100 Questions – Logic and Proofs

Fern Gossow

Introduction. Learning to write proofs is an essential skill for mathematics, but one which requires a lot of practice. Every proof you write should aim to be *valid* (meaning mathematically correct) and *readable* (easy to follow and understand). You can learn to write good proofs by first reading well-written proofs, writing your own and getting feedback from others.

There are also many proof techniques, such as contrapositive, contradiction and mathematical induction. An understanding of logical expressions and arguments is useful, and covered in the worksheet.

We try to write questions that are focused on the proofs rather than other content, but some knowledge of set theory notation, elementary number theory and other general topics will be assumed. Prepare for some difficult questions!

LOGICAL SYMBOLS

Q1) If P and Q are logical propositions, we can construct the propositions $\neg P$, $P \vee Q$, $P \wedge Q$ and $P \to Q$. Write the meaning of each of these symbols and their truth tables.

A) $\neg P$ means "not P", so is true whenever P is false and vice versa. In the truth table we let 0 represent 'False' and 1 represent 'True'.

P	$\neg P$
0	1
1	0

$\vee$ means 'or', $\wedge$ means 'and' and $\to$ means 'implies'.

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1

P	Q	$P \to Q$
0	0	1
0	1	1
1	0	0
1	1	1

Note that $\vee$ includes the case when both P and Q are true, and that implication is still true when P is false. For example, the statement "If Paris is the capital of Australia, then $1+1 = 3$", is true, since the antecedent is false. This is often referred to as *vacuous implication.*

Q2) If P and Q are true propositions and R is false, which of the following statements are true?

a) $P \vee R$

b) $(\neg P \vee Q) \wedge R$

c) $(P \to R) \to \neg R$

d) $(P \wedge \neg Q) \to (\neg P \vee Q)$

A) a) is true, b) is false since R is false, c) is true, d) is true since $P \wedge \neg Q$ is false.

Q3) By constructing the truth tables or otherwise, justify the following:

a) $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$

b) $\neg(P \wedge Q) \equiv \neg P \vee \neg Q$

These are known as de Morgan's laws.

A) Our truth table must consider all four cases between P and Q.

P	Q	$\neg P$	$\neg Q$	$P \vee Q$	$\neg P \wedge \neg Q$	$\neg(P \vee Q)$
0	0	1	1	0	1	1
0	1	1	0	1	0	0
1	0	0	1	1	0	0
1	1	0	0	1	0	0

Similarly, we have

P	Q	$\neg P$	$\neg Q$	$P \wedge Q$	$\neg P \vee \neg Q$	$\neg(P \wedge Q)$
0	0	1	1	0	1	1
0	1	1	0	0	1	1
1	0	0	1	0	1	1
1	1	0	0	1	0	0

Q4) By writing the truth tables, justify the logical equivalence

$$P \to Q \equiv \neg Q \to \neg P.$$

This is known as the *contrapositive*.

A)

P	Q	$\neg Q$	$\neg P$	$P \to Q$	$\neg Q \to \neg P$
0	0	1	1	1	1
0	1	0	1	1	1
1	0	1	0	0	0
1	1	0	0	1	1

Q5) Justify $P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R)$ and $P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)$.

A) We can show that the truth tables of $P \vee (Q \wedge R)$ and $(P \vee Q) \wedge (P \vee R)$ are the same. Since there are three variables, our truth table will have eight rows.

P	Q	R	$Q \wedge R$	$P \vee Q$	$P \vee R$	$P \vee (Q \wedge R)$	$(P \vee Q) \wedge (P \vee R)$
0	0	0	0	0	0	0	0
0	0	1	0	0	1	0	0
0	1	0	0	1	0	0	0
0	1	1	1	1	1	1	1
1	0	0	0	1	1	1	1
1	0	1	0	1	1	1	1
1	1	0	0	1	1	1	1
1	1	1	1	1	1	1	1

The other equivalence can be proved similarly.

Q6) Justify $(P \to Q) \wedge (Q \to R) \to (P \to R)$.

A) To prove an implication, we only need to consider the case where the antecedent is true, since the other case holds by vacuous implication, as explained in Q1). For this we need both $P \to Q$ and $Q \to R$ to be true.

If P is true, then Q is true and hence R is true, so $P \to R$ is true. If P is false, then $P \to R$ is vacuously true. This covers all possible cases, so the implication is proven.

Q7) Under what conditions do we have $P \to Q$ but not $Q \to P$?

A) For $Q \to P$ to be false, we need Q to be true but P to be false. This satisfies $P \to Q$ by vacuous implication.

Q8) Write the following sentences as logical statements involving an implication $\to$.

a) If P is true, then Q is true.

b) P implies Q.

c) P is true whenever Q is true.

d) P is true only if Q is true.

e) P can't be true unless Q is true.

A) a) $P \to Q$, b) $P \to Q$, c) $Q \to P$, d) $Q \to P$, e) $Q \to P$

Q9) Explain the meaning of the *quantifiers* $\exists$ and $\forall$.

A) $\exists$ means "there exists" and $\forall$ means "for all". These quantifiers are followed by propositions which depend on their variables. If they are multiple, such as $\forall x \exists y$, we read this as "for all x, there exists y such that ..".

Q10) Determine whether the following statements are true, where m, n are integers.

a) $\exists n(n \text{ is prime})$

b) $\forall n(n \text{ is prime})$

c) $\exists m \exists n(m \leq n)$

d) $\exists m \forall n(m \leq n)$

e) $\forall m \exists n(m \leq n)$

f) $\forall m \forall n(m \leq n)$

A) a) is true, because there exist prime numbers. b) is false, since not every integer is prime. c) is true. d) is not because there is no m which is smaller than every integer n. e) is true, because given any m, we can then choose n to be $m + 1$. f) is false, since it could be that m is bigger than n.

Note that the order of the quantifiers matters! The $\exists m \forall n(m \leq n)$ is false, whereas $\forall n \exists m(m \leq n)$ is true, since we are allowed to choose m depending on n.

Q11) If $P(n)$ is a logical proposition depending on n, which of the following is always true (regardless of the proposition P)?

a) $(\exists n(P(n))) \to (\forall n(P(n)))$

b) $(\forall n(P(n))) \to (\exists n(P(n)))$

A) b) is true, since we can take any n as an example. However, a) is false. Just because $P(n)$ is true for *some* n, this does not mean it will be true for *all* n. We jokingly call such arguments *proof by example*, but they are not valid proofs.

Q12) Give an example of a proposition $P(n)$ where n is an integer such that $\neg\exists n(P(n))$ is true, but $\exists n(\neg P(n))$ is false. This shows that the supposed equivalence

$$\neg(\exists n(P(n))) \equiv \exists n(\neg P(n))$$

is **not** valid. It turns out that the correct equivalence is

$$\neg(\exists n(P(n))) \equiv \forall n(\neg P(n)).$$

Check that this works with your proposition P.

A) Let $P(n)$ be the proposition "$n^2 < 0$". Then there does not exist an integer n such that $P(n)$ is true (since square numbers can't be negative). However, $\exists n(\neg P(n))$ is true, since we can take $n = 0$, and $\neg P(0)$ is true since $P(0)$ is false.

Because there does not exist n with $P(n)$ true, we know that $P(n)$ is false for *every* integer n, which gives $\forall n(\neg P(n))$.

Q13) Write a statement without negation symbols which is equivalent to

$$\neg(\forall n\exists m(\neg P(m) \vee \neg Q(n)).$$

A) Using the solution of Q12), the statement is equivalent to

$$\exists n\forall m(\neg(\neg P(m) \vee \neg Q(n))$$

which by Q3) is

$$\exists n\forall m(\neg\neg P(m) \wedge \neg\neg Q(n)).$$

Since $\neg\neg P \equiv P$ for any proposition we have

$$\exists n\forall m(P(m) \wedge Q(n)).$$

Q14) Suppose $\psi(n)$ is a proposition on integers such that

$$\psi(0) \wedge \forall n(\psi(n) \to (n = 0))$$

a) What does this statement say about ψ?

b) What is the proposition ψ?

A) This statement says that $\psi(0)$ is true, and if $\psi(n)$ is true then it must be that $n = 0$. In particular, this statement is true if and only if $n = 0$, so $\psi(n)$ is "n is equal to 0".

Q15) Suppose $\phi(n)$ is a proposition on positive integers which satisfies the following logical statement:

$$\forall n \exists m((m \geq n) \wedge \phi(m)).$$

a) What does this statement say about ϕ?

b) How many positive integers satisfy $\phi(n)$?

A) The statement says that for any positive integer n, we can find some positive integer m greater than n such that $\phi(m)$ is true. This is equivalent to saying that infinitely many positive integers satisfy ϕ, since no matter how large we make n there is still a larger value satisfying ϕ.

Q16) Given a proposition $P(n)$, write a formal expression which translates as

"7 is the smallest positive integer for which P is true."

A) We want to say that $P(7)$ is true, and any other value n where $P(n)$ is true must satisfy $n \geq 7$. This gives

$$P(7) \wedge \forall n(P(n) \rightarrow (n \geq 7))$$

Q17) Convert the following statements about a positive integer n into logical statements.

a) n is an odd number.

b) n is divisible by 5.

c) n is not a power of two.

d) n is a composite number.

e) n is a prime number.

A) Odd numbers are integers of the form $2k + 1$, so we have

$$\exists k(n = 2k + 1).$$

For a number to be divisible by 5, there needs be some k such that $n = 5k$, which gives

$$\exists k(n = 5k).$$

If n is not a power of two, then there is no k such that $n = 2^k$, which we can write as

$$\neg \exists k(n = 2^k).$$

Using Q12), we can rewrite this as

$$\forall k(n \neq 2^k).$$

For n to be a composite number, there exists integers $a, b > 1$ such that $n = ab$, which we can write as

$$\exists a \exists b((a > 1) \wedge (b > 1) \wedge (n = ab)).$$

Since being prime is the negation of being composite, this is

$$\forall a \forall b((a = 1) \vee (b = 1) \vee (n \neq ab)).$$

Using $\neg P \vee R \equiv P \to R$, rewrite this as

$$\forall a \forall b((n = ab) \to ((a = 1) \vee (b = 1))).$$

Q18) The following statement makes a claim about a sequence of integers $a_1, a_2, \ldots$. What claim is being made about the sequence?

$$\forall N \exists k \forall m((m \geq k) \to (a_m \geq N)).$$

(Hint: Replace N with a fixed number, like 1,000. What does it say now?)

A) Using the hint, the statement says there is some k such that $a_m \geq 1000$ for evey $m \geq k$. We can translate this to "the values of the sequence is eventually always bigger than 1000". Since we range over all N, this statement says "the sequence eventually exceeds any given value". This means the sequence trends towards $+\infty$, and we write $a_n \to +\infty$.

Q19) We can make similar statements for real-valued function $f : \mathbb{R} \to \mathbb{R}$, known as ε–δ definitions. Let ε and δ represent positive real numbers. What specifically is being claimed about the function here?

$$\forall \varepsilon \exists \delta \forall x((0 < x < \delta) \to (0 < f(x) < \varepsilon)).$$

A) The statement claims that for any positive number ε, the values of the function $f(x)$ for x between 0 and δ are less than ε. By letting ε get smaller and smaller, this means that the values of $f(x)$ get closer to 0 as x approaches 0 from the positive direction. In calculus we write this as

$$\lim_{x \to 0^+} f(x) = 0.$$

Q20) Translate the following into a logical statement:

"For any positive integer n, there is a prime number bigger than n."

If you like, you may let $\varrho(n)$ be the proposition "n is prime".

A)

$$\forall n \exists p(\varrho(p) \wedge (p \geq n)).$$

Using our expanded definition of being prime from Q17) we have

$$\forall n \exists p \forall a \forall b((p \geq n) \wedge ((p = ab) \to ((a = 1) \vee (b = 1))).$$

As in Q15), this statement is equivalent to saying "there are infinitely many prime numbers". We will prove this statement later!

Q21) Suppose $\varrho(n)$ is the proposition "n is prime". Translate the following famous open problems about prime numbers into words. All variables are positive integers.

a) Legendre. $\forall n \exists p(\varrho(p) \wedge (n^2 \leq p \leq (n+1)^2))$

b) Fermat. $\forall n(n > 4) \rightarrow \neg\varrho(2^{2^n} + 1))$

c) Goldbach. $\forall n \exists p \exists q(\varrho(p) \wedge \varrho(q) \wedge ((n = 1) \vee (2n = p + q)))$

d) Feit–Thompson.
$\forall p \forall q((\varrho(p) \wedge \varrho(q) \wedge \exists k(k(p^q - 1)/(p-1) = (q^p - 1)/(q-1)) \rightarrow (p = q)))$.

A) Legendre's conjecture says that there is a prime number between n^2 and $(n+1)^2$ for every n. Fermat's conjecture says that $2^{2^n} + 1$ is a composite number for every $n \geq 4$. Goldbach's conjecture says that every even number can be expressed as a sum of two primes, except for 2. The Feit–Thompson conjecture says that for all prime numbers p and q, $(p^q - 1)/(p-1)$ divides $(q^p - 1)/(q-1)$ only if $p = q$. In other words, for distinct prime numbers p and q, then $(p^q - 1)/(p-1)$ does not divide $(q^p - 1)/(q-1)$.

EXAMPLES AND COUNTEREXAMPLES

When given a proposition of the form $(\exists n : P(n))$, you can prove it is true by finding an n for which $P(n)$ is true. When given a proposition of the form $(\forall n : P(n))$, you need to give a *general proof* of $P(n)$ which works for every n. However, if you are trying to disprove the proposition, you can give a single counterexample.

For the following statements, determine whether they are true or false, and provide a proper justification of why. These may involve examples, counterexamples and general proofs.

Q22) For all integers m and n, if $m \leq n$ then $m^2 \leq n^2$.

A) This is false. For a counterexample, $-2 \leq -1$ but $(-2)^2 \not\leq (-1)^2$.

Q23) If the last digit of n is 5, then the last digit of n^2 is also 5.

A) This is true. If the last digit of n is 5, then $n = 10k + 5$ for some integer k, and by calculating n^2 we have

$$n^2 = (10k+5)^2 = 100k^2 + 100k + 25 = 10(10k^2 + 10k + 2) + 5$$

so the last digit of n^2 is also 5.

Q24) Every square number is divisible by four.

A) This is false, a counterexample is 9.

Q25) If x and y are real numbers, then $xy = 0$ if and only if $x = 0$ or $y = 0$.

A) This is true. If $x = 0$ then $xy = 0 \cdot y = 0$ and if $y = 0$, then $xy = 0$ similarly. Conversely, suppose $xy = 0$. If $x \neq 0$ then we can divide by x on both sides to get $y = 0/x = 0$, so $y = 0$. Likewise, if $y \neq 0$ then $x = 0$, so at least one of the two must be zero.

It is important to prove both directions of this implication!

Q26) If $x_1 \neq y_1$ and $x_2 \neq y_2$, then $x_1 y_1 \neq x_2 y_2$.

A) This is false, for a counterexample take $x_1 = 2$, $y_1 = 3$, $x_2 = 3$ and $y_2 = 2$. We have $x_1 \neq y_1$ and $x_2 \neq y_2$, but $x_1 y_1 = x_2 y_2$.

Q27) If a leaves a remainder of 1 when dividing by three, then $5a$ leaves a remainder of 2.

A) This is true. We have $a = 3k + 1$, hence

$$5a = 5(3k + 1) = 15k + 5 = 3(5k + 1) + 1$$

so we get a remainder of 2.

Q28) A triangle has an *obtuse* angle if and only if it has two angles such that the sum of these angles is less than $90°$.

A) This is true. If α, β and γ are the angles from in the triangle from largest to smallest, then $\alpha + \beta + \gamma = 180°$ and rearranging gives

$$\alpha = 180° - (\beta + \gamma).$$

If one of the angles is obtuse then $\alpha > 90°$, so $\beta + \gamma < 90°$. Conversely, if two angles add to less than $90°$, than the two smallest angles add to less than $90°$, hence $\beta + \gamma < 90°$ and hence $\alpha > 90°$.

Q29) The average of a list of numbers can't be bigger than the maximum value in the list.

A) This is true. Suppose $x_1, \ldots, x_n$ are the numbers, x is the largest value and μ is the average. Since $x \geq x_i$ for every i, we have

$$x = \frac{x + \cdots + x}{n} \geq \frac{x_1 + \cdots + x_n}{n} = \mu$$

and so the largest value is at least as big as the average.

Q30) Real numbers a and b are both irrational if and only if $a + b$ is irrational.

A) Both directions of this implication are false. For example, $a = \sqrt{2}$ and $b = -\sqrt{2}$ are both irrational, but $a + b = 0$ is rational. Convesely, $1 + \sqrt{2}$ is irrational, but we can write this as $a + b$ where $a = 1$ and $b = \sqrt{2}$, which are not both irrational.

Q31) $\forall m \exists n (n > 2^m)$

A) This is true. For any m, set $n = 2^m + 1$. Then $n > 2^m$.

Q32) $\forall x \exists y \forall z (((x \leq z) \wedge (0 < x)) \rightarrow (0 < y < z))$

A) This is true. Set $y = x/2$. We can rewrite the implication as

$$0 < x \leq z \rightarrow 0 < y < z$$

which is true since $0 < x/2 < x \leq z$, so $0 < y < z$ whenever $0 < x \leq z$.

Q33) $\forall m \exists n \forall p (m + n = p)$

A) This is false. Since n can only depend on m, we can choose p so that the equation doesn't work. For example, take $p = m + n + 1$.

Q34) $\neg \exists x \forall y (y = 5x + 1)$

A) This is true. We can rewrite this statement as

$$\forall x \exists y (y \neq 5x + 1).$$

We can choose $y = 5x$ for example.

Q35) $\exists x \forall y \exists z (z = xy)$.

A) This is true. Take $x = 0$ and $z = 0$. Then $0 = 0 \cdot y$ is true for all integers y, so the statement holds. Another option would be to take $x = 1$ and $z = y$.

Q36) There is a unique solution to $x^2 = x$ in the real numbers.

A) This is false. The solutions $x = 0$ and $x = 1$ give two distinct solutions.

Q37) An integer is divisible by 6 if and only if it divisible by 2 and divisible by 3.

A) If n is divisible by 6, then $n = 6k$ for some integer k, so we have $n = 2(3k)$ and $n = 3(2k)$, so n is divisible by 2 and 3.

Conversely, suppose n is divisible by 2 and 3. Then $n = 3k$ for some integer k, but since n is also even, k must be even, and so $k = 2m$ and $n = 3(2m) = 6m$, hence n is divisible by 6.

Q38) The number 123123123 is prime.

A) This is false, since $123123123 = 123 \times 1001001$.

Q39) There is a positive integer n such that the last digit of n^2 is 7. (Hint: Do you actually need to check *every* positive integer here?)

A) If the last digit of n is r, then $n = 10q + r$ for some integer q and $0 \leq< r < 10$. Then $n^2 = 100q^2 + 20qr + r^2 = 10(10q^2 + 2qr) + r^2$, so the last digit is the last digit of r^2. Hence, we only have to consider the squares of $0, 1, \ldots, 9$. We have

$$0 \to 0,\ 1 \to 1,\ 2 \to 4,\ 3 \to 9,\ 4 \to 6,\ 5 \to 5,\ 6 \to 6,\ 7 \to 9,\ 8 \to 4,\ 9 \to 1$$

and so the last digit is never 7.

CONTRAPOSITIVE

Replacing an implication $P \to Q$ by $\neg Q \to \neg P$ can sometimes result in a statement which is easier to prove (or disprove). It is a common mistake to replace the implication with $Q \to P$. This is the *converse*, and is not equivalent.

Q40) Consider the statement

"If it is raining, the bus will be late."

a) Write the contrapositive to the statement.

b) Write the converse to the statement.

c) What is a situation where the statement holds, but the converse doesn't?

A) The contrapositive is

"If the bus is on time, it's not ranining."

The converse statement is

"If the bus is late, it must be raining."

This is not equivalent to the original statement, since it is possible that the bus is late even though its sunny, maybe because the bus drivers union is on strike.

Q41) Write the contrapositive to: "prime numbers have exactly two divisors".

A) "Numbers which don't have two divisors are composite."

Q42) Write the contrapositive to the statement: "students who spend more time studying are less likely to fail the course".

A) "Students are more likely to fail the course when they spend less time studying". *Technically*, the statement should be "more or equally likely" and "less or equal time", since the negation of $x < y$ is $x \geq y$.

Q43) Write the contrapositive to: "reptiles are tetrapods with ectothermic metabolisms".

A) The contrapositive to a statement $P \to Q \wedge R$ is $(\neg Q \vee \neg R) \to \neg P$. Hence, we get "If an animal isn't a tetrapod or if it doesn't have an ectothermic metabolism, it is not a reptile".

Q44) Prove by contrapositive that if a^2 is an odd integer, then so is a.

A) The contrapositive is "a even $\to a^2$ even", which we need to prove. If a is even, then $a = 2k$ so $a^2 = 4k^2 = 2(2k^2)$ is even as required.

Q45) Prove by contrapositive that if $x \neq 0$ is an irrational number, then so is $1/x$.

A) Suppose $1/x$ is rational. Then $1/x = a/b$ for integers a and b. Then $x = b/a$ by taking the reciprocal, which is again rational.

Q46) Prove by contrapositive that if $x + y > 200$, then $x > 100$ or $y > 100$.

A) The contrapositive is

$$(x \leq 100) \wedge (y \leq 100) \to (x + y \leq 200).$$

This statement is now obvious, since $x + y \leq 100 + 100 = 200$.

Q47) Prove that for $p > 2$, if p is prime then p is odd.

A) If $p > 2$ is even, then $p = 2k$. Since $2 > 1$ and $k > 1$, p is a composite number and hence is not prime.

Q48) If n is a multiple of three, it can be written as the sum of three consecutive integers.

A) If n is not the sum of three consecutive integers, then

$$\forall k(k + (k+1) + (k+2) \neq n) \equiv \forall k(3(k+1) \neq n)$$

Substituting m for $k + 1$ and taking out the $\neg$ we get

$$\neg \exists m(3m = n)$$

and hence n is not a multiple of 3.

Q49) Call a real number x *Gausslike* if $x = a + b\sqrt{2}$ for integers a and b. Prove that if xy is not Gausslike, then at least one of x and y is not Gausslike.

A) For the contrapositive, assume x and y are both Gausslike. Then we have $x = a+b\sqrt{2}$ and $y = c + d\sqrt{2}$, and hence

$$xy = (ac + 2bd) + (ad + bc)\sqrt{2}$$

is Gausslike.

Q50) In a court case, the police make the following argument:

> "The drug test we use has a 100% detection rate, which means if you have smoked cannabis recently you will always test positive. Since you tested positive, we can prove you recently smoked."

Is this argument valid? What should your lawyer say?

A) The conclusion "tested positive → recently smoked" is the converse of the drug test having a 100% detection rate, instead of the contrapositive, which would be "if you test negative, you didn't smoke".

Your lawyer should explain to the jury that a 100% detection rate is very suspicious, because this means the testing kit is probably returning a positive no matter what.

Q51) Your landlord tells you that if electricity prices rise or a new school is built in your neighbourhood, your rent will increase. Neither of those happened this year, so what can you expect about your rent?

A) The converse to your landlord's statement is

"if your rent doesn't rise, electricity prices didn't rise and no schools were built".

This statement will be true if rents don't rise (because the consequent is true), but is also true if rents *do* rise (by vacuous implication). So this information is not enough to determine whether your rent will rise or not.

MATHEMATICAL INDUCTION

Induction is a technique for proving a statement $P(n)$ for all positive integers $n \geq 1$. This is accomplished by proving the following two facts:

- $P(1)$,
- $P(k) \to P(k+1)$ for every $k \geq 1$.

The proposition $P(1)$ is called the *base case* and is often very easy to prove. The statement $P(k)$ is called the *inductive hypothesis*, and you allowed to use this proposition to prove $P(k+1)$.

There are also variations on induction, called *strong induction.* The most general case is to strengthen the inductive hypothesis to give

- $P(1)$,
- $(P(1) \wedge P(2) \wedge \cdots \wedge P(k)) \to P(k+1)$ for every $k \geq 1$.

Q52) Let $S(n) := 1 + 2 + \cdots + n$. We want to prove a simple formula which calculates $S(n)$ for every $n \geq 1$ using mathematical induction.

a) Find $S(5)$.

b) It is known that $S(499) = 124,750$. What is $S(500)$?

c) Assuming that $S(k) = \dfrac{k(k+1)}{2}$, find a similar formula for $S(k+1)$.

d) Prove that $S(n) = \dfrac{n(n+1)}{2}$ for every $n \geq 1$ by induction.

A) $S(5) = 1 + 2 + 3 + 4 + 5 = 15$. Given $S(499)$, we know that

$$S(500) = \underbrace{1 + 2 + \cdots + 499}_{S(499)} + 500 = 124,750 + 500 = 125,250.$$

More generally, using the assumption from c) we have

$$S(k+1) = \underbrace{1 + \cdots + k}_{S(k)} + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}.$$

We use these facts to prove the necessary induction steps.

- $P(1)$. We have $S(1) = 1 = \dfrac{1(1+1)}{2}$ as required.
- $P(k) \to P(k+1)$. Assuming the formula holds for $S(k)$ and using the above calculation, we have

$$S(k+1) = \frac{(k+1)(k+2)}{2} = \frac{(n+1)((n+1)+1)}{2}$$

which proves the formula for $n = k + 1$ as required.

Q53) Guess a simple formula for $1 + 3 + \cdots + (2n - 1)$ by computing the sum for $n = 1, 2, 3$. Prove this formula using induction.

A) After calculating a few examples it seems we should try to prove the proposition $P(n)$ on all positive integers that

$$1 + 3 + \cdots + (2n - 1) = n^2.$$

The proposition $P(1)$ is "$1 = 1^2$", which is true. We assume the statement for $P(k)$. Then

$$1 + 3 + \cdots + (2k - 1) + (2k + 1) = k^2 + (2k + 1) = (k + 1)^2$$

and hence $P(k) \to P(k+1)$, so $P(n)$ is true for every $n \geq 1$ by mathematical induction.

Q54) Prove that $1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n + 1)! - 1$ for every $n \geq 1$.

A) The statement for $P(1)$ is "$1 \cdot 1! = 2! - 1$", which is true. Assuming $P(k)$, we have

$$1 \cdot 1! + \cdots + k \cdot k! + (k + 1) \cdot (k + 1)! = (k + 1)! - 1 + (k + 1)(k + 1)!$$

Taking out the common term gives $(k + 1 + 1)(k + 1)! - 1 = ((k + 1) + 1)! - 1$, so the statement $P(k + 1)$ is true. This gives $P(k) \to P(k + 1)$ and hence the formula is true for every $n \geq 1$ by induction.

Q55) Prove that the last digit of every positive power of 6 is also 6.

A) We first prove that if the last digit of x is 6, then the last digit of $6x$ is also 6. If $x = 10k + 6$, then

$$6x = 6(10x + 6) = 60x + 36 = 10(6x + 3) + 6.$$

We now prove the result by induction. Since $6^1 = 6$, the statement is true for $n = 1$. Assume the last digit of 6^k is 6. Then $6^{k+1} = 6 \cdot 6^k$ has last digit 6 by our first claim, so the result follows by induction.

Q56) Prove that $n^3 + 2n$ is divisible by 3 for every $n \geq 1$.

A) For $n = 1$ we hav $1^3 = 2 \cdot 1 = 3 = 3 \times 1$. Assume that $k^3 + 2k$ is divisible by 3. Then there exists an integer m such that $k^3 + 2k = 3m$. We need to prove that $(k+1)^3 + 2(k+1)$ is also divisible by 3. We have

$$\begin{aligned}(k+1)^3 + 2(k+1) &= k^3 + 3k^2 + 3k + 1 + 2k + 2\\ &= (k^3 + 2k) + 3k^2 + 3k + 4\\ &= 3m + 3(k^2 + k + 4) = 3(m + k^2 + k + 4)\end{aligned}$$

which is divisible by 3 since $m + k^2 + k + 4$ is an integer.

Q57) Prove that $7^{2n} - 1$ is divisible by 12 for every $n \geq 1$.

A) For $n = 2$ we have $7^2 - 1 = 48 = 12 \times 4$, so the result is true. We prove that $P(k) \to P(k+1)$. Assume that $7^{2k} - 1$ is divisible by 12, so $7^{2k} - 1 = 12m$ for some integer m. We prove the result of $n = k + 1$. We have

$$7^{2(k+1)} - 1 = 7^{2k+2} - 1 = 49(7^{2k}) - 1 = 49(12m + 1) - 1 = 12(49m + 4)$$

which is divisible by 12 as required.

Q58) Prove that $8^n - 3^n$ is divisible by 5 for every $n \geq 1$.

A) For $n = 1$ we have $8^1 - 3^1 = 5 = 5 \times 1$. Assume $8^k - 3^k = 5m$ for some integer m. This gives

$$\begin{aligned}8^{k+1} - 3^{k+1} &= 8(8^k) - 3(3^k)\\ &= 8(5m + 3^k) - 3(3^k)\\ &= 40m + 5(3^k) = 5(8m + 3^k)\end{aligned}$$

and since $8m + 3^k$ is an integer, we have proven that $8^{k+1} - 3^{k+1}$ is divisible by 5 and so the result is proven for every $n \geq 1$ by induction.

Q59) Let $P(n)$ be the statement: $5^n + 1$ is divisible by 6.

a) Show that $P(1)$ is true.

b) Prove that $P(k) \to P(k+2)$.

c) For which positive integers can you conclude the statement holds?

d) Is the statement true for all positive integers?

A) For $n = 1$ we have $5^n + 1 = 6 = 6 \times 1$. Assume that $5^k + 1 = 6m$ for some integer m. We want to prove that $P(k) \to P(k+2)$, so we have

$$5^{k+2} + 1 = 25(5^k) + 1 = 25(6m - 1) + 1 = 150m - 24 = 6(25m - 4)$$

which is divisible by 6. Since we have $P(1)$ and

$$P(1) \to P(3) \to P(5) \to P(7) \to \cdots$$

the result is true for all positive odd integers. We also have the chain of implications

$$P(2) \to P(4) \to P(6) \to P(8) \to \cdots$$

but none of these are true. In particular, $5^2 + 1 = 26 = 2 \times 13$ is not divisible by 6.

Q60) Prove that $2^n \geq n + 1$ for every $n \geq 0$.

A) For $n = 0$ we have $2^0 = 1 \geq 1 = 0 + 1$. We assume that $2^k \geq k + 1$, and we want to prove the result of $n = k + 1$. We have

$$2^{k+1} = 2 \cdot 2^k \geq 2(k+1) = 2k + 2 \geq k + 2 = (k+1) + 1$$

for every $k \geq 0$ as required, so the result is true for every $n \geq 0$ by induction.

Q61) Prove that $\dfrac{(2n)!}{2^n}$ is an integer for every $n \geq 0$.

A) For $n = 1$ we have

$$\frac{(2 \cdot 0)!}{2^0} = \frac{0!}{1} = \frac{1}{1} = 1$$

which is an integer. Assume the result for $n = k$. Then

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

which is an integer since this is a product of integers by the inductive assumption.

Q62) Find the flaw in the following strong induction proof, which ‘proves’ the proposition $P(n)$ that $2^n = 1$ for every $n \geq 0$.

- Proof of $P(0)$: We have $2^0 = 1$, since $a^0 = 1$ for every $a \neq 0$.
- Assumption: Assume that $2^j = 1$ for every $0 \leq j \leq k$.
- Proof of $P(k+1)$: We have

$$a^{k+1} = \frac{a^k \cdot a^k}{a^{k-1}} = \frac{1 \cdot 1}{1} = 1$$

using our assumptions.

A) The proof of $P(0)$ is correct, and the assumption is fine (we are using strong induction here). The proof of $P(k+1)$ works for any $k \geq 1$, but it does not work for $k = 0$ since we have not proven that $a^{-1} = 1$. So we never prove the implication $P(0) \to P(1)$, so the chain can't continue.

Q63) Consider the following argument:

> "1 is much less than a million. If k is much less than a million, then so is $k+1$. Hence, every positive integer is much less than a million by mathematical induction."

How does this make you feel?

A) I personally love this proof. It gets to the heart of why we need precise definitions in mathematics, and how induction says something deep about proving statements involving large numbers.

Q64) Suppose you have proven the statements

1. $P(2)$
2. $P(2) \wedge P(n) \to P(2n)$ for $n \geq 2$
3. $P(n) \to P(n-1)$ for $n \geq 2$

Is this sufficient to conclude that $P(n)$ is true for every integer $n \geq 1$?

A) Yes, this is sufficient. Once we prove $P(2)$, we have the implications

$$\begin{tikzcd}
P(2) \arrow[r] \arrow[d] & P(4) \arrow[r] \arrow[d] & P(8) \arrow[r] \arrow[d] & \cdots \\
P(1) & P(3) \arrow[d] & P(7) \arrow[d] & \\
& P(2) \arrow[d] & P(6) \arrow[d] & \\
& P(1) & \vdots &
\end{tikzcd}$$

so $P(n)$ will be true for every $n \geq 1$.

Q65) A row of n books are placed on a shelf. If you can only swap adjacent books, how many swaps does it take to completely reverse the order of the books? Prove your formula by mathematical induction.

A) Suppose is takes $S(n)$ swaps to reverse the order of n books. We can first reverse the order of the first $n-1$ books, and then make $n-1$ swaps to move the last book to the front. This is minimal since every swap involves two books which are out of order. Hence, we have

$$S(1) = 0 \text{ and } S(n) = S(n-1) + n - 1.$$

This gives $S(n) = 0 + 1 + 2 + \cdots + (n-1)$. From Q52) we guess that

$$S(n) = \frac{n(n-1)}{2}.$$

The claim is true for $n = 1$ since $S(1) = 0$. Assume the formula for $n = k$. Then

$$S(k+1) = S(k) + (k+1-1) = \frac{k(k-1)}{2} + k = \frac{k(k+1)}{2} = \frac{(k+1)(k+1-1)}{2}$$

as required.

Q66) Let a_n be the sequence given by $a_1 = \sqrt{2}$ and $a_{n+1} = \sqrt{2 + a_n}$ for every $n \geq 1$.

a) Find the value of a_1, a_2 and a_3 using a calculator.

b) Prove that $a_n < 2$ for every $n \geq 1$.

ecosia

A) We have $a_1 = 1.414\ldots$, $a_2 = 1.848\ldots$ and $a_3 = 1.962\ldots$. For $n = 1$ we have $a_1 < 2$ and we assume that $a_k < 2$. Then

$$a_{k+1} = \sqrt{2 + a_k} < \sqrt{2+2} = \sqrt{4} = 2.$$

Hence $a_n < 2$ for every $n \geq 1$ by induction. In fact, it turns out that as $n \to \infty$ we have $a_n \to 2$.

Q67) Define the function $f : \mathbb{R} \to \mathbb{R}$ by

$$f(x) = \frac{x}{1-x}.$$

Use induction to prove for every $n \geq 1$ that the n-fold function composition is given by

$$f^{(n)}(x) = f(f(f \cdots f(x))) = \frac{x}{1 - nx}.$$

A) For $n = 1$ we have

$$f^{(1)}(x) = f(x) = \frac{x}{1-x} = \frac{x}{1 - 1 \cdot x}$$

as required. Assuming the formula for $f^{(k)}(x)$, we have

$$f^{(k+1)}(x) = f^k(f(x)) = \frac{f(x)}{1 - kf(x)}.$$

We then expand the formula for $f(x)$ to get

$$\frac{\frac{x}{1-x}}{1 - \frac{kx}{1-x}} = \frac{x}{1 - x - kx} = \frac{x}{1 - (k+1)x}$$

as required, so the formula holds for all $n \geq 1$ by induction.

Q68) The *Fibonacci numbers* is the sequence $0, 1, 1, 2, 3, 5, 8, \ldots$ is is defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for every $n \geq 1$. These numbers naturally occur as the number of petals on a sunflower, for example. Let $\Psi(n)$ be the proposition

$$F_0 + F_1 + F_2 + \cdots + F_{n-1} = F_{n+1} - 1$$

for every $n \geq 1$, which we will prove by a variant of induction.

a) Check whether $\Psi(4)$ is true.

b) As base cases for the induction, prove $\Psi(1)$ and $\Psi(2)$.

c) By assuming $\Psi(k)$, prove $\Psi(k+2)$. Why do we need two base cases?

A) $\Psi(4)$ states that $F_0 + F_1 + F_2 + F_3 = F_5 - 1$, which is true since

$$0 + 1 + 1 + 2 = 4 = 5 - 1.$$

Our base cases are $\Psi(1)$: $F_0 = F_2 - 1$ and $\Psi(2)$: $F_0 + F_1 = F_3 - 1$ which are both true. Assuming $\Psi(k)$, we have

$$F_0 + F_1 + \cdots + F_{k+1} = (F_{k+1} - 1) + F_k + F_{k+1} = F_{k+2} + F_{k+1} - 1 = F_{k+3} - 1$$

which proves $\Psi(k+2)$. This sets up the implication chains

$$\Psi(1) \to \Psi(3) \to \Psi(5) \to \cdots \text{ and } \Psi(2) \to \Psi(4) \to \Psi(6) \to \cdots$$

which is why we needed to prove both $\Psi(1)$ and $\Psi(2)$.

Q69) The Fibonacci numbers have a closed form involving the *golden ratio*. We will prove a related result here. The golden ratio is the irrational value $\varphi = (1+\sqrt{5})/2$. We want to prove the proposition $\Phi(n)$ that $F_n \leq \varphi^n$ for every $n \geq 0$.

a) Prove that $\varphi^2 = 1 + \varphi$.

b) Prove the base cases $\Phi(0)$ and $\Phi(1)$.

c) Prove that $(\Phi(k-1) \wedge \Phi(k)) \to \Phi(k+1)$.

A) We have the identity

$$\varphi^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = 1 + \frac{2+2\sqrt{5}}{4} = 1 + \varphi.$$

We have $F_0 = 0 \leq 1 = \varphi^0$ and $F_1 = 1 \leq \varphi = \varphi^1$. We assume that $F_{k-1} \leq \varphi^{k-1}$ and $F_k \leq \varphi^k$ and we prove the result for $n = k+1$.

$$F_{k+1} = F_{k-1} + F_k \leq \varphi^{k-1} + \varphi^k = \varphi^{k-1}(1+\varphi) = \varphi^{k-1}\varphi^2 = \varphi^{k+1}.$$

Q70) Prove that every integer $n \geq 2$ can be expressed as a product of prime numbers.

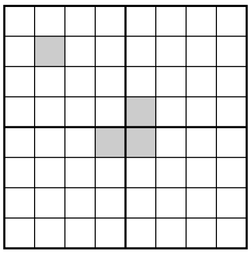
A) We will give a proof by strong induction. Since 2 is prime, the result is true for $n = 2$. We assume the result for every j satisfying $2 \leq j < k$. We now prove the result for k.

If k is already prime, we are done. Otherwise, $k = ab$ for integers a and b which satisfy $a > 1$ and $b > 1$. In particular, $2 \leq a, b < k$ and by our inductive hypotheses a and b can be expressed as products of primes, and hence so can k.

Q71) Consider a grid of size $2^n \times 2^n$ with a single square missing. Prove by induction that you can cover the remaining grid by ▛-shaped tiles.

A) For $n = 1$ we have a 2×2 grid with one square removed, which can be covered by a single ▛-shaped tile.

Now assume we can tile any $2^k \times 2^k$ grid with a single square missing. Consider a $2^{k+1} \times 2^{k+1}$ grid with a single square missing. We break these into four $2^k \times 2^k$ grids. Exactly one of these will have a square missing. We then remove the inner corner from the other three subgrids.



Each of the subgrids has a square missing, which we can tile by our inductive assumption. We then place a final tile to fill in the inner corners.

PROOF BY CONTRADICTION

In a proof by contradiction, we assume that the proposition P we are trying to prove is **false**, and derive a mathematical contradiction, such as the fact that $1 = 0$, or that P is in fact true. We can draw one of two conclusions from this:

- Mathematics has a fundamental error which you just found.
- Your assumption that P was false is incorrect.

We conclude that the second case is more reasonable, so P is true.

Q72) Prove that there are no integer solutions to $24a + 6b = 1$. (Hint: Assume a solution exists, and prove that a or b are not both integers.)

A) Assume an integer solution exists, so a and b are integers such that

$$24a + 6b = 1.$$

Rearranging the equation for b gives

$$b = \frac{1}{6} - 4a.$$

Since a is an integer, so is $-4a$, and hence b is not an integer. This gives a contradiction with the assumption our equation had an integer solution, so we can conclude that our assumption was incorrect.

Q73) Prove that if x is irrational and y is rational, then the sum $x + y$ is always irrational.

A) Assume that $x + y$ is rational. Since y is rational, and the difference of two rational numbers is still rational, we have that

$$(x + y) - y = x$$

is rational. This contradicts that x is irrational, so our assumption is incorrect and $x + y$ is indeed irrational.

For completeness, the reason that the difference between two rational numbers is rational is because we can explicitly write the difference. If a, b, c, d are integers with $b, d \neq 0$, then

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd}.$$

Q74) Prove that there is no triangle whose side lengths are all integers, and whose base side lengths are both odd. (Hint: Does the hypotenuse have even or odd length? Use Pythagoras.)

A) Let a, b be the base lengths and c the hypotenuse. By Pythagoras' theorem, we have the relationship

$$a^2 + b^2 = c^2.$$

Assume for a contradiction that a and b are both odd. Then there exists integers i and j such that $a = 2i + 1$ and $b = 2j + 1$. Since a^2 and b^2 are then odd, $a^2 + b^2$ is even, hence c^2 is even. We can then prove (for example by the contrapositive) that c is even, so $c = 2k$. Hence, we have

$$(2i + 1)^2 + (2j + 1)^2 = (2k)^2$$

which gives

$$4i^2 + 4i + 1 + 4j^2 + 4j + 1 = 4k^2.$$

After dividing by two and rearranging we obtain

$$k^2 - i^2 - i - j^2 - j = \frac{1}{2}$$

which is contradiction, since i, j, k are integers. This completes the proof.

Q75) We recreate Euclid's beautiful proof that there are infinitely many primes.

a) Given integers $p_1, p_2, \ldots, p_n$ with each $p_i \geq 2$, explain why $p_1 p_2 \cdots p_n + 1$ is not divisible by any of the original numbers.

b) Prove that there are infinitely many primes. (Hint: Assume there are only finitely many primes, and that $p_1, \ldots, p_n$ is a complete list.)

A) Take one of the numbers p_i. Then $p_1 \cdots p_n$ is divisible by p_i, so adding one to this number will give something which leaves remainder one when dividing by p_i, so is not divisible by it.

Assume for a contradiction that there are finitely many primes, and $p_1, \ldots, p_n$ is a list of all the primes. Take $p = p_1 \cdots p_n + 1$. This number must have a prime factory by Q70) but it cannot be any of $p_1, \ldots, p_n$, so there must be a prime not in our "complete" list, which gives a contradiction.

Q76) Prove that $\log_2(3)$ is irrational. (Hint: Assume it is rational).

A) Assume that $\log_2(3)$ is rational, so $\log_2(3) = a/b$ for integers a and b. Then we have $3 = 2^{a/b}$ (this is the definition of log), and by taking the b^{th} power on both sides we get $2^a = 3^b$. This gives a contradiction since 2^a is always even, but 3^b is always odd.

Q77) Pick apart the following supposed proof by contradiction, whose claim is that every number bigger than 8 is prime.

> "Assume that there are no primes bigger than 8. But 11 is bigger than 8, and the only divisors of 11 are 1 and itself. Hence, we obtain a contradiction, so the claim is correct."

A) This argument is secretly just a "proof by example" (not a real technique!), which is trying to prove the false statement

$$\forall p((p > 8) \to p \text{ is prime})$$

by proving the true statement

$$\exists p((p > 8) \to p \text{ is prime})$$

by taking $p = 11$. The issue with the proof is that the assumption should be "there exists a number bigger than 8 which is not prime". It will be hard to get a contradiction from this, because this statement is true!

Q78) Consider the following proof by contradiction, which proves that the sum of two even numbers is always even.

> "Assume (for a contradiction) that n and m are even numbers whose sum is odd. Since they are even, $n = 2i$ and $m = 2j$ for some integers i and j, so $n + m = 2(i + j)$ is an even number. This is not odd, which gives a contradiction."

This proof is mathematically valid, but it is not a good proof. Why?

A) The issue with this proof is that the contradiction is entirely unecessarily. Notice that if we remove the first and last sentence, this is a perfectly valid proof of why the sum of two even numbers is even. When doing a contradiction proof, see if you used the assumption $\neg P$ in any real way, or if you are really just doing a direct proof.

Q79) Suppose P, Q R and S are propositions satisfying the following:

1. $(\neg Q \vee R) \to P$
2. $Q \to S$
3. $R \vee \neg S$

Prove P by contradiction.

A) Suppose P is false. By the contrapositive of 1. we have $\neg P \to (Q \wedge \neg R)$ and so Q is true and R is false. We have $Q \to S$, so S is true. We also have that R is false, so $\neg S$ is true by 3. But we have proven $S \wedge \neg S$, which is a contradiction.

HARDER QUESTIONS

Q80) Prove or disprove that if $2^n - 1$ is composite, then n is composite.

A) This is false. The smallest counterexample is $n = 11$, since

$$2^{11} - 1 = 2047 = 23 \times 89$$

is compositive, but n is not composite.

Q81) Prove that the equations

$$Ax + By = U \quad \text{and} \quad Cx + Dy = V$$

have a unique solution if and only if $AD - BC \neq 0$.

A) Since this is an "if and only if", we need to prove both directions. First suppose that $AD - BC \neq 0$. We multiply both equations to give

$$ACx + BCy = UC \quad \text{and} \quad ACx + ADy = AV.$$

Subtracting the second equation from the first gives

$$(AD - BC)y = AV - UC.$$

Since $AD - BC \neq 0$ we can divide by this value to obtain a unique solution for y. Similarly, by multiplying and subtracting to eliminate y we have

$$(AD - BC)x = UD - BV.$$

and again diviing by $AD - BC$ we have a unique solution for x.

Now suppose $AD - BC = 0$. Then if $AV - UC \neq 0$ or $UD - BV \neq 0$, the equation will have no solution. If they are both zero, the equation has infinitely many solutions.

Q82) Prove that every square number leaves a remainder of 0 or 1 when dividing by 4.

A) We can prove this directly by considering two cases. If n is even, then $n = 2k$ where k is an integer so $n^2 = (2k)^2 = 4k^2$ is divisible by 4. If n is odd, then $n = 2k + 1$ where k is an integer so $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1$ which leaves a remainder of 1 when dividing by 4. Since every integer is either even or odd, this covers all cases.

Q83) Suppose x, y are positive real numbers with $x \neq y$. Prove that

$$\frac{x}{y} + \frac{y}{x} > 2.$$

A) Assume for a contradiction that $x/y + y/x \leq 2$. Then multiplying both sides of the equation by xy (which is positive) gives

$$x^2 + y^2 \leq 2xy.$$

Subtracting by $2xy$ and factorising gives

$$(x - y)^2 \leq 0.$$

However, a square number can never be negative, so this gives $(x - y)^2 = 0$, so $x = y$, which contradicts $x \neq y$ as required.

Q84) A function $f : X \to Y$ is *surjective* if every y in Y has an x in X such that $f(x) = y$.

a) Write the statement "f is surjective" using logical symbols.

b) Prove that if $f : X \to Y$ and $g : Y \to Z$ are surjective functions, then the composition $g \circ f : X \to Z$ is also surjective.

c) Prove that the converse is not true. That is, find functions such that $g \circ f$ is surjective, but f and g are not both surjective.

A) For x in X and y in Y, a function f is surjective if

$$\forall y \exists x (f(x) = y).$$

We need to prove that for all $z \in Z$, we can find x in X such that $g(f(x)) = z$. Since g is surjective, we can find y in Y such that $g(y) = z$. Since f is surjective, we can find x in X such that $f(x) = y$. Then $g(f(x)) = g(y) = z$ as required.

Let $\mathbb{Z}$ be the set of integers and $\{0\}$ the set containing only the element 0. Suppose $f : \mathbb{Z} \to \{0\}$ is given by $f(n) = 0$ for every n in $\mathbb{Z}$, and $g : \mathbb{Z} \to \mathbb{Z}$ is given by $g(n) = 2n$. Then $g(f(n)) = g(2n) = 0$ for every n, so the function $g \circ f$ is surjective but g is not. There are many other examples, but you will find that f is always surjective (but g might not be!)

Q85) Suppose we have 100 positive integers $n_1, n_2, \ldots, n_{100}$ such that

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_{100}} = 1.$$

Prove that at least one of the integers is even.

A) Assume by contradiction that all of the integers are odd. Multiplying through by the denominators gives

$$n_2 n_3 \cdots n_{100} + n_1 n_3 \cdots n_{100} + \cdots + n_1 n_2 \cdots n_{99} = n_1 n_2 \cdots n_{100}.$$

Every term is a product of odd numbers, so are all odd. But on the left hand side we have a sum of 100 odd numbers, which is an even number. This is a contradiction with being equal to the right-hand side, which is an odd number.

Q86) Suppose $P(x)$ is a proposition on an infinite set X which satisfies

$$\forall x \forall y((P(x) \wedge P(y)) \to (x = y)).$$

For how many x can $P(x)$ be true?

A) The statement about $P(x)$ proves that $P(x)$ can only be true for at most one element, since the contrapositive to our statement is

$$\forall x \forall y((x \neq y) \to (\neg P(x) \vee \neg P(y)).$$

However, we don't know whether $P(x)$ *has* to be true for any x, so $P(x)$ is true for either zero or one element.

Q87) Suppose $\varrho(n)$ is the proposition "n is prime". There is a famous result of Yitang Zhang proved in 2013 which claims the following:

$$\exists N(N \leq 70,000,000 \wedge \forall n \exists p(p \geq n \wedge \varrho(p) \wedge \varrho(p+N))).$$

What claim is being made? Try to express this as simply as possible.

A) The most direct translation is "there exists a number N, at most 70,000,000, such that for every n, we can find a number p greater than n such that p and $p+N$ are prime."

Recall from Q15) that this is saying the list of such p satisfying this property is infinitely long. Hence, we can rewrite our statement as "for some N at most $70,000,000$, there are infinitely many pairs of primes which differ by N".

If this result is true for $N = 2$ we get the famous twin prime conjecture, which is still unsolved.

Q88) Prove that there do not exist integers m and n such that $2n^2 = m^2$.

A) Assume $2n^2 = m^2$ and let $m = p_1 \cdots p_r$ and $n = q_1 \cdots q_s$ be prime factorisations for n and m. Then m^2 has prime factorisation $p_1^2 \cdots p_r^2$, which has an even number of factors. But $2n^2$ will have an odd number of prime factors (since n^2 has an even number, and 2 is prime), which gives a contradiction with uniqueness of prime decomposition given by the Fundamental Theorem of Arithmetic (which we proved half of in Q70), and the other half can be proved by induction).

Q89) Give a proof by contradiction that $\sqrt{2}$ is an irrational number. (Hint: Use the previous question!)

A) Suppose for a contradiction that $\sqrt{2}$ is rational, and so there are integers m and n such that $\sqrt{2} = m/n$. Then

$$2 = \frac{m^2}{n^2} \implies 2n^2 = m^2$$

which is a contradiction by the previous question.

Q90) Here is a *nonconstructive* existence proof, where we prove an object exists without ever specifically finding it. Our statement will be: there exist irrational numbers a and b such that a^b is rational.

- **a)** Prove the statement under the assumption that $r = \sqrt{2}^{\sqrt{2}}$ is rational.
- **b)** Prove the statement under the assumption that $r = \sqrt{2}^{\sqrt{2}}$ is irrational by considering $r^{\sqrt{2}}$.

A) If $r = \sqrt{2}^{\sqrt{2}}$ is rational, then the statement is true by taking $a = \sqrt{2}$ and $b = \sqrt{2}$. If on the other hand r is irrational, then

$$r^{\sqrt{2}} = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\times\sqrt{2}}\sqrt{2}^{2} = 2$$

is rational, so the statement is true by taking $a = r$ and $b = \sqrt{2}$.

Q91) [Assumes some calculus] A function $f : \mathbb{R} \to \mathbb{R}$ is called *weakly increasing* if

$$\forall x \forall y((x \leq y) \to (f(x) \leq f(y)).$$

Prove that a differentiable function is weakly increasing if and only if $f'(x) \geq 0$ for every x.

A) Suppose the function f is weakly increasing. The derivative is

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h}.$$

If $h \to 0$ from the positive direction, then $f(x+h) - f(x) \geq 0$, hence the limit is also nonnegative and $f'(x) \geq 0$. Conversely, suppose $f'(x) \geq 0$ for every x. Then for $x \leq y$ by the Fundamental Theorem of Calculus we have

$$f(y) - f(x) = \int_x^y f'(t)\,\mathrm{d}t \geq 0$$

and hence $f(x) \leq f(y)$.

Q92) Consider a line of 9 people. A *descent* is a pair of adjacent people where the shorter person is on the right. An *inversion* is a pair of people (not necessarily adjacent) with the shorter person on the right.

- **a)** Prove there are no inversions if and only if there are no descents.
- **b)** Is there exactly one inversion if and only if there is exactly one descent? Prove your claim.

A) Every descent is an inversion (amongst adjacent positions), so no inversions implies no descents by the contrapositive. If there are no descents, then we can argue by induction that everybody must be in height order. For $n = 1$ people this is trivial, and for $n = k + 1$ the tallest person must be on the right (otherwise there is a descent with the person on the right), and by the inductive hypothesis the remaining k people are in height order.

The claim is not true. Labelling people $1, 2, \ldots, 9$ by their height order, standing them in the order 6 7 8 9 1 2 3 4 5 has exactly one descent, but twenty inversions.

Q93) Suppose X is a set with a binary operation $\oplus$, meaning for every x and y in X, we are given an element $x \oplus y$ in X. Also suppose ι is a specific element such that $x \oplus \iota = x$ and $\iota \oplus x = x$ for every x. Prove that only one element in X can satisfy this property.

A) Suppose that ι' is an element in X satisfying the same property as ι. We want to show that in fact $\iota' = \iota$. Using the property for ι and then ι' we have $\iota = \iota \oplus \iota' = \iota'$.

Q94) What's the largest integer n which can't be written as $n = a + b$, where $a, b \geq 2$ are composite numbers? Prove your claim. (Hint: Consider $a = 4, 6, 8$.)

A) We claim that the answer is 11. We can sum to 11 with

$$2 + 9 \qquad 3 + 8 \qquad 4 + 7 \qquad 5 + 6$$

and in all of these one of them is prime. We now prove for $n \geq 12$ that this is possible. Consider the numbers $n - 4$, $n - 6$ and $n - 8$. When looking at the remainder after dividing by 3, we have

$$-4 \to 2 \qquad -6 \to 0 \qquad -8 \to 1$$

and so at least one of them is divisible by 3, since all possible remainders are covered. Moreover, $n - 8 > 3$ and hence one of the sums

$$4 + (n - 4) \qquad 6 + (n - 6) \qquad 8 + (n - 8)$$

is a sum of composite numbers bigger than 3.

Q95) The *probabilistic method* is another technique for nonconstructive proofs. Many of the proofs are quite advanced, but here is a silly one. We prove the following: if you paint 90% of a sphere red and paint the remaining 10% blue, you can always can fit a cube inside the sphere whose corners are all red.

a) Place a cube randomly inside the sphere, with the vertices lying on the sphere. What is the probability that a given vertex of the cube will be on the red part of the sphere?

b) Find the expected number of red corners.

c) Hence, explain why *some* cube has all red corners.

A) Because the cube is placed randomly, there is a 90% chance one of the corners is painted red. This is true for all corners, so the expected number of red corners is $8 \times 90\% = 7.3$.

Now assume by contradiction that no orientation of the cube has all red corners. Then the number of red corners is ≤ 7 for all orientations, so the expected value of the number of red corners will also be at most 7. This contradicts our above calculation.

Q96) Prove the AM–GM inequality: for positive real numbers $x_1, \ldots, x_n$ for $n \geq 1$:

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n}.$$

(Hint: Consider the implications from Q64).)

A) Let $P(n)$ be the statement for n variables. We first prove the claim for $n = 2$. Since $(\sqrt{x_1} - \sqrt{x_2})^2 \geq 0$, we have

$$x_1 - 2\sqrt{x_1}\sqrt{x_2} + x_2 \geq 0 \implies \frac{x_1 + x_2}{2} \geq \sqrt{x_1 x_2}.$$

Now we prove that $P(2) \wedge P(n) \to P(2n)$ by applying $P(n)$ on the first n and last n terms, which gives

$$\begin{aligned}\frac{x_1 + \cdots + x_{2n}}{2n} &= \frac{1}{2}\left(\frac{x_1 + \cdots + x_n}{n} + \frac{x_{n+1} + \cdots + x_{2n}}{n}\right) \\ &\geq \frac{1}{2}\left(\sqrt[n]{x_1 \cdots x_n} + \sqrt[n]{x_{n+1} \cdots x_{2n}}\right) \\ &\geq \sqrt{\sqrt[n]{x_1 \cdots x_n}\,\sqrt[n]{x_{n+1} \cdots x_{2n}}} \\ &\geq \sqrt[2n]{x_1 \cdots x_n x_{n+1} \cdots x_{2n}}\end{aligned}$$

as required. Finally we prove that $P(n) \to P(n-1)$ by setting x_n to be the mean of the first $n-1$ elements. Set

$$\mu = \frac{x_1 + \cdots + x_{n-1}}{n-1}.$$

Then we have

$$\mu = \frac{x_1 + \cdots + x_{n-1} + \mu}{n} \geq \sqrt[n]{x_1 \cdots x_{n-1}\mu}.$$

Then taking n^{th} powers and dividing by μ gives

$$\mu^{n-1} \geq x_1 \cdots x_{n-1} \implies \mu \geq \sqrt[n-1]{x_1 \cdots x_{n-1}}.$$

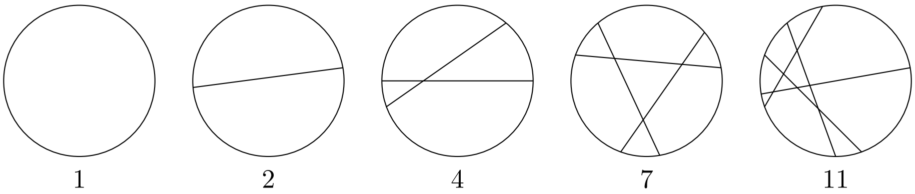
Q97) A foreign currency has bank notes of only \$4 and \$5. Prove that you can pay any dollar amount of at least \$12 with only these types of notes.

A) Note that we cannot make \$11. We prove the claim for $n \geq 12$ by induction. The base case is proven by \$12 = \$4 + \$4 + \$4. Assume we can make k, and we want to make $k + 1$.

If k can be made using a \$4, then we can replace this with a \$5. Otherwise, k is made of only \$5 notes, so is a multiple of 5. Since $k \geq 12$, there are at least three \$5 notes, and we can replace these with four \$4 notes to increase the amount by a dollar.

Q98) By drawing 3 chords through a circle, you can split the circle into a maximum of 7 regions. For $0 \leq n \leq 4$, find the maximum number of regions which the circle can be split into by drawing n chords. Find a general formula and prove it by induction.

A) The number of regions is given by the following:



We need to think about how many regions will be created by adding a new line. The region in which the line starts adds a new region, and it crosses each other line to make a new region. Hence, if $R(n)$ is the number of region after n lines, we have $R(0) = 1$ and $R(1) = R(n-1) + n$ for $n \geq 1$.

Hence, we guess that the formula is

$$R(n) = 1 + 1 + 2 + 3 + 4 + \cdots + n = 1 + \frac{n(n+1)}{2} = \frac{1}{2}(n^2 + n + 2).$$

We prove this by induction. For $n = 1$ we get $R(1) = 2$ as required. Assume the formula for $n = k$, and then

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

as required.

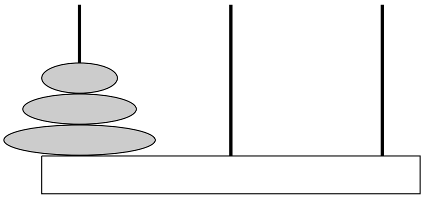
Q99) Recall the Fibonacci numbers from Q68). Prove that every positive integer can be written as a sum of distinct Fibonacci numbers.

A) We prove this by induction for every $n > 4$, since the cases $1 \leq n \leq 4$ can be done explicitly. Assume by induction we can express any $1 \leq k < n$ as a sum of distinct Fibonacci numbers. We prove the result for n using this (strong) inductive assumption.

Suppose F_j is the largest Fibonacci number such that $F_j \leq n$. Take $k = n - F_j$, which can be written as a sum of distinct Fibonacci numbers by our assumption. Also, $k = n - F_j < F_{j+1} - F_j = F_{j-1} < F_j$, so k does not contain F_j in its sum, and adding it gives n as required. The reason we assumed $n > 4$ is to have $F_{j-1} < F_j < F_{j+1}$.

In fact, you can prove that every positive integer has a *unique* representation as a sum of distinct Fibonacci numbers, known as Zeckendorf's theorem.

Q100) In this question we find an optimal solution for the Towers of Hanoi puzzle. Consider three poles, the first of which has n stones, stacked from largest to smallest. We want to move these stones to the third pole. We can only move one disc at a time, and we can never have a larger stone on top of a smaller one.



Find the minimum number of moves needed to transfer all stones onto the third pole when there are n stones for $n \leq 4$. Guess a formula, and give a proof by induction that your solution is optimal.

A) We can solve this puzzle inductively, where $T(n)$ is the optimal number of moves for n stones. At some point we have to move the bottom stone, which first requires the other $n-1$ stones to a single other pole, taking $T(n-1)$ moves. After that, the quickest solution must be to make a single move of the biggest stone to the third pole, and moving the stack of $n-1$ stones back on top of it. Hence, we have $T(1) = 1$ and $T(n) = 2T(n-1) + 1$.

This gives the optimal sequence of moves

n	1	2	3	4	5	6
$T(n)$	1	3	7	15	31	63

Hence, we guess that $T(n) = 2^n - 1$. For $n = 1$ the statement is true, and for $n = k$ we assume that $T(k) = 2^k - 1$. Then

$$T(k+1) = 2T(k) + 1 = 2(2^k - 1) + 1 = 2^{k+1} - 2 + 1 = 2^{k+1} - 1.$$