Discrete Mathematics

Exercises 1 – Solutions with Commentary

Marcelo Fiore   Ohad Kammar   Dima Szamozvancev

1. On proofs

1.1. Basic exercises

The main aim is to practice the analysis and understanding of mathematical statements (e.g. by isolating the different components of composite statements) and exercise the art of presenting a logical argument in the form of a clear proof (e.g. by following proof strategies and patterns).

The solutions will consist of the proper formal proof, showing the required level of detail and precision – you should try to present your answers in a similar form. Of course, a formal written proof is just a polished facade of the (usually more difficult) process of finding the correct sequence of reasoning steps and proof techniques, which often constitutes the "scratchwork". Therefore, most of the formal proofs will be accompanied with notes (marked ♪) on how the problem was approached, what guided the reasoning process and what mistakes should be avoided. Mastering the art of formal proof may take some practice, but it is a very important skill to acquire both for this course and your whole scientific education.

Prove or disprove the following statements.

Some fairly simple statements, but they showcase a wide range of proposition types and proof techniques. Accordingly, the proof notes can apply to most of the statements you will encounter, no matter how complicated.

1. Suppose n is a natural number larger than 2, and n is not a prime number. Then $2 \cdot n + 13$ is not a prime number.

   The statement is false. Choose $n = 9$. Then $n = 3 \cdot 3$ isn't prime, yet $2 \cdot n + 13 = 31$ is prime, and we disproved the statement by a counterexample.

   ♪ "Prove or disprove" questions should usually start with a sanity check: try a few numbers, and if things seem to work, try a formal proof. Unfortunately, this is not a sure-fire technique, as you may need to backtrack after realising that the statement is false after all. If you realise this in the middle of writing the formal proof (rather than just the scratchwork), you need to cross everything out and start again: there is no space for "plot twists" in a proof attempt, and you should state if the statement is true or false right away.

   ♪ To disprove a statement, all we need to present is a counterexample which falsifies it. There is no need to explain the general situation where the statement doesn't work, or try to prove the negation of the statement. The counterexample doesn't have to be very elaborate, often edge cases like 0 or the empty set do the job perfectly. However, we have to make sure that our counterexample falls under the consideration of the statement: 0 will not falsify a proposition that starts with "for every positive integer".

2. If $x^2 + y = 13$ and $y \neq 4$ then $x \neq 3$.

> We equivalently prove that if $x^2 + y = 13$ then $y \neq 4$ implies $x \neq 3$. Assume that $x^2 + y = 13$. We establish the contrapositive of the goal, i.e. if $x = 3$ then $y = 4$. Indeed, assume $x = 3$. Then, $y = 13 - x^2 = 13 - 9 = 4$, as required.
>
> ♪ The statement is of the form $(P \wedge Q) \Rightarrow R$, so our proof algorithm dictates that we should start by assuming P and Q, and prove R. However, in this case, Q and R are *negative* assertions: knowing that y could be anything other than 4 is less useful than knowing that it is equal to something. Since the consequent R is also negated, we may instead consider proving a contrapositive. However, the contrapositive of $(P \wedge Q) \Rightarrow R$ is $\neg R \Rightarrow \neg(P \wedge Q)$, which will turn our useful assumption P into a negated goal. Instead, we perform a *partial assumption*: we assume P only, and prove $Q \Rightarrow R$; this can now be done easily, since the contrapositive will give us the additional assumption $x = 3$ and the goal will be $y = 4$. Logically, this technique follows from the equivalence $(P \wedge Q) \Rightarrow R \simeq P \Rightarrow (Q \Rightarrow R)$, which can be seen as "currying" the proposition Q.

3. For an integer n, n^2 is even if and only if n is even.

> ($\Rightarrow$) We prove the following more general result: The product of an even integer with any integer is an even integer. The required proposition follows as a corollary.
>
> Consider any two integers m, n and assume that m is even. By definition of even integers, $m = 2k$ for some integer k. Therefore, $m \cdot n = 2k \cdot n = 2(k \cdot n)$ and thus, by definition, $m \cdot n$ is an even integer.
>
> ($\Leftarrow$) We prove the contrapositive; i.e., n odd implies n^2 odd. Assume n is odd, then by Proposition 8 (product of odd numbers is odd) of the notes, $n \cdot n = n^2$ is odd.
>
> ♪ As soon as we see the phrase "if and only if", we need to remember not to move on to the next question halfway through the proof. Most of the time such proofs will consist of two parts, so stating which direction is being proved is helpful for the reader (and a good reminder to you to complete both directions).
>
> ♪ Both directions follow as *corollaries* (logical consequences which are important in their own right) of more general statements about multiplying two different even/odd numbers. The advantage of making theorem statements as general as possible is that they can be applied in many contexts and give rise to useful corollaries; we could have proved that the square of an odd number is odd directly, but the underlying proof approach would have been exactly the same as Proposition 8 so we might as well use it!

4. For all real numbers x and y there is a real number z such that $x + z = y - z$.

> Consider arbitrary real numbers x, y, and choose $z = \frac{y-x}{2}$. Then, z is a real number satisfying $x + z = x + \frac{y-x}{2} = \frac{y+x}{2} = y + \frac{y-x}{2} = y - z$. Therefore, there exists a real number z satisfying $x + z = y - z$.

♪ This is an example of an existence proof, which tend to look a bit backwards when written formally: rather than deriving the witness as part of the proof, we "give away" the answer right away, then show that it satisfies the required property. Of course, we don't just pluck the witness out of thin air, or resort to a lucky guess. We find what it should be from the required properties via some sort of calculation, and once we found an answer, we present it as a witness at the very beginning of the formal proof. Showing that it satisfies the properties is of course straightforward (but can't be omitted), since that's how we found the witness in the first place. In this specific example, the answer $z = \frac{y-x}{2}$ can be found by simple rearrangement of the condition $x + z = y - z$, but, to present this as a formal existence proof, we need to state the witness and rigorously demonstrate that it satisfies the requirement.

5. For all integers x and y there is an integer z such that $x + z = y - z$.

The statement is false. Indeed, for the integers $x = 0$ and $y = 1$ we will prove that there does not exist an integer z satisfying $x + z = y - z$; i.e., equivalently, such that $z = 1 - z$. Assume to the contrary that such an integer, say z_0, existed. Then, we would have $2 \cdot z_0 = 1$ and hence $z_0 = \frac{1}{2}$; which is absurd as $\frac{1}{2}$ is not an integer. Therefore, there are integers x and y for which there is no integer z such that $x + z = y - z$.

♪ This proof may seem more verbose than it needs to be: surely we can just say "let $x = 0$ and $y = 1$, then $z = \frac{y-x}{2} = \frac{1}{2}$ which is not an integer". The problem with this reasoning is that it is not a nonexistence proof: we showed that the specific z that can be computed with the method above is not an integer, but that doesn't mean there cannot be any other z that works. To be completely rigorous, we need to show that the existence of any z that satisfies the property is a logical absurdity – from this follows the lengthy but airtight proof of the answer.

♪ Note how in two lines we got to a statement that is *obviously* false: that there exists an integer z such that $z = 1 - z$. We need to resist the temptation to take logical shortcuts and appeal to the intuition of the reader to fill in the holes of our argument: anyone with familiarity of basic arithmetic will recognise this as false (just rearrange the equation to get $z = \frac{1}{2}$, which is is not an integer), but this will not convince someone who reasons purely by logic (and, unfortunately, supervisors and examiners are such people). As explained in the previous point, the easiest logically rigorous way to show that such an integer z does *not* exist is by contradiction.

6. The addition of two rational numbers is a rational number.

Consider any two rational numbers r, s. By definition, there exist some integers a, c and some nonzero integers b, d such that $r = \frac{a}{b}$ and $s = \frac{c}{d}$. Then, $r + s = \frac{a \cdot d + b \cdot c}{b \cdot d}$ is a quotient of an integer (namely $a \cdot d + b \cdot c$) by a nonzero integer (namely $b \cdot d$), and hence a rational number.

♪ A large part of writing formal proofs is just expanding definitions: rather than trying to

reason about rational numbers, we use their formal definition to transition into a proof about integers. The more abstract the statement (quite common in set theory), the more layers of definitions we may need to unwrap. However, this can allow us to prove some rather difficult-looking propositions with a very simple, low-level reasoning step.

7. For every real number x, if $x \neq 2$ then there is a unique real number y such that $2 \cdot y / (y+1) = x$.

We need to show that for every real number x, if $x \neq 2$ then there exists a real number y satisfying: ① $\frac{2y}{y+1} = x$ and ② for all real numbers z, if $\frac{2z}{z+1} = x$ then $y = z$.

Consider an arbitrary real number x, and assume $x \neq 2$. Then, $y = \frac{x}{2-x}$ is a real number satisfying ①, and if z is any real number satisfying $\frac{2z}{z+1} = x$ then $2 \cdot z = z \cdot x + x$. Hence, $(2-x) \cdot z = x$. As $x \neq 2$, $z = \frac{x}{2-x} = y$.

🎵 This is a unique existence proof, so requires two separate arguments: existence and uniqueness. The standard way of proving uniqueness is to assume another value with the same property, and show that it must be equal to the existing witness. Uniqueness may seem like a relatively unimportant result, but in fact, it forms the basis of powerful proof techniques which we'll see later on.

8. For all integers m and n, if $m \cdot n$ is even, then either m is even or n is even.

One may prove the contrapositive of the statement; i.e. that if m and n are odd then $m \cdot n$ is odd. But this is nothing but Proposition 8 of the notes.

🎵 Negation-based proof techniques (contradiction or contraposition) are often used to avoid awkward proof patterns, usually involving existence or disjunction. Rather than have a disjunctive goal (which requires some sort of case-splitting), we negate it to turn (via the de Morgan laws) into a conjunctive assumption.

1.2. Core exercises

Having practised how to analyse and understand basic mathematical statements and clearly present their proofs, the aim is to get familiar with the basics of divisibility.

1. Characterise those integers d and n such that:

   a) $0 \mid n$

   We prove that an integer n satisfies $0 \mid n$ iff $n = 0$.

   ($\Rightarrow$) Assume $0 \mid n$. By definition, for some integer l, $n = l \cdot 0 = 0$.

   ($\Leftarrow$) Assume $n = 0$. Then, $n = 0 \cdot 0$ and, by definition, $0 \mid n$.

   🎵 A good example of the need to be precise when applying definitions. We may intuitively interpret $d \mid n$ ("d divides n") as "$\frac{n}{d}$ is an integer", and conclude that $0 \mid n$ is impossible because $\frac{n}{0}$ is undefined. However, the formal definition of $d \mid n$ makes no mention of the division operator: it is an algebraically more fundamental concept which only requires multiplication to express. Strictly speaking, we haven't

yet formally defined division in the course – sure, you *know* what division is from school, but giving a precise and rigorous definition is more difficult than it may seem! If we use the proper definition of divisibility for this exercise, we do find an appropriate value for n, namely 0: zero divides zero because there exists an integer l (any integer will work) such that $0 = l \cdot 0$.

b) $d \mid 0$

We prove that $d \mid 0$ for all integers d. Indeed, let d be an arbitrary integer. Then, $0 = 0 \cdot d$ and hence $d \mid 0$.

2. Let k, m, n be integers with k positive. Show that:

$$(k \cdot m) \mid (k \cdot n) \iff m \mid n$$

Consider any positive integer k and any two integers m, n.

($\Rightarrow$) Assume $(k \cdot m) \mid (k \cdot n)$. Then, $k \cdot n = l \cdot (k \cdot m)$. As $k > 0$, we can cancel k and deduce $n = l \cdot m$. Hence, $m \mid n$.

($\Leftarrow$) Assume $m \mid n$. Then, $n = a \cdot m$ for some integer a; and multiplying by k, we have $k \cdot n = a \cdot (k \cdot m)$. Hence, $(k \cdot m) \mid (k \cdot n)$.

♪ "Cancelling things" on both sides of an equation is a very standard process in elementary ("high-school") algebra. While in many cases it is still allowed in this course, you should pay extra attention to any side-conditions required for the cancellation, or if cancellation is even possible for the algebraic structure you're working with! It does hold for addition and multiplication (with a side-condition), but, for example, an equation between function composites $f \circ g = f \circ e$ cannot be simplified to $g = e$ in general (only if f is an *injection* – see later). Cancellability may be a property of the structure, or particular elements in a structure, rather than something you can just do arbitrarily.

♪ The ($\Rightarrow$) direction of this proof relied on the fact that k is positive, and in particular, nonzero – otherwise we wouldn't be able to cancel the ks (and the property wouldn't actually hold). We did not require any assumptions on k in the ($\Leftarrow$) direction, so we could extract a weaker form of the theorem, stating that for every integer k, m and n,

$$m \mid n \implies (k \cdot m) \mid (k \cdot n)$$

In some cases you may not have the assumption that k is positive but may still be able to apply this weaker form to make progress. However, this is technically not a corollary of the stronger statement, because that requires an unneeded assumption on k.

3. Prove or disprove that: For all natural numbers n, $2 \mid 2^n$.

This is false, as $2 \nmid 2^0$.

♪ This is just a gentle reminder that 0 is a natural number!

4. Show that for all integers l, m, n,

$$l \mid m \ \land \ m \mid n \Longrightarrow l \mid n$$

> Consider any integers l, m, n, and assume $l \mid m \land m \mid k$. As $l \mid m$, $m = a \cdot l$ for some integer a. As $m \mid n$, $n = b \cdot m$ for some integer b. But then: $n = b \cdot m = b \cdot (a \cdot l) = (b \cdot a) \cdot l$ and, as $b \cdot a$ is an integer, we have $l \mid n$.
>
> ♪ An example of a proof which is not particularly difficult or illuminating, but it's still presented in a clear, structured, formal manner. It should take about a line of scratchwork to convince yourself that the statement is true, but that is only the first step: next, you need to convince the reader of the proof, who may not find your sketch clear or rigorous enough. Learning how to present even the simplest arguments in a formal, systematic manner will massively aid you in tackling more difficult propositions which may seem very daunting at first, but are actually much easier to digest connective-by-connective, definition-by-definition.

5. Find a counterexample to the statement: For all positive integers k, m, n,

$$(m \mid k \ \land \ n \mid k) \Longrightarrow (m \cdot n) \mid k$$

> Choose $k = m = n = 2$. Then, k, m, n are positive integers. As $2 \mid 2$, we have $m \mid k \land n \mid k$ yet $(2 \cdot 2) \nmid 2$.
>
> ♪ While questions like this don't explicitly ask for it, you need to find a counterexample and also show that it is a counterexample, i.e. that it contradicts the statement. Only writing $k = m = n = 2$ is not enough; you need to justify your answer.

6. Prove that for all integers d, k, l, m, n,

a) $d \mid m \land d \mid n \Longrightarrow d \mid (m + n)$

> Assume $d \mid m \land d \mid n$. As $d \mid m$, $m = a \cdot d$ for some integer a. As $d \mid n$, $n = b \cdot d$ for some integer b. Therefore, $m + n = a \cdot d + b \cdot d = (a + b) \cdot d$. As $a + b$ is an integer, we have $d \mid (m + n)$ as required.

b) $d \mid m \Longrightarrow d \mid k \cdot m$

> Assume $d \mid m$; i.e. $m = a \cdot d$ for some integer a. Then, $k \cdot m = k \cdot (a \cdot d) = (k \cdot a) \cdot d$. As $k \cdot a$ is an integer, $d \mid (k \cdot m)$.

c) $d \mid m \land d \mid n \Longrightarrow d \mid (k \cdot m + l \cdot n)$

> Assume $d \mid m \land d \mid n$. As $d \mid m$, by 6(b) above, $d \mid (k \cdot m)$. Analogously, from $d \mid n$ we have $d \mid (l \cdot n)$. Thus, $d \mid (k \cdot m) \land d \mid (l \cdot n)$ so that applying 6(a) we conclude $d \mid (k \cdot m + l \cdot n)$ as required.

♪ Science is about building on the shoulders of giants – even if that giant is us, ten minutes ago. After proving two useful properties of divisibility in parts 6(a) and 6(b), they are now part of our "knowledge base" and we can refer back to them freely, without having to reprove them again.

Mathematics and computer science are all about decomposition and composition (also known as divide-and-conquer). Faced with a complicated proposition/problem, we break it up into smaller components which are much easier to reason about. Then, we find ways to solve the subproblems: prove lemmas and sub-theorems or write functions, classes and methods to perform well-defined tasks. Finally, we combine the sub-solutions and reap the rewards. In practice, however, the challenge is not always in solving the subproblems from scratch, but figuring out which existing elements of the knowledge base/programming library can be glued together to give the desired results: after all, if we or someone else has solved some difficult problem already, we shouldn't need to do it again! There may be a striking one-liner proof/program that does the job, but finding it may take significantly more effort than just solving the problem manually. But, seeing how programmers can spend hours finding the shortest, simplest, fastest, most space-efficient algorithms, there is a lot of enjoyment to be had in crafting concise and elegant proofs that combine clever reasoning techniques with existing propositions in satisfying ways. We will hopefully see examples of this in the course so you can appreciate proof-writing not as a chore, but something intellectually stimulating and often quite addictive!

7. Prove that for all integers n,

$$30 \mid n \iff (2 \mid n \ \wedge \ 3 \mid n \ \wedge \ 5 \mid n)$$

($\Rightarrow$) Assume $30 \mid n$. Then, $n = 30 \cdot a$ for some integer a. Thus, $n = 2 \cdot (15 \cdot a)$ and so $2 \mid n$. Similarly, $n = 3 \cdot (10 \cdot a)$ and therefore $3 \mid n$. And, as $n = 5 \cdot (6 \cdot a)$, we also deduce $5 \mid n$. Therefore $2 \mid n \ \wedge \ 3 \mid n \ \wedge \ 5 \mid n$.

($\Leftarrow$) Assume $2 \mid n \wedge 3 \mid n \wedge 5 \mid n$. As $2 \mid n$ and $3 \mid n$ and $5 \mid n$, we have $n = 2 \cdot a$ and $n = 3 \cdot b$ and $n = 5 \cdot c$ for some integers a, b, c. Moreover, we have:

$$30 \cdot (-a + b + c) = (-15) \cdot 2 \cdot a + 10 \cdot 3 \cdot b + 6 \cdot 5 \cdot c = (-15) \cdot n + 10 \cdot n + 6 \cdot n = n$$

Thus, $n = 30 \cdot k$ for the integer $k = -a + b + c$, as required.

♪ The ($\Leftarrow$) direction of this proof is more subtle than it may look – we can't just multiply $2, 3$ and 5 together (see §1.2.5 above). Instead, we know that $30 \mid 30a$, so $30 \mid 15n$; similarly, $30 \mid 10n$ and $30 \mid 6n$. We need to put these together to get $30 \mid n$, for which we make use of §1.2.6(a) above to find a linear combination of $15n$, $10n$ and $6n$ that adds up to n. After some thinking, we find that $(-1) \times 15 + 10 + 6$ works, giving us the desired coefficients of a, b and c.

8. Show that for all integers m and n,

$$(m \mid n \wedge n \mid m) \implies (m = n \vee m = -n)$$

Consider any pair of integers m, n, and assume that $m \mid n$ and that $n \mid m$. If $m = 0$ then, by §1.2.1(a) above, $n = 0$ and we have $m = n$.

Consider henceforth the case $m \neq 0$. As $m \mid n$ and $n \mid m$, there are integers a, b such that $n = a \cdot m$ and $m = b \cdot n$. Thus, $m = b \cdot a \cdot m$ and, as $m \neq 0$, we have $b \cdot a = 1$. Then, since a and b are integers, either $a = b = 1$ or $a = b = -1$ (otherwise, one would have $a \cdot b \geq 2$ or $a \cdot b \leq -2$). Finally, if $a = b = 1$ then $m = n$, and if $a = b = -1$ then $m = -n$. Either way, $m = n$ or $m = -n$ as required.

♪ You may have started the proof from the second paragraph, without assuming that $m \neq 0$. Then, at the step $m = b \cdot a \cdot m$, you would be stuck (if you're being careful): you can't divide by m because it may be 0. In such cases a common solution is to handle the problematic case ($m = 0$) separately, then have the desired extra assumption $m \neq 0$ in the main proof and continue from there.

9. Prove or disprove that: For all positive integers k, m, n,

$$k \mid (m \cdot n) \implies k \mid m \vee k \mid n$$

We disprove it by means of a counterexample. Choose $m = n = 2$ and $k = 4$. Then $k \mid m \cdot n$, yet neither $k \mid m$ nor $k \mid n$.

♪ It may sometimes be easier to disprove the contrapositive statement, since an implication holds if and only if its contrapositive holds.

10. Let $P(m)$ be a statement for m ranging over the natural numbers, and consider the following derived statement (with n also ranging over the natural numbers):

$$P^{\#}(n) \triangleq \forall k \in \mathbb{N}.\ 0 \leq k \leq n \implies P(k)$$

a) Show that, for all natural numbers ℓ, $P^{\#}(\ell) \implies P(\ell)$.

Let ℓ be a natural number, and assume that

$$P^{\#}(\ell) = \left(\forall \text{ natural number } k.\, 0 \leq k \leq \ell \implies P(k) \right)$$

holds.

Since ℓ is a natural number, it follows by instantiation that

$$0 \leq \ell \leq \ell \implies P(\ell)$$

and, since $0 \leq \ell \leq \ell$ is true by reflexivity of $\leq$, it follows by Modus Ponens that $P(\ell)$ holds as required.

♪ This last exercise starts to trip some students up, understandably: so far we've been proving properties about numbers and divisibility, while now we're proving things about seemingly nothing in particular. Such abstract proofs are very common in mathematics, for the very simple reason that they can be applied in a huge number of ways – in this case, $P(m)$ can be *any* logical statement about natural numbers, and the propositions will hold no matter how simple or complicated the definition of P is! You may think of this as a "polymorphic" theorem, since we are proving something about an arbitrary predicate P (any first-class function `nat -> bool`, if you will), but as a consequence, we cannot assume anything about how it's defined.

Thinking abstractly takes some getting used to, as you may feel like there isn't anything to go on or any familiar notion to grasp in order to build intuition. However, abstractness has the major benefit of avoiding any distracting details and low-level "fluff" that could lead the proof attempt astray. If the above proposition was specialised to $P(m)$ meaning "m is even", you might start by unwrapping the definition of evenness and incorporate it into the proof somehow, despite the property holding no matter what $P(m)$ actually is. Abstract proofs like this often involve purely logical reasoning, without invoking any number theory or algebra – and logical reasoning is often easier, since we essentially have an algorithm for proving logical statements. Thus, when you are faced with an incomprehensible jumble of logical symbols, the task may well be easier than proving a simple statement about natural numbers!

b) Exhibit a concrete statement $P(m)$ and a specific natural number n for which the following statement *does not* hold:
$$P(n) \implies P^{\#}(n)$$

Let $P(m) \triangleq (m = 1)$ and $n = 1$. Then $P(1)$ is the true proposition $(1 = 1)$, but $P^{\#}(1) \iff P(0) \land P(1)$ is equivalent to $(0 = 1) \land (1 = 1)$ which is false.

♪ Here we actually needed to "decode" the definition of $P^{\#}$ in order to find a way to falsify the above statement. Fortunately this is not too difficult in this case: $P^{\#}(n)$ holds if $P(k)$ holds for all naturals less than or equal to n, essentially turning a predicate P about naturals into a predicate $P^{\#}$ about a finite collection of naturals (similarly to how `map` turns a function on values into a function on lists of values). Then, we need to find a predicate P and $n \in \mathbb{N}$ that does not satisfy $P(n) \Rightarrow P^{\#}(n)$. This is trickier than just finding a number, since there are lots of ways we could define P. But, once again, we try something very simple ($P(m)$ holds for $m = 1$ only) and find that it can easily be turned into a counterexample. There are lots of other options for P of course, but there's no need to try something convoluted or interesting to get a contradiction (and equally, there's no need to spend time finding the *simplest* counterexample if you've already found a more complicated one).

c) Prove the following:

- $P^{\#}(0) \iff P(0)$

($\Rightarrow$) Assume $P^{\#}(0)$; that is, for all $0 \leq k \leq 0$, $P(k)$. As $0 \leq 0 \leq 0$, $P(0)$ holds.
($\Leftarrow$) Assume $P(0)$. Consider any k, and assume $0 \leq k \leq 0$. Then, $k = 0$ and $P(k)$ holds by assumption.

- $\forall n \in \mathbb{N}. \left(P^{\#}(n) \Longrightarrow P^{\#}(n+1) \right) \Longleftrightarrow \left(P^{\#}(n) \Longrightarrow P(n+1) \right)$

  ($\Rightarrow$) Assume that $\left(P^{\#}(n) \Longrightarrow P^{\#}(n+1) \right)$, and further assume that $P^{\#}(n)$ holds. Then, it follows that also $P^{\#}(n+1)$ holds; i.e. that

  $$\forall \text{ natural number } k. \, 0 \leq k \leq n+1 \Longrightarrow P(k).$$

  In particular, by instantiation, we have that

  $$0 \leq n+1 \leq n+1 \Longrightarrow P(n+1)$$

  and since the antecedent of this implication is true, we deduce that $P(n+1)$ holds, as required.

  ($\Leftarrow$) Assume that ① $\left(P^{\#}(n) \Longrightarrow P(n+1) \right)$, and further assume that ② $P^{\#}(n)$ holds. We need show that $P^{\#}(n+1)$ also holds; i.e. that

  $$\forall \text{ natural number } k. \, 0 \leq k \leq n+1 \Longrightarrow P(k).$$

  or, equivalently, that

  $$P^{\#}(n) \wedge P(n+1)$$

  hold, which is indeed the case because $P^{\#}(n)$ holds by assumption ② and $P(n+1)$ follows by Modus Ponens from assumptions ① and ②.

  ♪ This is the most complicated statement in this exercise sheet, so do not worry if had difficulties with it. We have universal quantification, bi-implication, nested implication, and unwrapping the definition of $P^{\#}$ gives another layer of quantification and implication. You may take a minute to get a feel for what the statement is saying, but the nice thing about purely logical proofs is that you can often dive in head-first without really thinking about what you're proving!

  Look at the top-level construct (universal quantification, bi-implication, etc.), apply the proof pattern for that construct (often giving you some assumptions), and continue until your goal becomes some atomic statement like $P(n+1)$ (which you can't unwrap further, since you don't know what P is). After "digesting" the proof goal, you should have a bunch of assumptions that you can work with: unwrapping some definitions, instantiating universals, applying Modus Ponens. Eventually you should end up with an assumption that matches the atomic proof goal, and that's enough to conclude the proof.

  At first, doing the "assume | prove"-style scratchwork is very helpful for practicing proof patterns and keeping track of goals and assumptions. It should mostly

feel like an algorithmic process: with a few rule applications you can turn a very scary-looking formula into a primitive goal and a lot of assumptions to work with, and the task usually boils down to finding a way of combining assumptions on the LHS to get something that matches the RHS. Occasionally there is a small bit of actual "thinking" required to make progress, such as finding an appropriate value to instantiate a $\forall$ with, or transforming an assumption in some useful way: in the ($\Longleftarrow$) direction above, really the only clever bit was figuring out that

$$\forall \text{ natural number } k.\, 0 \le k \le n+1 \Longrightarrow P(k).$$

is equivalent to

$$P^{\#}(n) \wedge P(n+1)$$

but even this step was not made in a vacuum, since we already had the assumptions $P^{\#}(n)$ and $P(n+1)$. With some practice these methodical proofs should become second nature, and you will be able to keep track of things in your head, directly writing down the formal proof without any prior scratchwork.

- $\left(\forall m \in \mathbb{N}.\, P^{\#}(m)\right) \iff (\forall m \in \mathbb{N}.\, P(m))$

  ($\Longrightarrow$) Assume that $\forall$ natural number $m.\, P^{\#}(m)$, and let n be an arbitrary natural number. Then, by assumption, $P^{\#}(n)$ holds; that is

  $$\forall \text{ natural number } k.\, 0 \le k \le n \Longrightarrow P(k)$$

  and, by instantiation, $0 \le n \le n \Longrightarrow P(n)$ so that $P(n)$ holds. Thus, we have shown

  $$\forall \text{ natural number } m.\, P(m)$$

  ($\Longleftarrow$) Assume that ① $\forall$ natural number $m.\, P(m)$. We need show that for all natural numbers m and k,

  $$0 \le k \le m \Longrightarrow P(k)$$

  To this end, let m and k be arbitrary natural numbers, and assume $0 \le k \le m$. Since k is a natural number, we may instantiate assumption ① with it yielding $P(k)$ as required.

  ♪ This theorem may seem both surprising and unsurprising. Even though $P^{\#}(m)$ is definitely more general than $P(m)$ (since $P^{\#}(m)$ implies $P(m)$ but not vice versa), in the "limit" of quantifying over *all* natural numbers, they become equivalent. Then again, if $P(m)$ holds for all natural numbers m, of course it would hold for all natural numbers smaller than any n! This theorem (and the properties proved as part of this exercise) form the basis of an important proof technique which will be discussed later in the course.

1.3. Optional exercises

1. A series of questions about the properties and relationship of triangular and square numbers (adapted from David Burton).

   a) A natural number is said to be *triangular* if it is of the form $\sum_{i=0}^{k} i = 0 + 1 + \cdots + k$, for some natural k. For example, the first three triangular numbers are $t_0 = 0$, $t_1 = 1$ and $t_2 = 3$.

   Find the next tree triangular numbers t_3, t_4 and t_5.

   > $t_3 = 6$, $t_4 = 10$, $t_5 = 15$.

   b) Find a formula for the kth triangular number t_k.

   Geometric approach.

   $$2 \cdot t_k = \quad + \quad = \quad = k \cdot (k+1)$$

   Algebraic approach.

   Note that, on the one hand,

   $$\sum_{i=0}^{k}(i+1)^2 - \sum_{i=0}^{k} i^2 \;=\; (k+1)^2 + \left(\sum_{i=0}^{k-1}(i+1)^2 \right) - \left(\sum_{i=1}^{k} i^2 \right) - 0^2$$
   $$=\; (k+1)^2$$

   and that, on the other,

   $$\sum_{i=0}^{k}(i+1)^2 - \sum_{i=0}^{k} i^2 \;=\; \sum_{i=0}^{k}\left((i+1)^2 - i^2 \right)$$
   $$=\; \sum_{i=0}^{k}(2 \cdot i + 1)$$
   $$=\; \left(2 \cdot \sum_{i=0}^{k} i \right) + \sum_{i=0}^{k} 1$$
   $$=\; 2 \cdot t_k + k + 1$$

   so that $t_k = \frac{k^2 + k}{2}$.

   c) A natural number is said to be *square* if it is of the form k^2 for some natural number k.

   Show that n is triangular iff $8 \cdot n + 1$ is a square. (Plutarch, circ. 100BC)

   $(\Rightarrow)$ Assume n is triangular; i.e. $n = t_k$ for some natural number k. By the previous item, $n = \frac{k \cdot (k+1)}{2}$ and one has that $8 \cdot n + 1 = (2 \cdot k + 1)^2$ is a square number.

   $(\Leftarrow)$ Assume that $8 \cdot n + 1$ is a square number; i.e. $8 \cdot n + 1 = a^2$ for some natural number a. Then a^2 is odd and, by Proposition 12 of the notes, thus so is a. Therefore, $a = 2 \cdot k + 1$

for some natural number k. Finally, since $8 \cdot n + 1 = a^2 = (2 \cdot k + 1)^2 = 4 \cdot k^2 + 4 \cdot k + 1$ one has $n = \frac{k^2 + k}{2} = t_k$ as required.

d) Show that the sum of every two consecutive triangular numbers is square. (Nicomachus, circ. 100BC)

Consider any two consecutive triangular numbers t_k and t_{k+1}. Then, a simple calculation shows that the sum $t_k + t_{k+1}$ equals $(k+1)^2$ and hence is square:

$$\frac{k^2 + k}{2} + \frac{(k+1)^2 + k + 1}{2} = \frac{2k^2 + 4k + 2}{2} = k^2 + 2k + 1 = (k+1)^2$$

e) Show that, for all natural numbers n, if n is triangular, then so are $9 \cdot n + 1$, $25 \cdot n + 3$, $49 \cdot n + 6$ and $81 \cdot n + 10$. (Euler, 1775)

Consider any natural number n, and assume that n is triangular; i.e. $n = \frac{k \cdot (k+1)}{2}$ for some natural number k. Then, calculate that $9 \cdot n + 1 = t_{3k+1}$:

$$9\frac{k^2 + k}{2} + 1 = \frac{9k^2 + 9k + 2}{2} = \frac{9k^2 + 6k + 1 + 3k + 1}{2} = \frac{(3k+1)^2 + 3k + 1}{2} = t_{3k+1}$$

Similarly, by completing the square, we can show that $25 \cdot n + 3 = t_{5k+2}$, $49 \cdot n + 6 = t_{7k+3}$, and $81n + 10 = t_{9k+4}$.

f) Prove the generalisation: For all n and k natural numbers, there exists a natural number q such that $(2n+1)^2 \cdot t_k + t_n = t_q$. (Jordan, 1991, attributed to Euler)

Here's a proof by a 2014/15 student (who wished to remain anonymous). Let n and k be arbitrary natural numbers. We know that:

$$t_k = \frac{k(k+1)}{2} \qquad \text{and} \qquad t_n = \frac{n(n+1)}{2}$$

Choose $q = 2nk + n + k$, and calculate:

$$\begin{aligned}
t_q &= \frac{q(q+1)}{2} = \frac{(2nk + n + k) \cdot (2nk + n + k + 1)}{2} \\
&= \frac{4n^2k^2 + 4n^2k + 4nk^2 + 4nk + k^2 + k + n^2 + n}{2} \\
&= \frac{(4n^2 + 4n + 1)(k^2 + k) + n^2 + n}{2} \\
&= (2n+1)^2 \cdot \frac{k(k+1)}{2} + \frac{n(n+1)}{2} \\
&= (2n+1)^2 \, t_k + t_n
\end{aligned}$$

Therefore we are done.

2. Let $P(x)$ be a predicate on a variable x and let Q be a statement not mentioning x. Show that the following equivalence holds:

$$\Big((\exists x.\, P(x)) \implies Q\Big) \iff \Big(\forall x.\, \big(P(x) \implies Q\big)\Big)$$

($\Rightarrow$) Assume $\big(\exists x.\, P(x)\big) \implies Q$. We need show $\forall x.\, \big(P(x) \implies Q\big)$. We do this by considering an arbitrary a and showing that $P(a) \implies Q$, for which in turn we further assume $P(a)$ and finally show Q.

To recap, then, we are in the following situation:

Assumptions	Goal
$\big(\exists x.\, P(x)\big) \implies Q$	Q
for arbitrary a	
$P(a)$	

Then, by the last assumption, $\exists x.\, P(x)$ and from this and the first assumption, by Modus Ponens, we deduce Q as required.

($\Leftarrow$) Assume $\forall x.\, \big(P(x) \implies Q\big)$. We need show $\big(\exists x.\, P(x)\big) \implies Q$. For which we further assume $\exists x.\, P(x)$ and show Q

To recap, then, we are in the following situation:

Assumptions	Goal
$\forall x.\, \big(P(x) \implies Q\big)$	Q
$\exists x.\, P(x)$	

From the second assumption, there is an a for which ① $P(a)$ holds and, by instantiation from the first assumption, ② $P(a) \implies Q$. By Modus Ponens from ② and ①, Q follows as required.

♪ This is a very important duality that crops up in many different forms in mathematics and computer science (and you will certainly encounter variants of it in future courses). Despite this, it may seem quite unintuitive: it almost seems to say that we can convert existential quantification into universal! Of course, we can't ignore the shifting of the parentheses: it's certainly *not* the case that

$$\big(\exists x.\, P(x) \implies Q\big) \iff \big(\forall x.\, P(x) \implies Q\big)$$

A good way to get an intuition for this property is as a generalisation of case analysis. If a property Q depends on the existence of a witness x satisfying $P(x)$, but not x itself, we need to prove Q no matter what x is. That is, our proof must hold for any actual value of the witness, so we can instead look at what possible values can x take, and show Q by assuming $P(x)$ for *all* values x. We are case analysing the potential values of the witness, and proving Q no matter what it is.

Alternatively, we can look at the contrapositives of both sides:

$$\big(\neg Q \implies \neg(\exists x.\, P(x))\big) \iff \big(\forall x.\, (\neg Q \implies \neg P(x))\big)$$

The LHS becomes $\neg Q \implies \big(\forall x.\, \neg P(x)\big)$ using the de Morgan rule for quantifiers; but now

the universal can be extended over the whole implication, since assuming $\neg Q$ first and then taking an arbitrary x is the same as taking an arbitrary x and then assuming $\neg Q$ (which doesn't say anything about x).