# Intro to Proofs: A Supplement

Viktor Blåsjö




## § 0. Introduction

The following notes have been written as a supplement to an "intro to proofs" course. Such courses can be very dry and focussed solely on the mechanics and minutia of proof writing, with little regard for *why* anyone would want to learn these things. They also often focus on monotonous, lifeless problems concocted for the sole purpose of rote practice. My goal in these notes have been to try to bring more motivation and purpose to such a course, by trying to convey a sense of the ideas more as they occur "in the wild" in varied and colourful forms. To this end I have tried to collect a series of intrinsically interesting problems that parallel the usual topics of such a course and do not assume any substantive prerequisite knowledge. I believe it will be more fun and educational to learn the respective techniques if one also sees some fascinating and powerful applications of them. For each topic I have also included a minimalistic "reference summary" of the material in question.

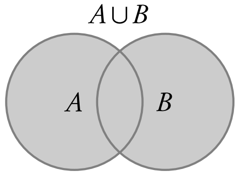
0.1. Discussion question for first day of class: What does the visually striking Figure 4 of the paper `http://dx.doi.org/10.1090/noti1263` tell us about the need for a course like this?

## § 1. Set theory

### § 1.1. *Reference summary*

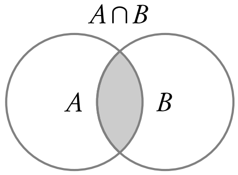
| | |
|---|---|
| $\cup$ | union (aggregate, "everything combined") |

$A \cup B$



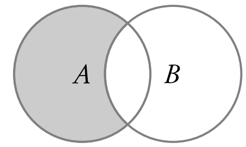

| | |
|---|---|
| $\cap$ | intersection (what is common to both) |

$A \cap B$




| | |
|---|---|
| $\setminus$ or $-$ | "set minus"; difference |
| $A \setminus B$ or $A - B$ | $A$ with everything from $B$ taken out |

$A - B$




| | |
|---|---|
| $\in$ | is an element of |
| $A \subset B$ | $A$ is contained in $B$, is a subset of $B$ |
| $A \subseteq B$ | $A$ is contained in $B$, and is possibly equal to it |
| $\overline{A}$ | complement of $A$; everything but $A$ |
| $\mathbb{N}$ | the natural numbers $(1, 2, 3, \ldots)$ |
| $\mathbb{Z}$ | the whole numbers, the integers $(\ldots, -2, -1, 0, 1, 2, 3, \ldots)$ |
| $\mathbb{Q}$ | the rational numbers; numbers that are the ratio of two integers |
| $\mathbb{R}$ | the real numbers; a "whole axis" |
| $\mathbb{C}$ | the complex numbers |
| $\emptyset$ or $\varnothing$ | the empty set; nothing |

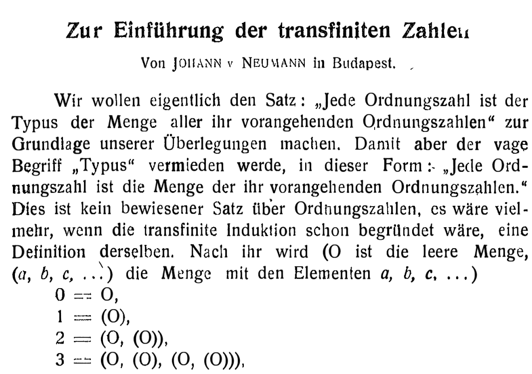
$$\underbrace{A}_{\text{set}} = \{ \underbrace{n \in \mathbb{Z}}_{\text{type of objects}} : \underbrace{n^2 < 5}_{\text{conditions}} \}$$
$$= \text{"the set of all integers whose square is less than 5"}$$
$$= \{-2, -1, 0, 1, 2\}$$

$$\varnothing \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

$$2 \in \mathbb{Z} \quad \tfrac{3}{2} \in \mathbb{Q} \quad \pi \in \mathbb{R} \quad \pi \notin \mathbb{Q}$$

### § 1.2. *Problems*

1.1. Sets have proven to be the mathematician's favourite language for expressing almost everything. Modern mathematicians even prefer to define numbers themselves in terms of sets. Here's an excerpt of a paper from 1923 where this is done:



**Zur Einführung der transfiniten Zahlen**

Von Johann v. Neumann in Budapest.

Wir wollen eigentlich den Satz: „Jede Ordnungszahl ist der Typus der Menge aller ihr vorangehenden Ordnungszahlen" zur Grundlage unserer Überlegungen machen. Damit aber der vage Begriff „Typus" vermieden werde, in dieser Form: „Jede Ordnungszahl ist die Menge der ihr vorangehenden Ordnungszahlen." Dies ist kein bewiesener Satz über Ordnungszahlen, es wäre vielmehr, wenn die transfinite Induktion schon begründet wäre, eine Definition derselben. Nach ihr wird (O ist die leere Menge, $(a, b, c, \ldots)$ die Menge mit den Elementen $a, b, c, \ldots$)

0 = O,
1 = (O),
2 = (O, (O)),
3 = (O, (O), (O, (O))),

(a) Von Neumann uses antiquated notation. Re-express his formulas in modern terms.

(b) Do $\cup, \cap, \subset, \in$ have arithmetical meaning in this context?

## § 2. Symbolic logic

### § 2.1. *Reference summary*

| | |
|---|---|
| $\wedge$ | and |
| $\vee$ | or |
| $\Longrightarrow$ | implies ("if … then …") |
| $\Longleftrightarrow$ | if and only if |
| $\sim$ or $\neg$ | not |
| $\forall$ | for all |
| $\exists$ | there exists |

Truth table:

| $P$ | $Q$ | $\sim P$ | $P \wedge Q$ | $P \vee Q$ | $P \Longrightarrow Q$ | $P \Longleftrightarrow Q$ |
|---|---|---|---|---|---|---|
| T | T | F | T | T | T | T |
| T | F | F | F | T | F | F |
| F | T | T | F | T | T | F |
| F | F | T | F | F | T | T |

Examples: If $P(n)$ is the statement "$n$ is a prime number" then:

| | |
|---|---|
| $P(2) \wedge P(3)$ | T |
| $P(2) \vee P(3)$ | T |
| $P(2) \wedge P(8)$ | F |
| $P(2) \wedge \sim P(8)$ | T |
| $P(7) \Longrightarrow P(3)$ | T |

| | $\forall x \in \mathbb{R}$ | $\exists x \in \mathbb{R}$ |
|---|---|---|
| $x^2 \geq 0$ | T | T |
| $x^2 = 2$ | F | T |
| $x^2 < 0$ | F | F |

$$8 \text{ is even} \Longleftrightarrow 8 \text{ is divisible by } 2$$

### § 2.2. *Problems*

2.1. The truth table for $P \Longrightarrow Q$ is somewhat counter-intuitive. For example, these statements are both true:

(a) If the moon is made of cheese, then I am the King of France.

(b) If the moon is made of cheese, then $1+1=2$.

Perhaps you think does not capture the real meaning of an "if … then …" statement. However, consider what happens if we change one or both of the corresponding entries in the truth table for $P \Longrightarrow Q$. Argue that that would get us even further from the intuitive meaning of an "if … then …" statement.

2.2. Prove that "everything follows from a contradiction" (i.e., from the assumptions $P$ and $\sim P$ one can deduce any proposition $Q$).

2.3. What is the truth value of the statement "if $1 = 0$, then I am the Pope"?

It is said that when Bertrand Russell taught logic his students found this to be abstract gibberish and asked for a direct proof, to which Russell replied: "Add 1 to both sides of the equation: then we have $2 = 1$. The set containing just me and the Pope has 2 members. But $2 = 1$, so it has only 1 member. Therefore, I am the Pope."

2.4. Leibniz envisioned in the 17th century that symbolic logic might become something like an "algebra of thought": a systematic way or reasoning that would produce conclusions by the manipulation of symbols just as automatically as one solves an equation for $x$. As he put it: "If someone should doubt my results, I should say to him: 'Let us calculate, Sir,' and thus by taking to pen and ink, we should settle the question." Leibniz's dream did not pan out the way he had hoped. Nevertheless it was not entirely off the mark. For example, consider this complicated logical information:

If either Jones witnessed the collision
or Smith was wearing his spectacles when he saw the collision
then if Coe was the driver of the stolen truck
then if the third witness was not intimidated
then the judge was bribed.

If the third witness was not intimidated
then Coe was the driver of the stolen truck.

The judge was not bribed.

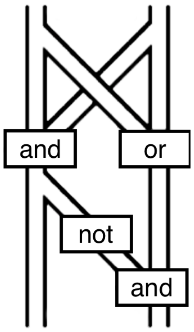
The third witness was not intimidated.

---

Was Smith wearing his spectacles when he saw the collision?

It is not very easy to answer this question using only verbal reasoning. Show, however, that by translating it into logical symbolism it becomes clear how to solve it in an easy and systematic fashion.

2.5. Computer circuitry is in a sense built on logical relations. Think of true and false as an electrical current being on or off. The simplest ultimate building blocks of computer circuitry are gates that take two incoming currents (that can be either on or off) and decides whether the outgoing current should be on or off, just as a logical operator takes two statements and decides whether compound statement is true or false. To get a computer to do mathematics we interpret on and off as 1 and 0. The following schema shows how one can do arithmetic this way:




(a) For each possible input (entering at the top of the diagram), follow the gates and determine the output.

| input | output |
|---|---|
| 0 0 | |
| 0 1 | |
| 1 0 | |
| 1 1 | |

(b) Which arithmetical operation is this? (Binary arithmetic has a base of 2. Thus for example 101 means $1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0 = 5$ rather than $1 \times 10^2 + 0 \times 10^1 + 1 \times 10^0$ as it would mean in base 10.)

## § 3. Proof techniques

### § *3.1. Reference summary*

- *Contradiction.* To prove $P$, assume $\sim P$ and derive a contradiction. Useful when $\sim P$ is more concrete or simpler or easier to express in algebraic form.
- *Contrapositive.* To prove $P \implies Q$, prove instead the logically equivalent statement $\sim Q \implies \sim P$. Useful when $\sim Q$ is more concrete etc. than $P$.
- *Enumeration of cases.* "It has to be either … or … or …." Prove the theorem in each case one by one.

### § *3.2. Problems*

3.1. Prove by contradiction and explain why this method is well suited to the task:

(a) $\sqrt{2}$ is irrational.

(b) There are infinitely many primes. (Hint: Suppose not. Then there is a complete list of all primes: $p_1, p_2, p_3, \ldots, p_n$. Let $\Pi = p_1 p_2 p_3 \cdots p_n$ be the product of all of them. What can you say about $\Pi + 1$?)

3.2. Argue that the equivalence of $P \implies Q$ and the contrapositive $\sim Q \implies \sim P$ is intuitively clear if you think of an example such as $P =$ "I'm at the party" and $Q =$ "my friend is at the party."

3.3. Some theorems are much easier to prove using the contrapositive than directly. Example: If $n$ is a prime $> 3$, then $n+1$ is not a square.

(a) Make a list of prime numbers $> 3$, and a list of square numbers. What does the theorem say about the relation of these two lists? It is obvious that this relation holds?

(b) Prove the theorem using the contrapositive.

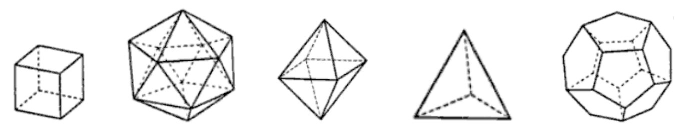
3.4. Argue that the contrapositive is convenient to explain why, for a differentiable function $f(x)$,

$$f(a) \text{ is a maximum or minimum} \implies f'(a) = 0$$

3.5. Prove by enumeration of cases and explain why this method is well suited to the task:

(a) The remainder of a square number when divided by 4 is 0 or 1.

(b) There are precisely five regular polyhedra (three-dimensional figures made up of regular polygons, and all of whose sides and corners are alike).

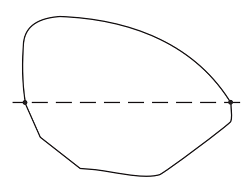


Cube Icosahedron Octahedron Tetrahedron Dodecahedron

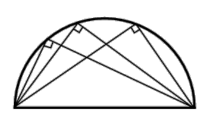
3.6. Among all figures with a given perimeter, the circle has the greatest area. Here is a way of proving this by contradiction.

Take a figure with maximal area for its perimeter. Cut its perimeter in half with a line.

(a) Argue by contradiction that this line will split the area in half as well.

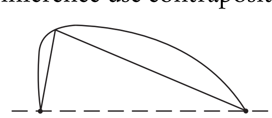


Consider one of these halves. Thales' Theorem says that in a semicircle these are all right angles:

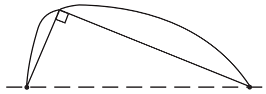


Suppose the half we are looking at is not a semicircle. Then by Thales' Theorem there will be some point on the boundary where lines drawn from the points on the symmetry line meet at an angle which is not right.

(b) Does this inference use contrapositive reasoning?



Think of there as being a void inside the triangle and think of the pieces on the sides as glued on. Slide the endpoints along the symmetry line to make the angle right.



(c) Conclude the proof.

3.7. Here's an issue with the logic of the preceding problem. From the fact that any non-circle is not the optimal figure, can we infer that the circle is? Illustrate a problem with such an inference by "proving" that 1 is the largest natural number using such logic (e.g., by considering the effect of $f(x) = x^2$ on all other natural numbers).

3.8. Below is a proof by contradiction. Illustrate each step with figures, and judge whether the proof is valid.

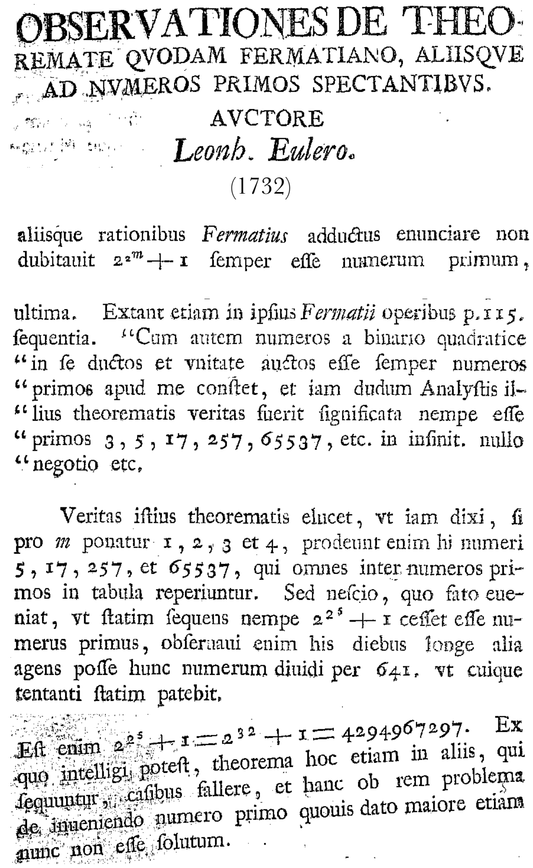
Theorem. Any continuous mapping of a disc onto itself has a fixed point.

Proof. Suppose it did not. Then any point in the circle can be connected with its image by an arrow. Now consider a point on the boundary. The arrow direction varies continuously as we walk once around the circle, and it end up where it started so it must have made an integer number of revolutions. But there is also a tangent at each point, and the tangent of course make one revolution as we walk once around. The arrows always point to some point in the disc so they could never point in a direction parallel to the tangent so the arrows in fact have to make one revolution also (they would have to be parallel to the tangent for a moment to overtake it, and if they stood still they would be parallel to the tangent at "six o'clock" so to speak). But if we consider the same situation for a concentric circle inside the disc then it too must have arrows making one revolution because the number of revolutions can not make jumps since the new circle is obtained by continuous shrinking of the circumference circle. But as we shrink this circle to infinitesimal radius then all its arrows point in the same direction, so they don't make one revolution, so we have a contradiction.

## § 4. Disproof

### § 4.1. Problems

4.1. To prove that a theorem is not true, it is enough to find a single counterexample. For instance, Fermat claimed that $2^{2^m} + 1$ is prime for all positive integers $m$. Euler proved him wrong by counterexample. Do the same. Hint:



OBSERVATIONES DE THEOREMATE QVODAM FERMATIANO, ALIISQVE AD NVMEROS PRIMOS SPECTANTIBVS.

AVCTORE

*Leonh. Eulero.*

(1732)

aliisque rationibus *Fermatius* adductus enunciare non dubitauit $2^{2^m}+1$ ſemper eſſe numerum primum,

ultima. Extant etiam in ipſius *Fermatii* operibus p. 115. ſequentia. "Cum autem numeros a binario quadratice "in ſe ductos et vnitate auctos eſſe ſemper numeros "primos apud me conſtet, et iam dudum Analyſtis il- "lius theorematis veritas fuerit ſignificata nempe eſſe "primos 3, 5, 17, 257, 65537, etc. in infinit. nullo "negotio etc.

Veritas iſtius theorematis elucet, vt iam dixi, ſi pro $m$ ponatur 1, 2, 3 et 4, prodeunt enim hi numeri 5, 17, 257, et 65537, qui omnes inter numeros primos in tabula reperiuntur. Sed neſcio, quo fato eueniat, vt ſtatim ſequens nempe $2^{2^5}+1$ ceſſet eſſe numerus primus, obſeruaui enim his diebus longe alia agens poſſe hunc numerum diuidi per 641, vt cuique tentanti ſtatim patebit.

Eſt enim $2^{2^5}+1 = 2^{32}+1 = 4294967297$. Ex quo intelligi poteſt, theorema hoc etiam in aliis, qui ſequuntur, caſibus fallere, et hanc ob rem problema de inueniendo numero primo quouis dato maiore etiam nunc non eſſe ſolutum.

4.2. Prove or disprove: $n^2 + n + 41$ is prime for all positive integers $n$. Hint (from *Mathematica*):

```
PrimeQ[Table[n^2 + n + 41, {n, 1, 30}]]
{True, True, True, True, True, True, True, True, True,
 True, True, True, True, True, True, True, True, True, True,
 True, True, True, True, True, True, True, True, True, True, True}
```

## § 5. Induction

### § 5.1. Reference summary

To prove $P(n)$ for all $n$, prove:

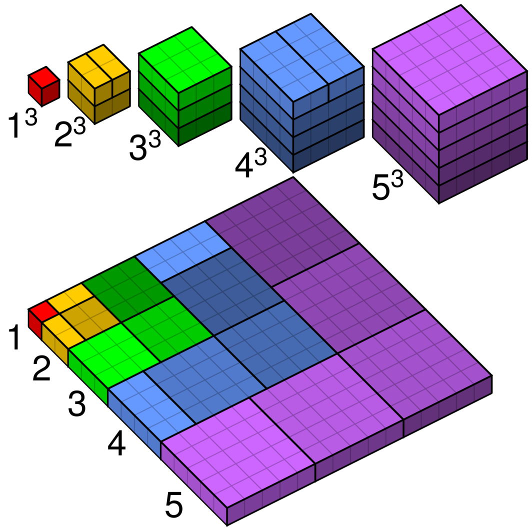
- $P(1)$
- $P(k) \implies P(k+1)$

Or in "strong" form:

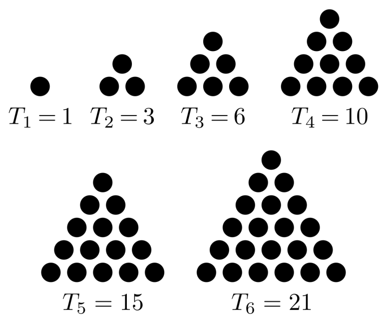
- $P(1)$
- $P(1) \wedge P(2) \wedge \cdots \wedge P(k) \implies P(k+1)$

### § 5.2. Problems

5.1. Find and prove the formula for the sum of squares $1^3 + 2^3 + 3^3 + \cdots + n^3$ suggested by this figure:




5.2. These are the first six “triangular numbers”:




(a) Argue visually that the $n$th triangular number is $1+2+3+4+\cdots+n$.

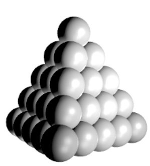
(b) Find a short algebraic expression for the $n$th triangular number. Prove by induction that your formula is correct.

Use your formula to prove:

(c) The sum of two consecutive triangular numbers is a square number.

(d) If a triangular number is multiplied by 8, and 1 is added, then the result is a square number.

“Tetrahedral numbers” can be arranged in a tetrahedral shape (i.e, by stacking triangular numbers):

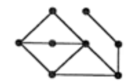


(e) Find a short algebraic expression for the $n$th tetrahedral number. Prove by induction that your formula is correct.

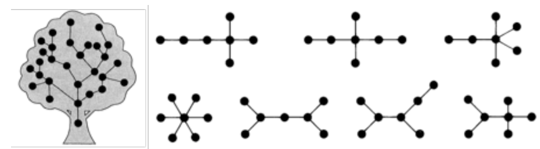
5.3. Consider a simplified “map” consisting of lines drawn in a plane. Prove by induction on the number of lines that any such map can be coloured using only two colours. Two bordering “countries” are not allowed to have the same colour.

Hint for the induction step: invert the colours on one side, leave them the same on the other.

5.4. A graph consists of vertices $V$ (dots) connected by edges $E$ (line segments). For example, this graph has 8 vertices and 10 edges:

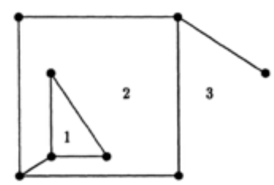


A tree is a graph with no closed paths (there is only one path between any two vertices). Examples of trees:



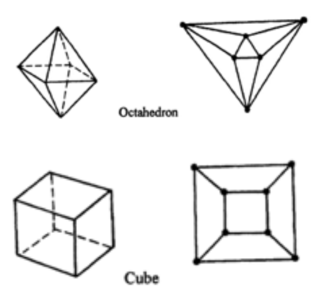
(a) Prove by induction on the number of vertices that $V - E = 1$ for any tree.

A graph is “plane” if its edges do not cross. If a plane graph is not a tree then it separates the plane into several faces $F$ (separated regions). A tree has only one face. This plane graph has 3 faces, as labelled:



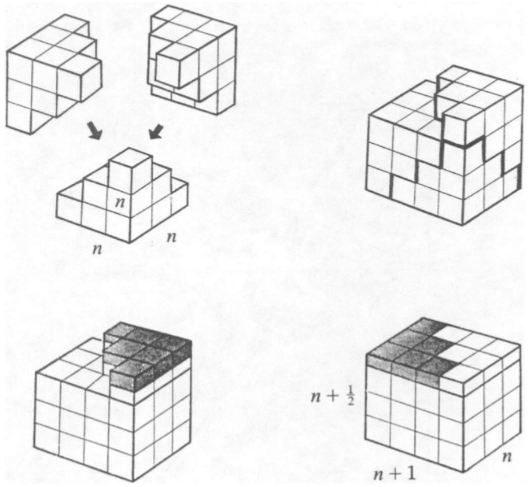

(b) Prove by induction on the number of closed paths that $V - E + F = 2$ for any plane graph.

(c) The formula $V - E + F = 2$ is more famous as a theorem about three-dimensional polyhedra. Explain how this theorem corresponds to the theorem for graphs. Hints:

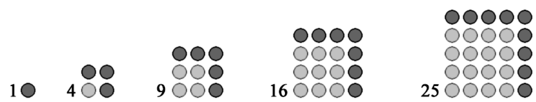



5.5. Example of strong induction: The “Tribonacci sequence” $T_n$ is defined by $T_1 = T_2 = T_3 = 1$ and $T_n = T_{n-1} + T_{n-2} + T_{n-3}$ when $n \geq 4$. Prove that $T_n < 2^n$ for all $n \in \mathbb{N}$.

5.6. Find and prove the formula for the sum of squares $1^2 + 2^2 + 3^2 + \cdots + n^2$ suggested by this figure (from Man-Keung Siu, Proof without Words: Sum of Squares, *Mathematics Magazine*, 57(2), 1984, p. 92):




5.7. Find and prove a formula for the relation between odd numbers and squares suggested by this figure:




5.8. Prove that the Towers of Hanoi puzzle with $n$ discs and 3 pegs can be solved in $2^n - 1$ moves.

5.9. In a certain kind of tournament, every player plays every other player exactly once and wither wins or loses. Define a *top* player to be a player who, for every other player $x$, either beat $x$ or beat a player who beat $x$. Prove that any tournament of $n$ players has at least one top player.

5.10. Explain what is wrong with the following reasoning.

Theorem. All horses have the same colour.

Proof. Let $P(n)$ be the statement: "In every set of $n$ horses, all the horses have the same colour." $P(1)$ is obviously true. Suppose $P(n)$ is true. Consider any set of $n+1$ horses. Take an element of the set, $a$. The $n$ horses other than $a$ form a set of $n$ horses, so they are all the same colour (since $P(n)$ is true). Now take a set of $n$ horses out of the $n+1$ which does include $a$. These are also all the same colour, so $a$ is the same colour as the rest. Therefore $P(n+1)$ is true. Hence, by induction, the theorem holds.

5.11. In the induction step of a proof by mathematical induction, one assumes $P(n)$. But $P(n)$ is precisely the theorem one is trying to prove in the first place. How can this be?

# § 6. Modulo arithmetic

## § *6.1. Reference summary*

In "modulo $n$" arithmetic we ignore multiples of $n$. For example, $5 \equiv 2 \mod 3$ ("5 is congruent to 2 modulo 3") since 5 and 2 differ by a multiple of 3. Similarly, $13 \equiv 3 \mod 5$.

$$n \equiv 0 \mod 2 \iff n \text{ is even}$$

$$a \equiv b \mod n \iff n \mid (a-b) \iff a-b = mn$$

Modulo arithmetic lumps together all equivalent integers into a few equivalence classes. For example, modulo 3 there are only 3 significantly distinct entities:

$$[0] = \{\ldots,-9,-6,-3,0,3,6,9,\ldots\}$$
$$[1] = \{\ldots,-8,-5,-2,1,4,7,10,\ldots\}$$
$$[2] = \{\ldots,-7,-4,-1,2,5,8,11,\ldots\}$$

Calculation rules:

$$[a]+[b] = [a+b] \quad \text{and} \quad [a]\cdot[b] = [ab]$$

Example modulo 3: $[61]\cdot[3005] = ([60]+[1])([3000]+[5]) = ([0]+[1])([0]+[2]) = [2]$, so $61 \cdot 3005 \equiv 2 \mod 3$.

## § *6.2. Problems*

6.1. (a) A number is divisible by 3 if the sum of its digits is divisible by 3. Prove this using modulo arithmetic.

(b) Find and prove a similar result for divisibility by 9.

(c) Find and prove a similar result for divisibility by 11.

6.2. Books published between 1985 and 2005 were assigned an International Standard Book Number (ISBN) consisting of ten digits: $a_1, a_2, a_3, \ldots, a_{10}$. The first nine digits identified the book uniquely, while the last digit $a_{10}$ was included for verification purposes. This last digit was chosen so that

$$10a_1 + 9a_2 + \cdots + 2a_9 + a_{10} \equiv 0 \mod 11$$

(a) Find some books and confirm the above equation in those cases.

The control digit was included to safeguard against typing errors. Prove or disprove:

(b) For any ISBN, if one digit is changed, the above equation will no longer hold.

(c) For any ISBN, if two digits are changed, the above equation will no longer hold.

(d) For any ISBN, if two distinct, adjacent digits swap places, the above equation will no longer hold.

(e) For any ISBN, if two distinct digits swap places, the above equation will no longer hold.

6.3. Start with any number whose digits are in increasing order. Multiply it by 9. Add the digits. What did you get? Prove that this always happens.

6.4. McNuggets can be bought and sold in quantities of 6, 9, or 20. Is it possible to conduct transactions so as to end up with a single McNugget?

# § 7. Number theory

## § 7.1. *Reference summary*

The deductive structure of the foundations of classical number theory can be outlined as follows:

Euclidean subtraction algorithm: Given a pair of integers, form a new pair consisting of: (larger number − smaller number) and (smaller number). Repeat until the process halts.

or Euclidean division algorithm: Given a pair of integers, form a new pair consisting of: (remainder when larger number is divided by smaller number) and (smaller number). Repeat until the process halts.

$\Longrightarrow$ Euclidean algorithm theorem: The resulting number is the greatest common divisor of the original pair.

$\Longrightarrow$ Euclidean algorithm corollary: The greatest common devisor of two integers is a linear combination of them.

$\Longrightarrow$ Prime divisor property: $p \mid ab \implies p \mid a$ or $p \mid b$.

$\Longrightarrow$ Unique prime factorisation.

## § 7.2. *Problems*

7.1. Consider the "Gaussian integers" $\{a+bi : a,b \in \mathbb{Z}\}$. Their number theory is very much analogous to that of ordinary integers, with only minor adaptations. For example, in the integer case one ignores factors $1,-1$, while in the Gaussian case one ignores the "unit" factors $1,-1,i,-i$. The role of smaller and larger numbers in the ordinary case is taken over by smaller or larger in terms of absolute value in the Gaussian case.

(a) Show that 2 is not a Gaussian prime.

(b) Find an odd prime that is also a Gaussian prime.

(c) Find an odd prime that is not a Gaussian prime.

Is prime factorisation unique in the Gaussian case? As §7.1 suggests, to prove this it is in effect enough to prove that Gaussian integers have a division algorithm, and the rest will follow as in ordinary number theory.

(d) Prove that Gaussian integers have a division algorithm, i.e., that for any given Gaussian integers $z,w$, one can find Gaussian integers $\alpha,\beta$ such that $z = \alpha w + \beta$, where $|\beta| < |w|$.

Hint: Think of the geometry of complex numbers and visualise the set of all Gaussian-integer multiples of $w$.

(e) Formulate and sketch a proof of the unique factorisation property for Gaussian integers.

7.2. Show that prime factorisation is not unique in the "integers" $\{a + b\sqrt{-5} : a,b \in \mathbb{Z}\}$.

7.3. Which numbers equal the sum of their factors? Very few numbers are "perfect" enough to have this pleasant property, as Nicomachus explains:

> When a number, comparing with itself the sum and combination of all the factors whose presence it will admit, it neither exceeds them in multitude nor is exceeded by them, then such a number is properly said to be perfect, as one which is equal to its own parts. Such numbers are 6 and 28; for 6 has the factors 3, 2, and 1, and these added together make 6 and are equal to the original number, and neither more nor less. 28 has the factors 14, 7, 4, 2, and 1; these added together make 28, and so neither are the parts greater than the whole nor the whole greater than the parts, but their comparison is in equality, which is the peculiar quality of the perfect number.
>
> It comes about that even as fair and excellent things are few and easily enumerated, while ugly and evil ones are widespread, so also are the superabundant and deficient numbers found in great multitude and irregularly placed, but the perfect numbers are easily enumerated and arranged with suitable order; for only one is found among the units, 6, only one among the tens, 28, and a third in the ranks of the hundreds, $\boxed{\phantom{000}}$, and a fourth within the limits of the thousands, 8128.

Euclid proved that if $p$ is a prime and $2^p-1$ is also prime then $2^{p-1}(2^p-1)$ is perfect. This is the grand finale of Euclid's number theory (*Elements* IX.36). The theorem amounts to a recipe for finding perfect numbers: in a column list the prime numbers; in a second column the values $2^p-1$; cross out all rows in which the second column is not a prime number; for the remaining rows, place $2^{p-1}(2^p-1)$ in the third column. Then the numbers in the third column are perfect numbers.

(a) Find the perfect number omitted in the Nicomachus quote above using Euclid's recipe. What prime $p$ did you need to use?

The following is essentially Euclid's proof of the theorem. If $2^p-1$ is prime, it is clear that the proper divisors of $2^{p-1}(2^p-1)$ are $1,2,2^2,\dots,2^{p-1}$ and $(2^p-1),2(2^p-1),2^2(2^p-1),\dots,2^{p-2}(2^p-1)$. So these are the numbers we need to add up to see if their sum equals the number itself.

(b) Show that $1+2+2^2+\ldots+2^{p-1} = 2^p-1$ by adding 1 at the very left and gradually simplify the series from that end.

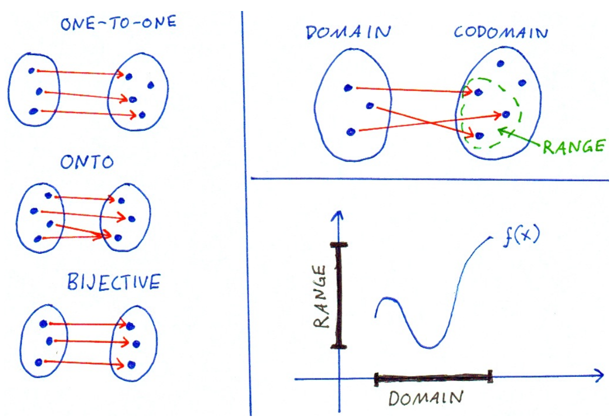
(c) Use a similar trick for the remaining sum, and thus conclude the proof.

# § 8. Functions

## § 8.1. *Reference summary*

A function $f$ from $A$ to $B$, written $f : A \to B$, assigns a unique "output" or "image" $b \in B$ to each "input" $a \in A$.

| concept | symbolically | verbally |
|---|---|---|
| domain | $A$ | Set of all possible inputs. |
| range | $\{f(x) : x \in A\} \subseteq B$ | Set of all possible outputs. |
| one-to-one (injective) | $x \neq y \implies f(x) \neq f(y)$, or equivalently: $f(x) = f(y) \implies x = y$ | No element in $B$ is hit more than once. (Unique "preimage" for each $b$ in range.) |
| onto (surjective) | $b \in B \implies \exists a \in A$ such that $f(a) = b$ | Every element in $B$ is hit at least once. |
| bijective | | one-to-one and onto |
| inverse $f^{-1}$ | $f^{-1}(f(a)) = a$ for all $a \in A$ | $f^{-1}$ "undoes" $f$ |
| composition $g \circ f$ | $(g \circ f)(a) = g(f(a))$ | "first do $f$ then do $g$ to the result" |




## § 8.2. *Problems*

8.1. What can you say about $f^{-1}$ if you know that $f : A \to B$ is

(a) 1-to-1?

(b) onto?

(c) bijective?

8.2. Fill in the blanks to complete the following proof outlines.

(a) Theorem. $f : \boxed{\phantom{xx}} \to \boxed{\phantom{xx}}$ is a $\boxed{\phantom{xx}}$ function.

Proof. Suppose $f(x_1) = f(x_2)$. Then $[\ldots]$, so $x_1 = x_2$.

(b) Theorem. $f : \boxed{\phantom{xx}} \to \boxed{\phantom{xx}}$ is a $\boxed{\phantom{xx}}$ function.

Proof. Let $y \in \boxed{\phantom{xx}}$. Then $f(\boxed{\phantom{xx}}) = [\ldots] = y$. So $y \in \boxed{\phantom{xx}}$.

# § 9. Cardinality

## § 9.1. *Reference summary*

| | |
|---|---|
| $\lvert A\rvert$ | cardinality ("size") of set $A$ |
| $\leftrightarrow$ | bijection |
| $\lvert A\rvert = \lvert B\rvert$ | $\exists$ bijection $A \leftrightarrow B$ |
| $\lvert A\rvert < \lvert B\rvert$ | $A \leftrightarrow B' \subset B$ but $A \not\leftrightarrow B$ |

Order of cardinalities:

$$\underbrace{\text{finite, denumerable } (\leftrightarrow \mathbb{N})}_{\text{countable}}, \text{ uncountable } (\not\leftrightarrow \mathbb{N})$$

$\mathscr{P}(A)$ = the power set of $A$ = the set of all subsets of $A$. Example: $\mathscr{P}(\{0,1\}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$.

Key theorems with sketches of proof idea:

- $A \subseteq B$, $B$ denumerable $\implies$ $A$ denumerable (or finite).

$$\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & \cdots \\
\updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots \\
b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & b_7 & \cdots \\
 & = & & = & = & & = & \cdots \\
 & a_1 & & a_2 & a_3 & & a_4 & \cdots \\
 & \updownarrow & & \updownarrow & \updownarrow & & \updownarrow & \cdots \\
 & 1 & & 2 & 3 & & 4 & \cdots
\end{array}$$

- $A \subseteq B$, $A$ uncountable $\implies$ $B$ uncountable.

  Corollary of the above.

- $\mathbb{R}$ uncountable.

  Assume not:

$$\begin{aligned}
1 &\leftrightarrow r_1 = 0.\underline{3}74685501\cdots \\
2 &\leftrightarrow r_2 = 0.8\underline{1}2673303\cdots \\
3 &\leftrightarrow r_3 = 0.13\underline{5}499112\cdots \\
4 &\leftrightarrow r_4 = 0.342\underline{7}70911\cdots \\
&\vdots
\end{aligned}$$

  Make $r_*$ different from $r_n$ in position $n$.

- $\lvert A\rvert < \lvert\mathscr{P}(A)\rvert$

  Assume not:

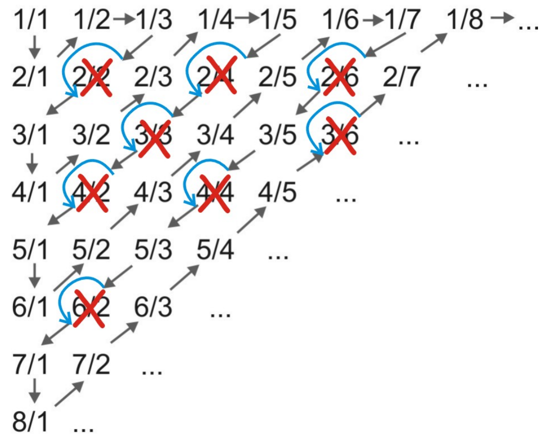
$$\begin{array}{ccc} a & \leftrightarrow & A_a \\ \in A & & \in \mathscr{P}(A) \end{array}$$

  Make $A_*$ different from $A_a$ in what it does with $A$:

$$\text{if } a \in A_a \text{ then } a \notin A_*$$

$$\text{if } a \notin A_a \text{ then } a \in A_*$$

- $\mathbb{Q}$ denumerable.




- If $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

  Given is $A \longleftrightarrow B' \subseteq B$ and $B \longleftrightarrow A' \subseteq A$. Following the image of $A$ we get $A \longleftrightarrow A'' \subseteq A' \subseteq A$. If we had $A \longleftrightarrow A'$ we would be done. We can produce this bijection by extending $A \longleftrightarrow A''$ as shown in problem 9.3.

---

## § *9.2. Problems*

9.1. An algebraic number is a root of a polynomial equation with integer coefficients. Prove that the set of all algebraic numbers is countable.

9.2. Hilbert's Hotel has countably infinitely many rooms, all of which are occupied. Explain how the hotel can accommodate:

(a) one further guest.

(b) one countably infinite busload of further guests.

(c) a countable infinity of countably infinite busloads of further guests.

9.3. Above we saw the need for the following theorem. Let $A'' \subseteq A' \subseteq A$ and suppose there is a bijection $A \longleftrightarrow A''$. Then there is also a bijection $A \longleftrightarrow A'$.

Below are two proofs of this theorem. Are they the same? Is one better than the other?

*Let $A$ and $B$ be nonempty sets such that $B \subseteq A$. If there exists an injective function from $A$ to $B$, then there exists a bijective function from $A$ to $B$.*

If $B = A$, then the identity function $i_A : A \to B = A$ is bijective. Thus we can assume that $B \subset A$ and so $A - B \neq \emptyset$. Let $f : A \to B$ be an injective function. If $f$ is bijective, then the proof is complete. Therefore, we can assume that $f$ is not onto. Hence $\operatorname{range}(f) \subset B$ and so $B - \operatorname{range}(f) \neq \emptyset$.

Consider the subset $B'$ of $B$ defined by

$$B' = \{f^n(x) : x \in A - B, n \in \mathbf{N}\}.$$

Thus $B' \subseteq \operatorname{range}(f)$. Hence, for each $x \in A - B$, its image $f(x)$ belongs to $B'$. Moreover, for $x \in A - B$, the element $f^2(x) = f(f(x)) \in B'$, $f^3(x) = f(f^2(x)) \in B'$ and so on.

Let $C = (A - B) \cup B'$ and consider the restriction $f_1 : C \to B'$ of $f$ to $C$. We show that $f_1$ is onto. Let $y \in B'$. Then $y = f^n(x)$ for some $x \in A - B$ and some $n \in \mathbf{N}$. This implies that $y = f(x)$ for some $x \in A - B$ or $y = f(x)$ for some $x \in B'$. Therefore, $f_1(x) = y$ for some $x \in C$ and so $f_1$ is onto. Furthermore, since $f$ is one-to-one, the function $f_1$ is also one-to-one. Hence $f_1 : C \to B'$ is bijective.

Let $D = B - B'$. Since $B - \operatorname{range}(f) \neq \emptyset$ and $B - \operatorname{range}(f) \subseteq B - B'$, it follows that $D \neq \emptyset$. Also, $D$ and $B'$ are disjoint, as are $D$ and $C$. Certainly, the identity function $i_D : D \to D$ is bijective. Let $h : C \cup D \to B' \cup D$ be defined by

$$h(x) = \begin{cases} f_1(x) & \text{if } x \in C \\ i_D(x) & \text{if } x \in D. \end{cases}$$

By Lemma 10.18, $h$ is bijective. However, $C \cup D = A$ and $B' \cup D = B$; so $h$ is a bijective function from $A$ to $B$. ■

Second proof. Think of these sets as the populations of Sweden ($A''$), Europe ($A'$), and the world ($A$). Imagine that all of these populations are infinite, and that every person lives alone in one apartment, and that every apartment in the world is occupied.

What does the bijection $A \longleftrightarrow A''$ mean in this context? It means everyone in the world can be matched up with a unique Swedish person. We might be tempted to think of it as "everyone marries a Swedish person." But this would be misleading, because marriage is mutual: if I marry you, you marry me. But that is not what the bijection is saying. The bijection is not only pairing up non-Swedish with Swedish people. Swedish people are themselves part of the world population $A$, so they too get assigned another Swedish person in the course of the bijection. Therefore it is better to think of $A \longleftrightarrow A''$ as matching members of the world population with Swedish apartments. Since there was precisely one Swedish person per Swedish apartment to begin with this just another way of looking at the same bijection. This is a better analogy than marriage because it is not mutual: if I move into your apartment, you do not have to move into mine.

So the bijection says that the whole world can move into precisely one apartment each in Sweden. This will involve Swedish people moving around within Sweden to "make room" even though there was already one person per apartment (in the manner of Hilbert's Hotel of problem 9.2).

Given such a bijection, we want to find a bijection $A \longleftrightarrow A'$. That is to say, we want a scheme for everyone in the world to move to Europe in such a way that every European apartment has precisely one person in it.

Maybe some natural disaster made much of the world uninhabitable, and the United Nations hired some mathematicians to figure out how to move everyone to Sweden, which they thought would be the only inhabitable country. But then it turned out the scale of the disaster was not as bad as thought, so actually all of Europe would still be inhabitable.

Therefore we are now facing the problem of how to adapt the original move-everyone-to-Sweden scheme and turn it into a move-everyone-to-Europe scheme. Intuitively we feel it must be doable since it should be "easier" than moving everyone to Sweden, but how exactly should we do it? We might be tempted to say: Everyone outside of Sweden but in Europe just stay put, and everyone in the rest of the world and Sweden move according to the original scheme. Sure enough this will get everyone to Europe. But it won't fulfil the condition that no apartment be left empty. For in the original scheme Swedish people moved about to make room for other Europeans, and since those Europeans are now staying home these apartments will become empty.

Instead we must issue the following instructions. First everyone outside Europe move to the Swedish apartments assigned to them under the original scheme. This means a number of Swedish people will be "bumped" out of their apartments. Let them also move to the apartment assigned to them under the original scheme, and the same for those they bump out in turn, and so on. Let such repercussion moves play out in as many steps as needed, and let everyone not affected simply stay put where they are.

In this way we are left with precisely on person per apartment in Europe. For it is clear that no apartment is left empty since people only move after someone has taken their place. And it is clear that no two moving people are assigned the same apartment, since all moves take place according to the original moving scheme, which by assumption assigned everyone a unique apartment.

We have thus constructed a bijection between the world population and European apartments. By associating each European apartment with its original occupant (when there was precisely one European per European apartment before the moves), this gives a bijection between world population and Europeans, as required.