1. Let $S$ be the statement

“If $a_1, b_1, a_2, b_2$ are arbitrary real numbers, then $a_1 b_1 + a_2 b_2 \leq \sqrt{a_1^2 + a_2^2}\sqrt{b_1^2 + b_2^2}$.”

i. Write $S$ is formal language.

**ANSWER.**

$$(\forall a_1, b_1, a_2, b_2 \in \mathbb{R}) a_1 b_1 + a_2 b_2 \leq \sqrt{a_1^2 + a_2^2}\sqrt{b_1^2 + b_2^2}$$

ii. Prove $S$.

**PROOF:**

Let $a_1, a_2, b_1, b_2$ be arbitrary real numbers.

We will prove that $a_1 b_1 + a_2 b_2 \leq \sqrt{a_1^2 + a_2^2}\sqrt{b_1^2 + b_2^2}$.

We will do a proof by contradiction.

Assume $\sim a_1 b_1 + a_2 b_2 \leq \sqrt{a_1^2 + a_2^2}\sqrt{b_1^2 + b_2^2}$.

Then $a_1 b_1 + a_2 b_2 > \sqrt{a_1^2 + a_2^2}\sqrt{b_1^2 + b_2^2}$.

Therefore $(a_1 b_1 + a_2 b_2)^2 > (a_1^2 + a_2^2)(b_1^2 + b_2^2)$.

On the other hand,

$$(a_1 b_1 + a_2 b_2)^2 = a_1^2 b_1^2 + a_2^2 b_2^2 + 2a_1 b_1 a_2 b_2,$$

and

$$(a_1^2 + a_2^2)(b_1^2 + b_2^2) = a_1^2 b_1^2 + a_2^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2.$$

Therefore

$$a_1^2 b_1^2 + a_2^2 b_2^2 + 2a_1 b_1 a_2 b_2 > a_1^2 b_1^2 + a_2^2 b_2^2 + a_1^2 b_2^2 + a_2^2 b_1^2.$$

Hence

$$2a_1 b_1 a_2 b_2 > a_2^2 b_2^2 + a_2^2 b_1^2,$$

so that

$$0 > a_1^2 b_2^2 + a_2^2 b_1^2 - 2a_1 b_1 a_2 b_2,$$

But

$$a_1^2 b_2^2 + a_2^2 b_1^2 - 2a_1 b_1 a_2 b_2 = (a_1 b_2 - a_2 b_1)^2,$$

and then

$$0 > (a_1 b_2 - a_2 b_1)^2.$$

However, $x^2 \geq 0$ for all $x \in \mathbb{R},$

so, in particular,

$$(a_1 b_2 - a_2 b_1)^2 \geq 0,$$
from which it follows that
\[ \sim 0 > (a_1 b_2 - a_2 b_1)^2. \]

Hence
\[ 0 > (a_1 b_2 - a_2 b_1)^2 \wedge \sim 0 > (a_1 b_2 - a_2 b_1)^2, \]
which is a contradiction.

Hence \( a_1 b_1 + a_2 b_2 \leq \sqrt{a_1^2 + a_2^2} \sqrt{b_1^2 + b_2^2}. \)

Since this has been proved for arbitrary real numbers \( a_1, a_2, b_1, b_2, \) it follows that
\[ (\forall a_1, b_1, a_2, b_2 \in \mathbb{R}) a_1 b_1 + a_2 b_2 \leq \sqrt{a_1^2 + a_2^2} \sqrt{b_1^2 + b_2^2}, \]
and our proof is complete.

2. Prove that the function \( f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \) defined by
\[ f(m, n) = 2^{m-1}(2n - 1) \quad \text{for} \quad (m, n) \in \mathbb{N} \times \mathbb{N} \]
is a bijection from \( \mathbb{N} \times \mathbb{N} \) to \( \mathbb{N} \).

PROOF:
We have to prove that \( f \) is injective and that \( f \) is onto \( \mathbb{N} \).

First we prove that \( f \) is injective.

Let \((m, n), (m', n')\) be two arbitrary members of \( \mathbb{N} \times \mathbb{N} \).
Assume \( f(m, n) = f(m', n') \).
We want to prove that \((m, n) = (m', n')\).

Since \( f(m, n) = f(m', n') \), it follows that \( 2^{m-1}(2n - 1) = 2^{m'-1}(2n' - 1) \).

Suppose \( m' > m \).
Then \( 2^{m-1}(2n - 1) = 2^{m'-1}(2n' - 1) = 2^{m'-m}2^{m-1}(2n' - 1) \), so \( 2n - 1 = 2^{m'-m}(2n' - 1) \).
Since \( m' > m \), the number \( 2^{m'-m}(2n' - 1) \) is even.
So \( 2^{m'-m}(2n' - 1) \) is not odd.
On the other hand, \( 2n - 1 \) is odd.
But \( 2n - 1 = 2^{m'-m}(2n' - 1) \), so the number \( 2n - 1 \) is both odd and not odd, which is a contradiction.

So \( m' > m \)
A similar argument shows that \( m > m' \).

Hence \( m' = m \).
Since \( 2^{m-1}(2n - 1) = 2^{m'-1}(2n' - 1) \) and \( m' = m \), it follows that \( 2n - 1 = 2n' - 1 \)
Hence \( n' = n \).
Since \( m' = m \) and \( n' = n \), we can conclude that \((m', n') = (m, n)\).
So \( f(m, n) = f(m', n') \Rightarrow (m', n') = (m, n) \).

Since \((m, n)\) and \((m', n')\) are arbitrary members of \( \mathbb{N} \times \mathbb{N} \), we have proved that \( f \) is injective.

We now prove that \( f \) is onto \( \mathbb{N} \).

Let \( q \) be an arbitrary natural number.
We want to find \((m, n) \in \mathbb{N} \times \mathbb{N} \) such that \( f(m, n) = q \).
The number \( q \) is either equal to \( 1 \) or \( > 1 \).
In the case when \( q = 1 \), we have \( 1 = 2^01 = 2^{1-1}(2 \times 1 - 1) \), so \( 1 = f(1, 1) \).
Now consider the case when \( q > 1 \).
Then \( q \) is prime or a product of primes.
Let \( \mu \) be the number of prime factors of \( q \) that are equal to \( 2 \).
Then \( q = 2^\mu \hat{q} \), where the number \( \hat{q} \) is odd.
Let \( m = \nu + 1 \).
Let \( n \in \mathbb{N} \) be such that \( \hat{q} = 2^n - 1 \).
Then \( q = 2^{m-1}(2n - 1) \).
So \( q = f(m, n) \).
Therefore \( f \) is onto \( \mathbb{N} \), and our proof is complete.
3. The theorem on the greatest common divisor says that “if $a, b$ are integers that are not both zero, and $c$ is the greatest common divisor of $a$ and $b$, then $c$ is an integer linear combination of $a$ and $b$.”

i. Give a precise mathematical definition of “greatest common divisor”.

ANSWER: If $a, b$ are integers, the greatest common divisor of $a$ and $b$ is an integer $c$ such that

- $c$ divides $a$ and $c$ divides $b$,
- if $x$ is any integer that divides $a$ and divides $b$, then $x \leq c$.

ii. Give a precise mathematical definition of “integer linear combination”.

ANSWER: If $a, b$ are integers, an integer linear combination of $a$ and $b$ is an integer $q$ such that $(\exists u, v \in \mathbb{Z})q = ua + vb$.

iii. Find the greatest common divisor of 15 and 22, and express it as an integer linear combination of 15 and 22.

ANSWER: The greatest common divisor of 15 and 22 is 1, because 15 and 22 have no common positive integer factors other than 1. An expression of 1 as an integer linear combination of 15 and 22 is

$$1 = 3 \times 15 + (-2) \times 22,$$

because $3 \times 15 = 45$, $(-2) \times 22 = 44$, and $45 + (-44) = 1$. (WARNING: In the final exam I am going to use other numbers, not 15 and 22, but they are also going to be easy ones.)

iv. Prove the theorem.

PROOF:

Let $S$ be the set of all positive integers that are linear combinations of $a$ and $b$. That is, let

$$S = \{n \in \mathbb{Z} : n > 0 \land (\exists u, v \in \mathbb{Z})n = ua + vb\}$$

Then $S$ is nonempty, because $a^2 + b^2 \in S$ (since $a^2 + b^2$ is clearly an integer linear combination of $a$ and $b$, and $a^2 + b^2$ because of our hypothesis that $a$ and $b$ are not both zero). So by the Well-ordering Principle $S$ has a smallest member $c$.

We now prove that $c$ is the greatest common divisor of $a$ and $b$.

We have to prove that

(I) $c$ divides $a$ and $b$.

(II) If $d$ is any integer that divides both $a$ and $b$, then $d \leq c$.

First we use the fact that $c$ is a linear combination of $a$ and $b$ to pick integers $m, n$ such that $c = ma + nb$.

We now prove that $c$ divides $a$.

Using the division theorem, we pick integers $q, r$ such that $a = cq + r$ and $0 \leq r < c$.

Then $a = (ma + nb)q + r$, so $r = (1 - mq)a + (-nq)b$. So $r$ is a linear combination of $a$ and $b$.

If $r > 0$ it would follow that $r \in S$, so $r$ would be a member of $S$ smaller than $c$, contradicting the fact that $c$ is the smallest member of $S$. So $r = 0$.

Then $a = cq$, so $c$ divides $a$.

The proof that $c$ divides $b$ is similar, so we omit it.

Finally, we prove Property (II) above.

Let $d$ be an integer that divides $a$ and $b$.

Pick integers $u, v$ such that $a = ud$ and $b = vd$.

Then $c = ma + nb = uda + vdb = (ua + vb)d$, so $d$ divides $c$.

Therefore, $d \leq c$ (because, if $c = kd, k \in \mathbb{Z}$, then $c = |c| = |k||d| \geq |d| \geq d$, using the fact that $|k| \geq 1$, which follows because $k \in \mathbb{Z}$ and $k \neq 0$; the fact that $k \neq 0$ is a consequence of the equality $c = kd$ and the inequality $c > 0$).

So we have proved (I) and (II).