Proofs in Mathematics

Definitions

A *definition* is an exact, unambiguous description that provides a meaning for a term or a phrase. Its purpose is to make sure that everyone agrees on the exact meaning of each term. The sets N, Z, R, and Q and the relations $\in$ and $\subseteq$ have been defined when we studied set theory. The following are some examples of mathematical definitions.

Definition 1 (Even integers) $n = 2a$

An integer n is *even* if and only if $n = 2a$ for some integer a.

Definition 2 (Odd integers) $n = 2a+1$

An integer n is *odd* if and only if $n = 2a + 1$ for some integer a.

Definition 3

Two integers are said to have the *same parity* if they are both even or they are both odd; otherwise they are said to have *opposite parity*.

Definition 4 (Division) $b = ac$

Suppose a and b are integers where $a \neq 0$. We say that a *divides* b, written $a|b$, if and only if $b = ac$ for some integer c. In this case we also say that a is a *divisor* of b, and that b is a *multiple* of a. Ex :- $3|12 \Rightarrow$ True , $5|12 \Rightarrow$ False, $6|6 \Rightarrow$ True, $-1|6 \Rightarrow$ True

Definition 5 (Primes and composites)

A *prime number* (a *prime*) is any integer greater than 1 which has exactly two positive divisors, 1 and n. An integer greater than 1 that is not a prime is said to be a *composite*.

Definition 6 (GCD and LCM)

The *greatest common divisor* of integers a and b, denoted $gcd(a, b)$, is the largest integer that divides both a and b. The *least common multiple* of non-zero integers a and b, denoted $lcm(a, b)$, is smallest positive integer that is a multiple of both a and b.

Axioms ⇒ Assume to be true, without any explanation

When studying a certain subject, an *axiom* (also called a *postulate*) is a statement that is assumed to be true or which everyone studying that subject accepts as true without requiring an explanation. Axioms are usually starting points for deriving further statements that are true (given that the axioms are true).

Definition 7 (Axioms of Algebra)

For any numbers x, y, and z,

- (Axiom of Reflexivity) $x = x$
- (Axiom of Symmetry) $x = y$ implies $y = x$
- (Axiom of Transitivity) $x = y$ and $y = z$ implies $x = z$
- (Axiom of Addition) $x = y$ implies $x + z = y + z$
- (Axiom of Multiplication) $x = y$ implies $xz = yz$.

Some axioms are used to define certain objects or concepts.

Definition 8 (Groups) (Next Semester)

A *group* is a set, say G, together with a binary operation, say $\cdot$, satisfying the following properties (called the *group axioms*):

- (Closure) For all x and y in G, the result of the operation $x \cdot y$ is also in G.
- (Associativity) For all x, y, and z in G, the equation $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ holds.
- (Identity) There exists an element e in G called an identity element, such that for every element x in G, the equation $e \cdot x = x \cdot e = x$ holds.
- (Inverse) For each x in G, there exists an element y in G such that $x \cdot y = y \cdot x = e$, where e is an identity element.

Sometimes an axiom is called a *law*. A *law* is often accepted to be true based on empirical evidence from observations or experiments. For example, Newton's three laws of motion were generally accepted to be true based on empirical evidence.

But some laws are <u>not</u> axioms but are statements which have been proved to be true. For example, the Law of Sines:

$$\frac{\sin(A)}{a} = \frac{\sin(B)}{b} = \frac{\sin(C)}{c}$$

<u>Facts</u> → consequences of axioms and def. ; no need for explanation

When mathematicians studying a subject, there might be certain statements which are well known and commonly accepted to be true. They may then state those statements as facts and use them in their study without giving any justification.

Fact 9. An integer is odd if and only if it is <u>not</u> even.

Fact 10. Suppose a and b are integers. Then

- $a + b$ is an integer,
- $a - b$ is an integer,
- ab is an integer.

Theorems, Propositions, Lemmas, Corollaries

A *theorem* is a statement that [redacted] has been proved to be true. Mathematicians usually reserve the word theorem for a statement which is important or significant to the subject under study.

A theorem which is useful or worth mentioning but not particularly important is often called a *proposition*.

A *lemma* is a proposition whose main purpose is to help proving another statement.

A *corollary* is a theorem which immediately follows from a theorem or a proposition.

Proofs

A *proof* of a statement is an argument which unequivocally demonstrates the truth of the statement. Stated in logical terms, a proof for a statement p is a valid deductive argument whose conclusion is p.

A *disproof* of a statement is a proof of the negation of the statement. In other words, a disproof is an argument which unequivocally refutes the truth of the statement.

To *prove* a statement means to find a proof of that statement. Conversely, to *disprove* a statement means to find a disproof of that statement.

An unproven statement that is believed to be true is called a *conjecture*.

For example, the Goldbach's Conjecture "*Every even integer greater than 2 can be expressed as the sum of two primes*" has neither been proved nor disproved for more than two centuries.

Examples of theorems, propositions, lemmas, and corollaries and their proofs

In the rest of this section, we give some examples of lemmas and theorems from the subject called Number Theory, as well as their proof. In the future, when you are asked to prove some statement, you may refer to these lemmas or theorems. Be noted that the proofs explained in this section rely on the proof techniques which we will be studying after this section. So at first you may want to skim the proofs given here and then come back to study them more carefully after you have studied proof techniques in more detail.

Theorem 11 (Division Algorithm). For any integer x and integer $y > 0$, there are unique integers m and r such that $x = my + r$ and $0 \leq r < y$.

Proof.

[Existence] Suppose x and y are any integers such that $y > 0$. Consider the sequence:

$$\ldots, -4y, -3y, -2y, -y, 0, y, 2y, 3y, 4y, \ldots.$$

Since $y > 0$, this is an infinite increasing sequence. Hence, x must be less than some number in this sequence. Let cy be the least number in this sequence such that $x < cy$. Hence,

$$(c-1)y \leq x < cy.$$

Let m be $c - 1$ and r be $x - (c-1)y$.

Then clearly, $x = my + r$ and $0 \leq r < m$.

[Uniqueness] Suppose there are integers m_1, m_2, r_1, r_2 such that

$$x = m_1 y + r_1 \text{ and } 0 \leq r_1 < y$$

$$x = m_2 y + r_2 \text{ and } 0 \leq r_2 < y$$

WLOG, assume that $r_1 \leq r_2$.

It follows that

$$m_1 y + r_1 = m_2 y + r_2$$

$$(m_2 - m_1)\, y = r_1 - r_2$$

Since $0 \leq r_1 < y$ and $0 \leq r_2 < y$ and $r_1 \leq r_2$, it must be that $0 \leq r_1 - r_2 < y$.

This implies that

$$0 \leq (m_2 - m_1)\, y < y.$$

Dividing y across this inequality,

$$0 \leq m_2 - m_1 < 1.$$

Since m_2 and m_1 are integers, then $m_2 - m_1 = 0\ or\ m_2 = m_1$.

Since $x = m_1 y + r_1 = m_2 y + r_2$, it follows that $r_1 = r_2$.

Therefore, there are unique integers m and r such that $x = my + r$ and $0 \leq r < y$.

■

Definition 12 (Quotients and Remainders). For any integer x and integer $y > 0$, if $x = my + r$ where $0 \leq r < y$, then m is called the (integer) *quotient* of the division of x by y and r is called the *remainder* of the division of x by y. The remainder r is sometimes denoted by $x\ mod\ y$.

Fact 13. For any integer x and integer $y > 0$, the remainder of the division of x by y must be in the set $\{0,1,2,\ldots,y-1\}$.

Definition 14 (Congruence). Given any integers a and b and a positive integer m, it is said that a is *congruent* to b modulo m if and only if $m|(a-b)$.

Example 15. The following statements are true.

- 8 is congruent to 2 modulo 3.
- 1 is congruent to 11 modulo 5.
- 1 is <u>not</u> congruent to 11 modulo 3.

Lemma 16. Suppose a, b, c are any integers such that $a \neq 0$.

A. If $a|b$ and $a|c$ then $a|(b+c)$.
B. If $a|(b+c)$ and $a|b$ then $a|c$.

Proof.

(A) Suppose $a|b$ and $a|c$. Hence, for some integers m and n,

$$b = ma$$
$$c = na$$

Adding these two equations, we obtain

$$b + c = ma + na = (m + n)a,$$

which implies that $a|(b + c)$.

(B) Suppose $a|(b + c)$ and $a|b$. Hence, for some integers m and n,

$$b + c = ma$$
$$b = na$$

Subtracting the first equation by the second one, we obtain

$$c = ma - na = (m - n)a,$$

which implies that $a|c$.

■

Lemma 17. Suppose a and b are positive integers and z is the smallest positive integers such that $a|bz$. For any positive integer c, if $a|bc$, then $z|c$.

Proof. Suppose $a|bc$. Assume that $z \nmid c$.

By **Theorem 11Theorem 11Theorem 11**,

$$c = zm + r \tag{1}$$

where $0 < r < z$.

Multiplying (1) by b,

$$bc = bzm + br$$

Since $a|bc$ and $a|bzm$ (because $a|bz$), by **Lemma 16**, it follows that $a|br$.

But since $r < z$, this contradicts the fact that z is the smallest positive integer where $a|bz$. Therefore, $z|c$.

■

Lemma 18 (Euclid's Lemma). Suppose p is prime and x and y are any integers. If $p|xy$, then either $p|x$ or $p|y$.

Proof. Suppose $p|xy$. Let z be the *smallest* positive integer such that

$$p|xz \tag{1}$$

By **Lemma 17**, since $p|xy$, it follows that

$$z|y \tag{2}$$

And because $p|xp$, by **Lemma 17** again, it follows that $z|p$. Since p is prime, then either $z = 1$ or $z = p$.

- If $z = 1$, from (1), it follows that $p|x$.
- If $z = p$, from (2), it follows that $p|y$.

Therefore, if $p|xy$, then either $p|x$ or $p|y$.

■

Definition 19 (Prime Factorization). Given an integer $x > 1$, a prime factorization of x is a product of the form $p_1p_2p_3 \ldots p_n$ where $p_1, p_2, p_3, \ldots, p_n$ $(n \geq 1)$ are primes such that $p_1 \leq p_2 \leq p_3 \leq \cdots \leq p_n$.

Example 20. A prime factorization of 3500 is $2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 \cdot 7 = 2^2 \cdot 5^3 \cdot 7$.

It may seem clear to you that every integer greater than 1 has a prime factorization and it is also a unique one. This is, in fact, the case. This existence of unique prime factorization is called the **Fundamental Theorem of Arithmetic**. Before we proceed to show the proof of this theorem, let us prove a lemma which is a consequence of Euclid's Lemma.

Lemma 21. Suppose p is prime and $q_1, q_2, \ldots, q_n$, where $n \geq 1$, are any primes.

$$p|q_1q_2 \ldots q_n \text{ if and only if } p = q_i \text{ for some } i.$$

Proof. (⇒) We need to show that if $p|q_1q_2 \ldots q_n$ then $p = q_i$ for some i. Assume that this is not the case. Thus, there are some primes $p, q_1, q_2, \ldots, q_n$ for some $n \geq 1$ such that

$$p|q_1q_2 \ldots q_n \text{ and } p \neq q_i \text{ for all } i \tag{1}$$

- Since $p|q_1(q_2 \ldots q_n)$, by Euclid's Lemma, it follows that either $p|q_1$ or $p|q_2 \ldots . q_n$. Because q_1 is a prime, the only factors of q_1 are 1 and q_1. Since p is a prime (thus must be greater than 1), $p|q_1$ would imply that $p = q_1$. But this contradicts the assumption (1) above. So it must be that $p|q_2 \ldots . q_n$.
- Since $p|q_2(q_3 \ldots q_n)$, by Euclid's Lemma, it follows that either $p|q_2$ or $p|q_3 \ldots . q_n$. Because q_2 is a prime, the only factors of q_2 are 1 and q_2. Since p is a prime (thus must be greater than 1), $p|q_2$ would imply that $p = q_2$. But this contradicts our assumption (1) above. So it must be that $p|q_3 \ldots . q_n$.
- …

- Since $p|q_{n-1}q_n$, by Euclid's Lemma, it follows that either $p|q_{n-1}$ or $p|q_n$. Because q_{n-1} is a prime, the only factors of q_{n-1} are 1 and q_{n-1}. Since p is a prime (thus must be greater than 1), $p|q_{n-1}$ would imply that $p = q_{n-1}$. But this contradicts the assumption (1) above. So it must be that $p|q_n$.
- Since $p|q_n$ and q_n is a prime, either $p = 1$ or $p = q_n$. But since p is also a prime, p must be greater than 1 and, by the assumption (1) above, $p \neq q_n$. We thus have a contradiction.

Therefore, if $p|q_1q_2 \dots q_n$ then $p = q_i$ for some i.

(⇐) We need to show that if $p = q_i$ for some i then $p|q_1q_2 \dots q_n$. But this is obvious.

■

Theorem 22 (Fundamental Theorem of Arithmetic)

Every integer greater than 1 has a unique prime factorization.

Proof.

[Existence] Assume for the sake of contradiction that there is an integer greater than 1 that has no prime factorization. In particular, let x be the *smallest* integer greater than 1 that has no prime factorization. Obviously, x cannot be prime, otherwise x itself would be its prime factorization. Hence, x is a composite, and thus $x = yz$ for some integers y and z greater than 1. Since x is the smallest integer greater than 1 that has no prime factorization, it follows that both y and z must have prime factorizations. It is clear that we can multiply a prime factorization of y with a prime factorization of z and rearrange the factors to obtain a prime factorization of x. This contradicts the assumption that x has no prime factorization.

[Uniqueness] Suppose there is an integer greater than 1 which has two different prime factorizations. In particular, let x be the *smallest* integer greater than 1 with two different prime factorizations, say

$$x = p_1p_2p_3 \dots p_m$$

$$x = q_1q_2q_3 \dots q_n$$

Clearly, $p_1p_2p_3 \dots p_m$ and $q_1q_2q_3 \dots q_n$ cannot have a common factor, otherwise we would be able to cancel out a common factor and obtain an integer smaller than x with two different prime factorizations. This means that p_1 is not equal to any factor $q_1, q_2, \dots, q_n$. By **Lemma 21**, this would imply that $p_1 \nmid q_1q_2q_3 \dots q_n$ which would mean that $p_1 \nmid x$. This is a contradiction since p_1 is a factor of x.

■

Proof Techniques

1. Direct proof - Proving a conditional statement directly.

To prove "If P then Q" (or "P implies Q" or "Q if P"),

assume P then try to prove Q.

> Assume/Suppose P.
>
> ⋮
>
> Hence, Q.
>
> Therefore, if P then Q.

Q) P → q

Ass P

⋮

q

Therefore if P then q

Proposition 23. If x is an odd integer, then so is x^2.

Proof. Assume that x is an odd integer.

By **Definition 2**, let y be an integer such that $x = 2y + 1$.

Then

$$\begin{aligned} x^2 &= (2y+1)^2 \\ &= 4y^2 + 4y + 1 \\ &= 2(2y^2 + 2y) + 1 \end{aligned}$$

Hence, $x^2 = 2z + 1$ where $z = 2y^2 + 2y$.

By **Definition 2**, x^2 is also odd.

Therefore, if x is an odd integer, then so is x^2.

■

If x is odd, then x^2 is odd

Ans) Ass x is odd

By def. → $x = 2a+1$; some a is interger

$x^2 = (2a+1)^2$

$x^2 = 4a^2+4a+1$

$= 2(2a^2+2a)+1$

$x^2 = 2b+1$; some b is interger

$\therefore x^2 =$ odd

Proposition 24. If x is an odd integer, then $x + 1$ is even.

Proof. Suppose x is an odd integer.

By **Definition 2**, let y be an integer such that $x = 2y + 1$.

$$x + 1 = 2y + 1 + 1 = 2y + 2 = 2(y + 1)$$

By **Definition 1**, since $x + 1 = 2c$ for some integer c, it follows that $x + 1$ is even.

Therefore, if x is an odd integer, $x + 1$ is even.

■

Proposition 25. If x and y are even integers, then so is $x + y$.

Proof. Assume that x and y are even integers.

By **Definition 1**, let a and b be integers such that $x = 2a$ and $y = 2b$.

Then

$$x + y = 2a + 2b = 2(a + b)$$

Hence, $x + y = 2c$ for some integer c.

By **Definition 1**, $x + y$ is an even integer.

Therefore, if x and y are even integers, then so is $x + y$.

■

Proposition 26. If x is even and y is odd, then $x + y$ is odd.

Proof. Suppose x is even and y is odd.

By **Definition 1**, let a be an integer such that $x = 2a$.

By **Definition 2**, let b be an integer such that $y = 2b + 1$.

$$x + y = 2a + 2b + 1 = 2(a + b) + 1$$

Hence, $x + y = 2c + 1$, for some integer c.

By **Definition 2**, $x + y$ is odd.

Therefore, if x is even and y is odd, then $x + y$ is odd.

■

2. Proving a conditional statement by contraposition.

To prove “If P then Q” (or “P implies Q” or “Q if P”),

assume Q is not true then try to prove P cannot be true .

Assume/Suppose Q is not true.

⋮

Hence, P is not true.

Therefore, if P then Q.

Corollary 27. If x^2 is even, then x also is even.

Proof. Assume that x is not even.

By **Fact 9**, x is odd.

By **Proposition 23**, x^2 is odd.

By **Fact 9** again, x^2 is also not even.

Therefore, if x^2 is even, then x also is even.

■

Proposition 28. If $7x + 9$ is even, then x is odd.

Proof. (Direct) Suppose $7x + 9$ is even.

Thus $7x + 9 = 2a$, for some integer a.

Subtracting $6x + 9$ from both sides, we get $x = 2a - 6x - 9$.

Thus

$$\begin{aligned} x &= 2a - 6x - 9 \\ &= 2a - 6x - 10 + 1 \\ &= 2(a - 3x - 5) + 1. \end{aligned}$$

Consequently, $x = 2b + 1$, for some integer b.

By **Definition 2**, this implies that x is odd.

Therefore, if $7x + 9$ is even, then x is odd.

■

Proof. (Contrapositive) Suppose x is not odd.

Thus, by **Fact 9**, x is even. By **Definition 1**, $x = 2a$ for some integer a.

Then

$$\begin{aligned} 7x + 9 &= 7(2a) + 9 \\ &= 14a + 8 + 1 \\ &= 2(7a + 4) + 1. \end{aligned}$$

Therefore, $7x + 9 = 2b + 1$, for some integer b, which implies that $7x + 9$ is odd.

Consequently, $7x + 9$ is not even.

Therefore, if $7x + 9$ is even, then x is odd.

■

Proposition 29. If xy is even, then either x or y is even.

Proof. Assume that it is not the case that either x or y is even.

This means that both x and y are not even.

By **Fact 9**, they are both odd.

By **Definition 2**, let a and b be integers such that $x = 2a + 1$ and $y = 2b + 1$.

Then

$$xy = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1.$$

Since $xy = 2c$ for some integer c, it follows by **Definition 2** that xy is odd.

By **Fact 9**, xy is not even.

Therefore, if xy is even, then either x or y is even.

■

3. Proof by cases (also called, “Proof by exhaustion”) → consider all possibilities

Suppose either P_1 or P_2 or ... or P_m is true and each P_i implies Q.

Then, we can infer Q.

> Since P_1 or P_2 or ... P_m must be true, we prove by cases, as follows:
>
> **Case 1**. Suppose P_1.
>
> ...
>
> Therefore, Q.
>
> ⋮
>
> **Case m**. Suppose P_m.
>
> ...
>
> Therefore, Q.
>
> Since Q is true in all cases, we can conclude that Q must be true.

Proposition 30. If x and y are both odd or both even, then $x - y$ is even.

Proof. Assume that x and y are both odd or both even both odd $\vee$ both even

Case 1: x and y are both odd. From the definition of odd integers, there are some integers a and b such that

$$\boxed{\begin{aligned} x &= 2a+1 \\ y &= 2b+1 \end{aligned}}$$

It follows that

$$\boxed{\begin{aligned} x - y &= (2a+1) - (2b+1) \\ &= 2a - 2b \\ &= 2(a-b). \end{aligned}}$$

This implies that $x - y$ is even.

Case 2: x and y are both even. From the definition of even integers, there are some integers a and b such that

$$\boxed{\begin{aligned} x &= 2a \\ y &= 2b \end{aligned}}$$

It follows that

$$\boxed{\begin{aligned} x - y &= 2a - 2b \\ &= 2(a - b). \end{aligned}}$$

This implies that $x - y$ is even.

Since, in any case, $x - y$ is even, we can conclude that, if x and y are both odd or both even, then $x - y$ is even.

■

When we do proof by cases, if it is clear that the proof in each case is very similar to the others, then you can prove just one case and omit the others.

Trick 1. Prove Case 1 and, in other cases, write "*Similar to Case 1*".

Trick 2. Write "*Without loss of generality, we assume P_1*". The acronym WLOG is sometimes used to abbreviate this phrase.

Warning. Very often, a proof is later found out to be wrong because of an erroneous assumption that the cases are similar, when in fact they are not. So be really sure that the omitted cases are really similar to what you proved.

Proposition 31. If m and n have opposite parity (i.e. they are not both odd and not both even), then $m + n$ is odd.

Proof (Long version). Suppose m and n are two integers with opposite parity. We need to show that $m + n$ is odd. This is done in two cases, as follows.

Case 1. Suppose m is even and n is odd. Thus $m = 2a$ and $n = 2b + 1$ for some integers a and b. Therefore $m + n = 2a + 2b + 1 = 2(a + b) + 1$, which is odd.

Case 2. Suppose m is odd and n is even. Thus $m = 2a + 1$ and $n = 2b$ for some integers a and b. Therefore $m + n = 2a + 1 + 2b = 2(a + b) + 1$, which is odd.

In either case, $m + n$ is odd.

■

Proof (Shortened version). Suppose m and n are two integers with opposite parity. We need to show that $m + n$ is odd. **WLOG, suppose m is even and n is odd.**

Thus $m = 2a$ and $n = 2b + 1$ for some integers a and b.

Therefore, $m + n = 2a + 2b + 1 = 2(a + b) + 1$, which is odd.

■

Another way: Case 1 (done)

Case 2: (similar to Case 1)

4. Proof by contradiction (also called, Reductio Ad Absurdum)

Sometimes it is difficult to prove that a statement holds directly. Instead, we could assume that the statement is not true, and show that it's impossible as it would lead a contradiction.

To prove P, assume that P is not true and try to derive a contradiction

Assume P is not true. ⋮ So P must be true, contradicting what we assumed earlier. Therefore, P.	Assume P is not true. ⋮ Q ⋮ ¬Q, a contradiction. Therefore, P.

Proposition 32. If a and b are integers, $a^2 - 4b - 2 \neq 0$.

Proof. Suppose a and b are integers.

Assume that $a^2 - 4b - 2 = 0$. Then

$a^2 = 4b + 2 = 2(2b + 1) \qquad (1)$

This implies that a^2 is even.

Either a is odd or it is <u>not</u> odd.

Case 1: Suppose a is odd.

By **Definition 2**, $a = 2x + 1$ for some integer x.

$$a^2 = (2x+1)^2 = 4x^2 + 4x + 1 = 2(2x^2 + 2x) + 1,$$

which is odd, contradicting what we have shown earlier.

Case 2: Suppose a is <u>not</u> odd. By **Fact 9**, a is even.

By **Definition 1**, $a = 2x$ for some integer x.

$$a^2 = (2x)^2 = 4x^2$$

From equation (1),

$$4b + 2 = 4x^2$$
$$2 = 4x^2 - 4b$$
$$2 = 4(x^2 - b)$$
$$1 = 2(x^2 - b),$$

which is clearly false because 1 is odd but $2(x^2 - b)$ is even. A contradiction!

Since we have contradictions in both cases, we can conclude that $a^2 - 4b - 2 \neq 0$. Therefore, the proposition is true.

■

Theorem 33. The number $\sqrt{2}$ is irrational.

Proof. Suppose for the sake of contradiction that it is not true that $\sqrt{2}$ is irrational. Then $\sqrt{2}$ is rational, so there are integers a and b for which

$$\sqrt{2} = a/b. \qquad (1)$$

Let this fraction be fully reduced; in particular, this means that a and b are not both even. (If they were both even, the fraction could be further reduced by factoring 2's from the numerator and denominator and canceling.)

Squaring both sides of Equation (1) gives $2 = a^2/b^2$, and therefore

$$a^2 = 2b^2. \qquad (2)$$

From this it follows that a^2 is even. But we proved earlier that a^2 being even implies a is even. Thus, as we know that a and b are not both even, it follows that b is odd.

Now, since a is even there is an integer c for which $a = 2c$. Plugging this value for a into Equation (2), we get $(2c)^2 = 2b^2$ which implies that $4c^2 = 2b^2$ and so $b^2 = 2c^2$. This means b^2 is even, so b is even also. But previously we deduced that b is odd. Thus we have a contradiction. Therefore, our assumption that $\sqrt{2}$ is not irrational is wrong.

■

5. Instantiation rule

From a universally quantified statement “For all x, P(x)”,

we can derive P(c) for any term c.

For all x, P(x).
Hence, P(c).

$$\frac{\forall x\ p(x)}{p(t)}\ \forall E$$

for any term t

From a universally quantified statement, “For all x in S, P(x)” where S is a set,

we can derive P(c) for any element c in S.

Everyone ~~is~~ in SE1 is smart.
Jay is in SE1.
Therefore, Jay is smart.

For all x in SE1, smart(x).
Jay is in SE1
Therefore, smart(Jay).

Fact 34. Every SE student likes Python.

Proposition 35. If Jay is an SE student, then he must like Python.

Proof. Suppose Jay is an SE student.

Since, from **Fact 34**, every SE student likes Python, it follows that Jay likes Python.

Therefore, if Jay is an SE student, then he must like Python. ✓

■

6. Prove that some statement P(x) is true for all x

Let c is any object

⋮

P(C)

$\forall x\ P(x)$

(generalization rule)

Use Generalization Rule

To prove "For all x, P(x)", we let a variable x be any object in the universe (to avoid confusion, choose a variable x which is not used earlier in the proof).

Then try to prove that P(x) holds.

> Let x be any integer/number/character.
>
> ⋮
>
> Hence, P(x).
>
> Therefore, P(x) is true for every x.

To prove "For all x in S, P(x)", we let a variable x be any element of the set S.

Then try to prove that P(x) holds.

> Let x be any element in S.
>
> ⋮
>
> Hence, P(x).
>
> Therefore, P(x) is true for every x in S.

Proposition 36. Suppose everyone in this class is a cat and every cat likes fish. Then everyone in this class likes fish.

Proof. Suppose x is any person in the class.

Since every in this class is a cat, x must be a cat. instantiation rule

Since every cat likes fish, x must like fish.

Therefore, everyone in this class likes fish.

generiazation

■

Fact 37. Every prime number greater than 2 is odd.

Proposition 38. The square of every prime number greater than 2 is odd.

(In other words, for every prime number x greater than 2, the square of x is odd.)

Proof. Let x be a prime number greater than 2.

By **Fact 37**, x is odd.

By **Proposition 23**, the square of x must be odd.

Therefore, we can conclude that the square of every prime number greater than 2 is odd.

(Alternative) Proof. Suppose x is a prime number greater than 2.

Since every prime number greater than 2 is odd, therefore x is odd.

Since the square of every odd number is odd, so the square of x is odd.

Therefore, the square of every prime number greater than 2 is odd.

■

For all even interger x, x^2 is even

Proposition 39. The square of an even integer is also even.

Proof. Suppose x is an even integer.

By **Definition 1**, $x = 2y$ for some number y.

Thus

$$\begin{aligned} x^2 &= (2y)^2 \\ &= 2(2y^2) \end{aligned}$$

This means that x^2 is divisible by 2, and is thus even.

Therefore, for any even number x, the square of x is also even.

■

7. Prove that there is some x such that P(x) is true

A constructive approach is to find some object c such that P(c) is true.

Suppose P(c) is true for some object c. Then we can derive "For some x, P(x)" or "There exists x such that P(x)".

P(c)

Hence, P(x) for some x.

$$\frac{P(c)}{\exists x\, P(x)}\ \exists I$$

Suppose P(c) is true for some element c in a set S. Then we can derive "For some x in S, P(x)" or "There exists some c in S such that P(c)."

c is in S.

P(c)

Therefore, P(x) for some x in S.

Just pick any number

Proposition 40. There exists an even integer that can be written as the sum of two prime numbers (possibly the same) in two different ways.

Proof. Let n be 10. Clearly, n is even.

Moreover,

$$n = 10 = 3 + 7 = 5 + 5.$$

Since 3, 5, and 7 are primes, it follows that n can be written as the sum of two prime numbers in two ways.

Therefore, there exists an even integer that can be written as the sum of two prime numbers in two ways.

■

8. Existential elimination rule

Suppose it is given or has been shown that there is some x such that P(x) holds. Then we can infer that there is an element c such that P(c) holds.

$\exists x \; p(x)$

Let c be element such that p(c) is true

> There is some x such that P(x) holds.
>
> Let c be an element such that P(c) holds.

Suppose it is given or has been shown that there is some x in set S such that P(x) holds. Then we can infer that there is an element c in S such that P(c) holds.

> There is some x in S such that P(x) holds.
>
> Let c be an element in S such that P(c) holds.

Fact 41. Every necktie found in the school belongs to some male student in the school.

Fact 42. Every male student wear leather shoes.

Proposition 43. If a necktie is found in the school, then there must be some student in the school wearing leather shoes.

Proof. Suppose a necktie is found in the school.

Let x denote such a necktie.

By **Fact 41**, necktie x belongs to some male student in the school; let m denote that male student.

By **Fact 42**, m must wear leather shoes. Hence, there is some student in the school that wears leather shoes.

Therefore, we can conclude that if there is a necktie found in the school, then there must be some student in the school that wears leather shoes.

■

$p \Leftrightarrow q \equiv (p \to q) \wedge (q \to p)$

9. Proving "if and only if"

To show that "p if and only if q" or that p and q are equivalent, there are two steps:

1. Prove that p implies q $p \to q$
2. Prove that q implies p $q \to p$
   (or alternatively, prove that ¬p implies ¬q)

To prove that p if and only if q

(→) Suppose p is true.

....

q is also true. Hence, p implies q.

(←) Suppose q is true.

....

To prove that p if and only if q

(→) Suppose p is true.

....

q is also true. Hence, p implies q.

(←) Suppose p is false.

....

Proposition 44. x is odd if and only if x is <u>not</u> even.

Proof. Since this an "if and only if" statement, we need to prove two things:

(⇒) If x is odd, then x is not even.

(⇐) If x is not even, then x is odd.

Proof of (⇒). Suppose x is odd. Assume that x is also even. Then, by **Definition 1** and **Definition 2**, there are some a and b such that

$$\begin{aligned} x &= 2a \\ x &= 2b + 1 \end{aligned}$$

Subtracting these two equations, we obtain

$$\begin{aligned} 0 &= 2a - 2b - 1 \\ &= 2(a - b) - 1 \end{aligned}$$

This implies that $2(a - b) = 1$ and thus $(a - b) = \frac{1}{2}$. Since a and b are integers, $(a - b)$ must also be an integer. But since $\frac{1}{2}$ is <u>not</u> an integer, we have a contradiction. Therefore, x cannot be even.

Proof of (⇐). Suppose x is not even. The remainder of x divided by 2 is either 0 or 1. Since x is not even, the remainder of x divided by 2 must be 1. Therefore, $x = 2m + 1$. By the definition of odd integers, it follows that x is odd.

■

To prove that some given statements

- p1
- p2
- …
- pn

are all equivalent, you only need to prove that

- p1 implies p2
- p2 implies p3
- …
- pn implies p1

Proof) P_1, P_2, P_3, P_4 are equivalent

$P_1 \Leftrightarrow P_2$

$P_2 \Leftrightarrow P_3$

$P_3 \Leftrightarrow P_4$

$P_1 \Leftrightarrow P_3$

$P_2 \Leftrightarrow P_4$

$P_1 \Leftrightarrow P_4$

$P_1 \to P_2 \left< \begin{matrix} P_1 \to P_2 \\ P_2 \to P_1 \end{matrix} \right.$

easier method

$P_1 \to P_2$

$P_{12} \to P_3$

$P_3 \to P_4$

$P_4 \to P_1$

$$\exists!\, x\ P(x) \equiv \underbrace{\left[\exists_x P(x)\right]}_{\text{Existence}} \wedge \underbrace{\left[\forall x\, \forall_y\ P(x) \wedge P(y) \rightarrow x = y\right]}_{\text{Uniqueness}}$$

10. Proving unique existence

To prove that there exists a unique element in some set S satisfying a given property P, we need to show two things:

- at least 1 **Existence**: Show that there is an element, say c, in S satisfying property P.
- at most 1 **Uniqueness**: Show that all the elements in S satisfying P must be equal.

Proposition 45. There exists a unique real number x such that $2x - 1 = 0$.

Proof.

[Existence] It is easily seen that $x = 0.5$ satisfies the equation $2x - 1 = 0$.

[Uniqueness] Suppose real numbers a and b both satisfy the equation. Thus,

$$2a - 1 = 0 \ \text{-①}$$

$$2b - 1 = 0 \ \text{-②}$$

มีแค่ตัวเดียว

กำหนดให้ ① ② เป็น 2 ตัวแปล

Proof ว่า a=b, ∴ ①=②

This implies that

$$2a - 1 = 2b - 1$$

$$2a = 2b$$

$$a = b$$

Hence, all solutions to equation $2x - 1 = 0$ are equal.

Therefore, $x = 0.5$ is the unique real number such that $2x - 1 = 0$.

■

10. Proving that an element is a member of a set

Suppose a set S is defined to contain all elements having a property P. To show that an element c is in S, you only need to show that c has property P.

Suppose $S = \{x|P(x)\}$.

To show that $c \in S$,
we show that $P(c)$ is true.

Suppose $S = \{x \in U|P(x)\}$.

To show that $c \in S$, we show that c is in U and $P(c)$ is

Proposition 46. There is a prime number in the set $S = \{x \in Z \mid x \bmod 7 = 4\}$.

Proof. The set S consists of all integers x where $x \bmod 7 = 4$. Clearly, $11 \in S$ because $11 \bmod 7 = 4$. Since 11 is a prime number, this proposition is true.

■

$S = \{x \in Z \mid x \bmod 7 = 4\}$

$11 \in S\ ? \begin{cases} 11 \in Z \ \checkmark \ (Z = \text{interger}) \\ 11 \bmod 7 = 4 \ \checkmark \end{cases}$

$\therefore \ 11 \in S$ #

$A \subseteq B$ iff $\forall x\,(x \in A \to x \in B)$

11. Proving that one set is a subset of another.

To prove that $A \subseteq B$, we show that every member of A is also in B.

Suppose x is a member of A.

…

x is also a member of B.

Hence, $A \subseteq B$.

$S \subseteq T$

Ass $x \in S$

$\vdots$

$x \in T$

Proposition 47. $\{x \in Z \mid 12|x\} \subseteq \{x \in Z \mid 3|x\}$.

Proof. Let S and T denote the following sets:

$$\begin{aligned} S &= \{x \in Z \mid \underbrace{12|x}\}^{\text{all interger divisible by 12}} && \frac{x}{12} = y \;;\; x = 12y \Rightarrow x = 3(4y) \\ T &= \{x \in Z \mid \underbrace{3|x}_{\text{all interger divisible by 3}}\} && \frac{x}{3} = y \;;\; x = 3y \Rightarrow x = 3y \end{aligned}$$

Suppose $x \in S$. Hence, $12|x$, which means that, for some integer y,

$$x = 12y$$

$$x = 3(4y)$$

This implies that $3|x$ and thus $x \in T$.

Therefore, $S \subseteq T$.

■

$A = B$ iff $(A \subseteq B) \wedge (B \subseteq A)$

12. Proving that two sets are equal.

To prove that $A = B$, we show that $A \subseteq B$ and $B \subseteq A$.

$[A \subseteq B]$ Suppose x is a member of A.
…
x is also a member of B.
Hence, $A \subseteq B$.
$[B \subseteq A]$ Suppose x is a member of B.
…
x is also a member of A.
Hence, $B \subseteq A$.

Therefore, $A = B$.

Proposition 48. $\{x \in Z \mid \overbrace{12|x\}}^{A} = \{x \in Z \mid \overbrace{3|x\}}^{B} \cap \{x \in Z \mid \overbrace{4|x\}}^{C}$.

$A = B \cap C$

$x \in B \cap C$ iff $x \in B$ and $x \in C$

Proof. Let A, B, C denote the following sets:

$$A = \{x \in Z \mid 12|x\} \quad x = 12a$$
$$B = \{x \in Z \mid 3|x\} \quad x = 3b$$
$$C = \{x \in Z \mid 4|x\} \quad x = 4c$$

[$A \subseteq B \cap C$] Suppose $x \in A$. Hence, $12|x$, which means that, for some integer y,

$$x = 12y = 3(4y) = 4(3y).$$

This implies that $3|x$ and $4|x$. So $x \in B$ and $x \in C$, and hence $x \in B \cap C$. Therefore, $A \subseteq B \cap C$.

[$B \cap C \subseteq A$] Suppose $x \in B \cap C$. Hence, $x \in B$ and $x \in C$, which imply that $3|x$ and $4|x$.

Therefore, for some integers y and z,

$$x = 3y \tag{1}$$
$$x = 4z \tag{2}$$

From these two equations, it follows that $3|4z$. By Euclid's Lemma, either $3|4$ or $3|z$. Clearly, $3 \nmid 4$. Hence, it must be that $3|z$, which means that $z = 3w$, for some integer w. Substituting this into equation (2), we obtain

$$x = 4(3w) = 12w.$$

This means that $12|x$ and hence $x \in A$. Therefore, $B \cap C \subseteq A$.

$3|4z$ Since 3 is prime, by Euclid's Lemma

$3 \nmid 4$

■

???

13. Proving that two sets have the same cardinality (size).

Suppose we want to prove that two given sets A and B have the same cardinality (i.e. same number of elements).

If both sets are finite, one direct method is to fine the number of elements of A and the number of elements of B and show that both numbers are equal.

Another method, which is also applicable when both sets are infinite, is to find a bijection between the two sets.

Definition 49. Suppose x and y are any real numbers. Define the following sets of real numbers:

- $(x, y) = \{z \in R \mid x < z < y\}$
- $[x, y) = \{z \in R \mid x \leq z < y\}$
- $(x, y] = \{z \in R \mid x < z \leq y\}$
- $[x, y] = \{z \in R \mid x \leq z \leq y\}$

Proposition 50. The sets $[-1,2]$ and $[0,1]$ have the same cardinality.

Proof. We shall define a bijection f from $[-1,2]$ to $[0,1]$. In particular, define

$$f(x) = (x+1)/3$$

for all $x \in [-1,2]$.

It can be shown that f is a bijection from $[-1,2]$ to $[0,1]$, i.e. f is one-one and onto.

[One-one] Suppose $f(x) = f(y)$. Then

injection

$$(x+1)/3 = (y+1)/3$$
$$x+1 = y+1$$
$$x = y$$

Hence, $f(x) = f(y)$ implies $x = y$, for any real numbers x and y. Therefore, f is one-one.

$x = 3y - 1$

[Onto] For any number y in $[0,1]$, let x be $3y - 1$. It is clear that $x \in [-1,2]$ because

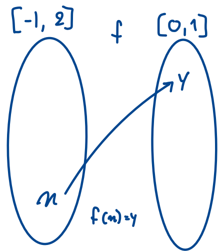
Surjection

$$0 \leq y \leq 1$$
$$0 \leq 3y \leq 3$$
$$-1 \leq 3y - 1 \leq 2$$
$$-1 \leqslant x \leqslant 2$$

$f(x) = \frac{x+1}{3}$

$f(x) = f(3y-1) = \frac{(3y-1)+1}{3} = y$

$f(x) = y$



$$-1 \leq x \leq 2$$

It is also easy to show that $f(x) = y$:

$$f(x) = f(3y - 1) = ((3y - 1) + 1)/3 = 3y/3 = y.$$

Therefore, for any number y in $[0,1]$, there is some number x in $[-1,2]$, such that $f(x) = y$. Hence, f maps $[-1,2]$ *onto* $[0,1]$.

■