlb} \), when we divide \( a \) by \( d \), the division algorithm give \( a = qd + r \) with \( 0 \leq r < d \).

\[ r = a - q \cdot d \]
\[ = a - q(ab + bl) \]
\[ = a(1 - q) + b(1 - qd) = r + \alpha \]

\( 0 \leq r < d \) and \( d \) is the smallest positive number in \( A \).

\( r = 0 \quad a = qd \quad d \mid a \)

With a similar argument we can see \( d \mid b + d \mid b \)

(Because \( b = qd + r \))

\( d \) is a common divisor of \( a \) and \( b \).

We can write \( a = \gcd(a, b) 
\quad b = \gcd(a, b) \cdot n 
\) for \( n, m \in \mathbb{Z} \)

\[ d = ak + b \mid = \gcd(a, b) \cdot mk + \gcd(a, b) \cdot n. \]

\[ \therefore \quad d = \gcd(a, b) \cdot n \]
\[ d = \gcd(a, b) (mk + nl) \]

We have \( d \geq \gcd(a, b) \)
\( d \) is a common divisor.

Therefore, \( d = \gcd(a, b) \)
\[ \gcd(a, b) = ak + bd \]