7 Proving Non-Conditional Statements

Benjamin Basseri

January 10, 2025

Problem 1

Suppose $x \in \mathbb{Z}$. Then x is even if and only if $3x + 5$ is odd.

Solution: Use biconditional statements

$$x \text{ even} \iff 3x \text{ even} \iff 3x + 5 \text{ odd}$$

Problem 2

Suppose $x \in \mathbb{Z}$. Then x is odd if and only if $3x + 6$ is odd.

Solution: Use biconditional statements

$$x \text{ odd} \iff 3x \text{ odd} \iff 3x + 6 \text{ odd}$$

Problem 3

Given an integer a, then $a^3 + a^2 + a$ is even if and only if a is even.

Solution: Prove implication both ways

Forward direction. Using the contrapositive argument, we can prove this direction by showing a odd implies $a^3 + a^2 + a$ is odd. Since a is odd, a^2 is odd and a^3 is odd as well. That means $a^3 + a^2 + a$ is the sum of three odd numbers, which is odd.
Reverse direction.. If a is even then a^2 is even and so is a^3. Then $a^3 + a^2 + a$ is the sum of three even numbers, which is even.

Problem 4

Given an integer a, then $a^2 + 4a + 5$ is odd if and only if a is even.

Solution: Prove implication both ways

Forward direction. Using the contrapositive argument, we can prove this direction by showing a odd implies $a^2 + 4a + 5$ is even. Since a is odd, the expression $a^2 + 4a + 5$ represents (odd) + (odd) + (odd) which is even.
Reverse direction.. If a is even then a^2 is even and so is $4a$. Then $a^2 + 4a + 5$ is the sum of two even numbers and an odd number, which is odd.

Problem 5

An integer a is odd if and only if a^3 is odd.

Solution: Prove implication both ways

Forward direction. If a is odd then a^3 represents (odd)(odd)(odd), which is odd.
Reverse direction.. Using the contrapositive argument, if a is even then a^3 represents (even)(even)(even), which is even.

Problem 6

Suppose $x, y \in \mathbb{R}$. Then $x^3 + x^2y = y^2 + xy$ if and only if $y = x^2$ or $y = -x$.

Solution: Prove implication both ways

Forward direction. If $x^3 + x^2y = y^2 + xy$ then $x^3 + x^2y - y^2 - xy = 0$. Factoring, we can rewrite this as $x^2(x + y) = y(x + y)$. If $x + y = 0$ then $y = -x$. Otherwise, $x + y \neq 0$ and we can divide both sides by $x + y$, leaving $x^2 = y$.
Reverse direction.. As we saw, if $y = -x$ then both sides simplify to 0. If $y = x^2$ then plugging in x^2 for y gives $x^3 + x^4 = x^4 + x^3$, which makes the equation true.

Problem 7

Suppose $x, y \in \mathbb{R}$. Then $(x + y)^2 = x^2 + y^2$ if and only if $x = 0$ or $y = 0$.

Solution: Use algebraic manipulation

$$\begin{gathered}(x+y)^2 = x^2 + y^2 \\ \Updownarrow \\ x^2 + 2xy + y^2 = x^2 + y^2 \\ \Updownarrow \\ 2xy = 0 \\ \Updownarrow \\ xy = 0 \\ \Updownarrow \\ x = 0 \text{ or } y = 0\end{gathered}$$

Problem 8

Suppose $a, b \in \mathbb{Z}$. Prove that $a \equiv b \pmod{10}$ if and only if $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$.

Solution: Use definition of modular congruence

Forward direction. If $a \equiv b \pmod{10}$ then $10 \mid (a - b)$. This means $2 \mid (a - b)$ and $5 \mid (a - b)$, since 2 and 5 both divide 10. Therefore $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$.)
Reverse direction.. If $a \equiv b \pmod{2}$ and $a \equiv b \pmod{5}$ then $2 \mid (a - b)$ and $5 \mid (a - b)$. This means $(a - b)$ has a factor of 2 and a factor of 5, so we can write it as $2 \cdot 5k$ for some integer k, or

more simply $10k$. Therefore $10 \mid (a-b)$, so $a \equiv b \pmod{10}$.

Problem 9

Suppose $a \in \mathbb{Z}$. Prove that $14 \mid a$ if and only if $7 \mid a$ and $2 \mid a$.

Solution: Prove implication both ways

Forward direction.

$$14 \mid a \implies 7 \cdot 2 \mid a \implies 7 \mid a, 2 \mid a$$

Reverse direction.. If $7 \mid a$ and $2 \mid a$ then a has factors of both 7 and 2, and we can write $a = 7 \cdot 2k$ for some integer k or more simply $a = 14k$. Therefore $14 \mid a$.

Problem 10

If $a \in \mathbb{Z}$, then $a^3 \equiv a \pmod 3$.

Solution: Use cases

Suppose $a \equiv 0 \pmod 3$. Then $a = 3k$ for some k and $a^3 = 27k^3 = 3(9k^2)$. Therefore 3 divides a^3 and $a^3 \equiv a \pmod 3$.
If $a \equiv 1 \pmod 3$ then we can write $a = 3k+1$ for some k. Its cube is $a^3 = 27k^3 + 27k^2 + 9k + 1 = 3(9k^3 + 9k^2 + 3k) + 1$. Therefore 3 leaves a remainder of 1 after dividing a^3, and $a^3 \equiv a \pmod 3$.
If $a \equiv 2 \pmod 3$ then we can write $a = 3k+2$ for some k. Its cube is $a^3 = 27k^3 + 54k^2 + 36k + 8 = 3(9k^3 + 18k^2 + 12k + 2) + 2$. Therefore 3 leaves a remainder of 2 after dividing a^3, and $a^3 \equiv a \pmod 3$.
Another approach: Write $a = 3k + r$ for some remainder r. The binomial theorem states

$$(3k+r)^3 = \sum_{j=0}^{3} \binom{3}{j} (3k)^j r^{3-j}.$$

Notice that every term of the sum above will have a factor of 3 except for when $j = 0$, and that term is just r^3. So it suffices to check the cubes of r for $r = 0, 1, 2$. The cubes are 0, 1, and 8, each of which have the same value mod 3 as r itself. Therefore $a^3 \equiv a \pmod 3$.

Problem 11

Suppose $a, b \in \mathbb{Z}$. Prove that $(a-3)b^2$ is even if and only if a is odd or b is even.

Solution: Prove implication both ways

Forward direction. Prove the contrapositive statement: if a is even and b is odd, then $(a-3)$ is odd and b^2 is odd. This makes $(a-3)b^2$ an odd times an odd, which is odd. **Reverse direction.** If a is odd then $a-3$ is even, making the product $(a-3)b^2$ even. If b is even then b^2 is even, making the product $(a-3)b^2$ even.

Problem 12

There exists a positive real number x for which $x^2 < \sqrt{x}$.

Solution:

Positive reals get bigger when you square them if they're above 1, and they get smaller if they're between 0 and 1. So consider a number $k > 1$,

$$\left(\frac{1}{k}\right)^4 < \left(\frac{1}{k}\right)^2 < \frac{1}{k}$$

Notice that $1/k^2$ has the property that it's a positive real number and its square is less than its root.

Problem 13

Suppose $a, b \in \mathbb{Z}$. If $a + b$ is odd, then $a^2 + b^2$ is odd.

Solution: Use direct proof

Suppose $a + b$ is odd. Then one of the two terms must be odd and the other is even, making it (odd) + (even). Squaring preserves parity, so $a^2 + b^2$ reduces to (odd) + (event), which is odd.

Problem 14

Suppose $a \in \mathbb{Z}$. Then $a^2 \mid a$ if and only if $a \in \{-1, 0, 1\}$.

Solution: Prove implication both ways

Forward direction. Using the contrapositive statement, assume that $a \notin \{-1, 0, 1\}$. Then a is at least 2 or less than -2. For any such integer its square is strictly bigger than the base, so a^2 could not be a factor of a.

Reverse direction. If $a \in \{-1, 0, 1\}$ then a^2 is 1, 0, or 1 respectively, and each of these divides a.

Problem 15

Suppose $a, b \in \mathbb{Z}$. Prove that $a + b$ is even if and only if a and b have the same parity.

Solution: Prove implication both ways

Forward direction. If $a + b$ is even then either a and b are both even or both odd. If they had different parity, the expression would simplify to (odd) + (even), which is odd.
Reverse direction. The sum of two evens is even and the sum of two odds is even. So if a and b have the same parity then $a + b$ is even.

Problem 16

Suppose $a, b \in \mathbb{Z}$. If ab is odd, then $a^2 + b^2$ is even.

Solution: Use direct proof

If ab is odd, it must be that both a and b are odd. Otherwise, ab would be the product of an even number and another number, which would be even. Squaring preserves parity, so a^2 and b^2 are both odd. This makes $a^2 + b^2$ the sum of two odds, which is even.

Problem 17

There is a prime number between 90 and 100.

Solution: Show the example

The prime number 97 is between 90 and 100.

Problem 18

There is a set X for which $\mathbb{N} \in X$ and $\mathbb{N} \subseteq X$.

Solution: Construct an example

Let $X = \mathbb{N} \cup \{\mathbb{N}\}$. Then $\mathbb{N}$ is both a member of and a subset of X.

Problem 19

If $n \in \mathbb{N}$, then $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

Solution: Use induction

Base case. Let $n = 1$. Then we have $2^0 + 2^1 = 3$ and $2^{n+1} - 1 = 2^2 - 1 = 3$ as well.

Inductive hypothesis: Assume that $2^0 + 2^1 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

Inductive step: Consider the $n + 1$ case. The sum becomes:

$$\sum_{k=0}^{n+1} 2^k = 2^{n+1} + \sum_{k=0}^{n} 2^k$$

By the inductive hypothesis, $\sum_{k=0}^{n} 2^k = 2^{n+1} - 1$. Therefore the entire sum becomes:

$$2^{n+1} + 2^{n+1} - 1 = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$$

which confirms the inductive step.

Problem 20

There exists an $n \in \mathbb{N}$ for which $11 \mid (2^n - 1)$.

Solution: Show an example

We want to find a number such that is one more than a multiple of 11. The number 10 works, since $2^{10} = 1024$ and $1024 - 1 = 1023 = 11 \cdot 93$. Therefore $11 \mid (2^{10} - 1)$.

Problem 21

Every real solution of $x^3 + x + 3 = 0$ is irrational.

Solution: Use contradiction

Suppose there is a real solution $x = \frac{p}{q}$ where p and q are integers in lowest terms. Then we can rewrite the equation as:

$$\left(\frac{p}{q}\right)^3 + \frac{p}{q} + 3 = 0$$

Multiplying by q^3 gives:

$$\begin{aligned} p^3 + pq^2 + 3q^3 &= 0 \\ \implies p^3 &= q^2(-p - 3q) \end{aligned}$$

This means p^3 is a multiple of q, which implies p is a multiple of q. But this contradicts the assumption that p/q was in lowest terms.

Problem 22

If $n \in \mathbb{Z}$ then $4 \mid n^2$ or $4 \mid (n^2 - 1)$.

Solution: Use cases

Split into two cases: n is even or n is odd.

If n is even, then $n = 2k$ for some integer k. Then $n^2 = 4k^2$ which is divisible by 4.

If n is odd then $n = 2k + 1$ for some integer k, and its square is $4k^2 + 4k + 1 = 4(k^2 + k) + 1$, which has a remainder of 1 when divided by 4. Therefore $4 \mid (n^2 - 1)$.

Problem 23

Suppose a, b and c are integers. If $a \mid b$ and $a \mid (b^2 - c)$, then $a \mid c$.

Solution: Represent with modular forms

Since $a \mid b$ as $b \equiv 0 \pmod{a}$. Then $b^2 \equiv 0 \pmod{a}$ as well. And since $a \mid (b^2 - c)$, this means $b^2 \equiv c \pmod{a}$. Since b^2 is equivalent to 0 and c modulo a it must be that $c \equiv 0 \pmod{a}$ (modular congruence is transitive), which means that c is a multiple of a and $a \mid c$.

Problem 24

If $a \in \mathbb{Z}$, then $4 \nmid (a^2 - 3)$.

Solution: Use key fact that squares are 0 or 1 mod 4

Note that any integer a, when squared, is 0 or 1 mod 4. Therefore $a^2 - 3$ is either 1 or 2 mod 4 which means indivisible by 4.

Problem 25

If $p > 1$ is an integer and $n \nmid p$ for each integer n for which $2 \leq n \leq \sqrt{p}$, then p is prime.

Solution: Use contrapositive

The contrapositive statement is if integer $p > 1$ is composite, there exists an n between 2 and $\sqrt{p}$ that divides p.

Given p is composite, it has some factor n. Suppose $n = \sqrt{p}$, then $n^2 = p$ and $n \mid p$. Otherwise, n is either strictly greater or stricly less than $\sqrt{p}$.

If $n < \sqrt{p}$ then we have satistied the proof. But if $n > \sqrt{p}$ then it must have a corresponding factor m such that $nm = p$ and $m < \sqrt{p}$. For if $m > \sqrt{p}$, the product nm would exceed p as both factors would be larger than $\sqrt{p}$. Therefore $m < \sqrt{p}$ and m satisfies the statement.

Problem 26

The product of any n consecutive positive integers is divisible by $n!$.

Solution: Use induction

Base case. Let $n = 1$. Then the product of 1 consecutive positive integers is 1, which is divisible by $1!$.

Inductive hypothesis. Assume that the product of n consecutive positive integers is divisible by $n!$.

Inductive step. Take the $n+1$ case, and its product $k(k+1)\dots(k+n+1)$. If the inductive hypothesis product $k\dots(k+n)$ was divisible by $(n+1)!$ then so is the inductive step product $k\dots(k+n+1)$ and the proof is done. Otherwise, the hypothesis product does not have a factor of $n+1$. Moving onto the step's product $k\dots(k+n+1)$, by the pigeonhole principle it must contain a multiple of $n+1$ whereas the previous product did not. Therefore we can say $k\dots(k+n+1)$ is divisible by $n!$ and has a 'new' multiple of $n+1$ which makes it divisible by $(n+1)!$.

Problem 27

Suppose $a, b \in Z$ If $a^2 + b^2$ is a perfect square, then a and b are not both odd.

Solution: Use key fact that squares are 0 or 1 mod 4 to derive a contradiction

If $a^2 + b^2$ is a perfect square then it is 0 or 1 mod 4. If a and b were both odd their squares would be 1 mod 4, and their sum would be 2 mod 4, which is a contradiction.

Problem 28

Prove the division algorithm: If $a, b \in \mathbb{N}$, there exist *unique* integers q, r for which $a = bq + r$ and $0 \leq r < b$.

Solution: Use mutual inequality to prove uniqueness

The existence was proven in the text. We know that the coefficient on b is the largest non-negative multiple of b that does not exceed a, so to prove q's uniqueness we need to show that this maximum is unique.
Let $M = \{q \in \mathbb{Z} : 0 \leq bq \leq a\}$, the set of non-negative multiples of b that do not exceed a. Since $0 \in M$, M is non-empty. To show its maximum is unique, suppose q_1 and q_2 both have the property that for all $x \in M$, $x \leq q_1$ and $x \leq q_2$. Then $q_1 \leq q_2$ and $q_2 \leq q_1$, which means $q_1 = q_2$. Therefore the coefficient on b is unique.

Going back to the algorithm $a = qb + r$ we can solve for r by writing $a - qb = r$. This has a unique solution in the integers, therefore r is unique.

Problem 29

If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Solution:

Suppose $\gcd(a, b) = 1$. If $a = 1$ then a divides c. Otherwise, a and b have no factors in common, including a itself. Therefore a cannot divide b. But since a divides the product bc, it must divide c.

Problem 30

Suppose $a, b, p \in \mathbb{Z}$ and p is prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$.

Solution: Use prime decomposition

Since p divides the product ab, it must be that p appears in the prime decomposition of a, b or both. Since p is prime, it cannot be that it is the product of some prime in a and another in b, making it a factor of neither. Therefore p must divide a or b.

Problem 31

If $n \in \mathbb{Z}$, then $\gcd(n, n + 1) = 1$.

Solution: Direct proof, rewriting $n, n + 1$ as multiples of d

Let $d = \gcd(n, n + 1)$. Then $n = dx$ and $n + 1 = dy$ for some integers, x, y. Then write:

$$n + 1 - n = 1 = dy - dx = d(y - x)$$

Since d, x, y are all integers, for $d(y - x)$ to equal 1 d must be ± 1. And since 1 is the greatest of the two and indeed a valid divisor for any $n, n + 1$, we have $\gcd(n, n + 1) = 1$.

Problem 32

If $n \in \mathbb{Z}$ then $\gcd(n, n + 2) \in \{1, 2\}$.

Solution: Use direct proof, rewriting $n, n + 2$ as multiples of d

Let $d = \gcd(n, n + 2)$. Then $n = dx$ and $n + 2 = dy$ for some integers, x, y. Then write:

$$n + 2 - n = 2 = dy - dx = d(y - x)$$

Since d is a positive integer it must be either 1 or 2.

Problem 33

If $n \in \mathbb{Z}$, then $\gcd(2n + 1, 4n^2 + 1) = 1$.

Solution: Express one of the numbers in terms of the other

Let $d = \gcd(2n+1, 4n^2+1)$. Then $2n+1 = dx$ and $4n^2+1 = dy$ for some integers x, y. However, we can rewrite $4n^2+1 = (2n+1)(2n-1)+2$. Using dx we can then say:

$$\begin{aligned}(2n+1)(2n-1)+2 &= dy\\ dx(2n-1)+2 &= dy\\ 2 &= dy - dx(2n-1)\\ 2 &= d(y - x(2n-1))\end{aligned}$$

This shows that d divides 2, so it must be 1 or 2. However we also know $dx = 2n+1$, an odd number. Since only odd numbers can multiply to an odd number, d must be odd, which means $d = 1$.

Problem 34

Suppose $a, b \in \mathbb{N}$. Then $a = \gcd(a, b)$ if and only if $a \mid b$.

Solution: Prove implication both ways

Forward direction. Suppose $a = \gcd(a, b)$. Then a divides b so $a \mid b$.

Reverse direction. Suppose $a \mid b$. Of course a divides itself so a divides both a and b making it a common divisor. No number higher than a can divide a so it is the greatest common divisor.

Problem 35

Suppose $a, b \in \mathbb{N}$. Then $a = \operatorname{lcm}(a, b)$ If and only if $b \mid a$.

Solution: Prove implication both ways

Forward direction. Suppose $a = \operatorname{lcm}(a, b)$. Then a is a multiple of b so $b \mid a$.

Reverse direction. Suppose $b \mid a$, making b a multiple of a. It is also trivially a multiple of itself, so it is a common multiple. No number smaller than b can be a multiple of b, so b is the least common multiple.