Proving Things

1 Logic

1. Suppose that all ravens are black. Which of the following statements are then true?

   (a) **If X is a raven, then X is black.**
   (b) If X is black, then X is a raven.
   (c) If X is not a raven, then X is not black.
   (d) **If X is not black, then X is not a raven.**

2. All humans are mortal, for that is the way of life. All mortals are afraid of bees, for their sting is deadly. Suppose Sif is immortal. Which of the following *must* be true?

   (a) **Sif is not a human.**
   (b) Sif is not afraid of bees.
   (c) Sif is afraid of bees.
   (d) **All humans are afraid of bees.**

3. Mr. Mersenne claims that if p is a prime number, then $2^p - 1$ will also be a prime number. For each of the following observations, decide whether the observation supports the claim, refutes the claim, or is irrelevant to the claim.

   (a) $2^7 - 1 = 127$, which is prime. **SUPPORTS**
   (b) 12 is not prime, and is not of the form $2^p - 1$. **IRRELEVANT**
   (c) $2^1 1 - 1 = 23 * 89$, and so is not prime. **REFUTES**
   (d) 19 is prime, but is not of the form $2^p - 1$. **IRRELEVANT**

4. The statement "If A is true, then B is true" may be written as $A \Rightarrow B$ for short. Likewise, "If B is true, then A is true" may be written as $A \Leftarrow B$ (or $B \Rightarrow A$). If both of these statements are true, then we can write $A \Leftrightarrow B$. Draw the appropriate arrow to describe the relation between each pair of statements below.

$$\begin{array}{ccc} x^2 = y^2 & \Leftarrow & x = y \\ 3x = 15 & \Leftrightarrow & x = 5 \\ x \text{ is prime} & () & x \text{ is odd} \\ x = \pi & \Rightarrow & x \text{ is irrational} \end{array}$$

1.1 The Island of Knights and Knaves (and sometimes werewolves)

Adapted from puzzles by Raymond Smullyan
Welcome to the island of Knights and Knaves. Knights are virtuous and always tell the truth, while knaves are wicked and always lie. You cannot tell which is which just by looking, so you'll have to keep your wits about you so as not to be misled.

1. You come across a single person along the road, who tell you:

   A: I am a knight.

   Can you tell from this statement whether the person is a knight or a knave?

   No. Either a knight or a knave could make this statement.

2. Now you come across two people. One of them tells you:

   A: We are both knaves.

   What can you deduce about the two travelers?

   If A were a knight, then his statement would imply that he is a knave, which is impossible. Thus A is a knave, and his statement is false. If his statement is false then he and his partner are not both knaves. Since A is a knave, his partner must be a knight.

3. This time you come across three people, who say the following:

   A: Exactly one of us is a knave.

   B: Exactly two of us are knaves.

   C: All three of us are knaves.

   What can you deduce about the three people?

   The three statments contradict each other, so at least two of the statements must be false; thus there are either 2 or 3 knaves. If there are 3 knaves, then C's statement would be true, contradicting the fact that he is a knave. Thus there must be exactly 2 knaves, with B as the lone knight.

4. Werewolves can be either knights or knaves, but they are also werewolves. You must choose a travel partner from among three people (exactly one of which is a werewolf), and you would rather not travel with the werewolf. The three people tell you the following:

   A: I am not the werewolf.

   B: The werewolf is a knave.

   C: All three of us are knaves.

   Is the werewolf a knight or a knave? Can you tell from this information alone who the werewolf is?

   C must be a knave, so the travelers are not all knaves. Thus either A or B (or both) is a knight. If both are knights, then B's statement means that C must be the werewolf. If A is a knave, then his statement implies that he is the werewolf, fitting with (the knight) B's statement that the werewolf is a knave.

   Assuming that A is a knight and B is a knave leads to a contradiction. Thus the werewolf is a knave, but could be either A or C.

5. Suppose now that A also says, "C is a knave." Now can you tell who the werewolf is?

   We know that C is a knave, so this shows that A is a knight. Assuming B is a knave leads to a logical contradiction, and so B must be a knight as well. Thus C is the werewolf.

6. A man is on trial for stealing an elephant. In his defense he states, "I am either an innocent knight or a guilty knave." Can you tell whether he is innocent or guilty? Can you tell whether he is a knight or a knave?

   If he is a knight, then his statement shows that he is innocent. If he is a knave, then he is not a guilty knave (since his statement is false), and so again must be innocent. Thus the man is innocent, but could be either a knight or a knave.

1.2 Funny Joke

Three logicians walk into a bar. The bartender asks them, "Do all of you want a drink?" The first says, "I don't know." The second says, "I don't know." The third says, "Yes."

2 Proofs by Algebra

Adapted from 'Elementary Number Theory in Nine Chapters', by James Tattersall
Given: For any real number r, $r^2 \geq 0$, and $r^2 = 0$ only if $r = 0$.

1. Prove: $x^2 + 2x + 1 = -1$ has no real solutions. (Do not use the quadratic formula!)

   $x^2 + 2x + 1 = (x+1)^2 \geq 0 > -1$ *for all* x*, and so* $x^2 + 2x + 1 \neq -1$.

2. Prove: $x^2 - 2x = -1$ has exactly one solution.

$$\begin{aligned} x^2 - 2x &= -1 \\ x^2 - 2x + 1 &= 0 \\ (x-1)^2 &= 0 \\ x - 1 &= 0 \\ x &= 1 \end{aligned}$$

3. Call a number x *even* if we can write $x = 2n$ for some integer n. Call x *odd* if we can write $x = 2n + 1$ for some integer n.

   (Example) Prove: If x is even and y is even, then $x + y$ is even.

   Proof: $x = 2n$ *and* $y = 2m$ *for some integers* n, m *so* $x + y = 2n + 2m = 2(n + m)$.

4. Prove that if x is even and y is odd, then $x + y$ is odd.

   Let $x = 2n, y = 2m + 1$. *Then* $x + y = 2n + (2m + 1) = 2(n + m) + 1$*, and so is odd.*

5. Prove that if x is odd and y is odd, then $x + y$ is even.

   Let $x = 2n + 1, y = 2m + 1$. *Then* $x + y = 2n + 1 + 2m + 1 = 2(n + m + 1)$*, and so is even.*

6. Prove: even * even = even, even * odd = even, odd * odd = odd.

$$(2n)(2m) = 4nm = 2(2mn) = \textit{even}$$

$$(2n)(2m+1) = 4nm + 2n = 2(2nm + n) = \textit{even}$$

$$(2n+1)(2m+1) = 4nm + 2n + 2m + 1 = 2(2nm + n + m) + 1 = \textit{odd}$$

7. Call $T_n = 1 + 2 + \ldots + n$ the n-th *triangular number*. One well-known formula for triangular numbers is $T_n = n(n+1)/2$. Prove: $T_n + T_{n+1}$ is a square number.

$$\begin{aligned} T_n + T_{n+1} &= \frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} \\ &= \frac{(n+1)(n+n+2)}{2} \\ &= \frac{(n+1)(2n+2)}{2} \\ &= (n+1)^2 \end{aligned}$$

8. Prove: $9T_n + 1$ is also a triangular number.

$$\begin{aligned} 9T_n + 1 &= 9\frac{n(n+1)}{2} + 1 \\ &= \frac{9n^2 + 9^n + 2}{2} \\ &= \frac{(3n+1)(3n+2)}{2} \\ &= T_{3n+1} \end{aligned}$$

9. Prove: $T_{n+1}^2 - T_n^2$ is a perfect cube.

$$\begin{aligned} T_{n+1}^2 - T_n^2 &= \frac{(n+1)^2(n+2)^2}{4} - \frac{n^2(n+1)^2}{4} \\ &= \frac{(n+1)^2[(n+2)^2 - n^2]}{4} \\ &= \frac{(n+1)^2(4n+4)}{4} \\ &= (n+1)^3 \end{aligned}$$

10. Show that $n(n+1)(n+2)(n+3)+1$ is always a square number (for n an integer).

$$\begin{aligned} n(n+1)(n+2)(n+3)+1 &= (n^2+n)(n^2+5n+6)+1 \\ &= n^4 + 6n^3 + 11n^2 + 6n + 1 \\ &= (n^2+3n+1)^2 \end{aligned}$$

11. Prove the *aritmetic-geometric mean inequality*: if $x, y \geq 0$, then $(x+y)/2 \geq \sqrt{xy}$. (Hint: work backwards from the desired result, then check that your logic holds in the forward direction.)

$$(x+y)/2 \geq \sqrt{xy} \tag{1}$$
$$(x+y) \geq 2\sqrt{xy} \tag{2}$$
$$x^2 + 2xy + y^2 \geq 4xy \tag{3}$$
$$x^2 - 2xy + y^2 \geq 0 \tag{4}$$
$$(x-y)^2 \geq 0 \tag{5}$$

The final statement is true. Looking at the chain of logic, we see that (5) $\Leftrightarrow$ (4) $\Leftrightarrow$ (3) $\Leftarrow$ (2) $\Leftrightarrow$ (1), so the problematic step in asserting (5) $\Rightarrow$ (1) is the step from (3) to (2), which is the assertion that if $a^2 = b^2$ then $a = b$. We would normally only be able to conclude that $a = \pm b$, but since we have the requirement that $x, y \geq 0$, we can conclude that (3) $\Rightarrow$ (2). Therefore the chain of logic works in reverse, and our proof is complete.

3 Functions

Call a function f 1-1 if $x \neq y \Rightarrow f(x) \neq f(y)$ (alternatively, $f(x) = f(y) \Rightarrow x = y$). Call a function *increasing* if $x > y \Rightarrow f(x) > f(y)$. A functions f is *even* if $f(-x) = f(x)$ for all x, and *odd* if $f(-x) = -f(x)$.
Prove the following statements:

1. If f is increasing, then f is 1-1 (thus f^{-1} exists).

   Let $x \neq y$, so either $x > y$ or $y > x$. If $x > y$, then $f(x) > f(y)$ and so $f(x) \neq f(y)$. Similarly, $y > x \Rightarrow f(y) > f(x) \Rightarrow f(y) \neq f(x)$. Thus if f is increasing then f is 1-1.

2. If f is 1-1, then f^{-1} is also 1-1.

   If $a \neq b$, then we want to show that $f^{-1}(a) \neq f^{-1}(b)$. Since $a = f(x), b = f(y)$ for some y, this amounts to showing that if $f(x) \neq f(y)$, then $x \neq y$. Looking at the contrapositive of the statement, this is the same as showing that if $x = y$ then $f(x) = f(y)$, which is true of all functions. Thus f^{-1} is 1-1.

3. If f and g are increasing, then $f + g$ is increasing.

   If $x > y$ then $f(x) > f(y), g(x) > g(y)$, and so $(f+g)(x) = f(x)+g(x) > f(y)+g(y) > (f+g)(y)$, so $f + g$ is increasing.

4. If f and g are increasing, then $f \circ g$ is increasing.

   $x > y \Rightarrow g(x) > g(y) \Rightarrow f(g(x)) > f(g(y))$.

5. If f and g are increasing, then $f \cdot g$ is not necessarily increasing (Give a counterexample).

   Let $f(x) = g(x) = x$. Then $(f \cdot g)(x) = x^2$, which is not increasing in general.

6. If f and g are 1-1, then $f \circ g$ is 1-1.

   $x \neq y \Rightarrow g(x) \neq g(y) \Rightarrow f(g(x)) \neq f(g(y))$.

   Alternately, $f(g(x)) = f(g(y)) \Rightarrow g(x) = g(y) \Rightarrow x = y$.

7. If f is odd and g is even, then $g \circ f$ is even.

   $(g \circ f)(-x) = g(f(-x)) = g(-f(x)) = g(f(x)) = (g \circ f)(x)$.

8. If f is odd and g is odd, then $g \circ f$ is odd, but $g \cdot f$ is even.

   $g(f(-x)) = g(-f(x)) = -g(f(x))$, so $g \circ f$ is odd.

   $g(-x)f(-x) = (-g(x))(-f(x)) = g(x)f(x)$, so $g \cdot f$ is even.

9. If f is odd and f^{-1} exists, then f^{-1} is also odd.

   Say $f^{-1}(x) = a$, so $f(a) = x$. Then $f^{-1}(-x) = f^{-1}(-f(a)) = f^{-1}(f(-a)) = -a$, so f^{-1} is odd.

10. If f is increasing, then $f(x) > f(y) \Rightarrow x > y$ (Hint: for any x and y either $x > y, x < y$ or $x = y$).

    Let $f(x) > f(y)$. We have three possibilities: $x < y, x = y$, or $x > y$. If $x < y$ then $f(x) < f(y)$, which is a contradiction. $x = y$ is equally impossible, so the only option left is $x > y$.

11. If f is increasing, then f^{-1} is also increasing (Hint: use the result from the previous question).

    Let $a > b$, where $a = f(x), b = f(y)$ (equivalently, $f^{-1}(a) = x, f^{-1}(b) = y$). The previous result gives that $x > y$, and so $f^{-1}(a) > f^{-1}(b)$. Thus f^{-1} is increasing.

12. Call a function g *decreasing* if $x > y \Rightarrow g(x) < g(y)$. If f is increasing and g is decreasing, is $f \circ g$ increasing, decreasing, or neither? What about $g \circ f$ and $g \circ g$?

    $x > y \Rightarrow g(x) < g(y) \Rightarrow f(g(x)) < f(g(y))$, so $f \circ g$ is decreasing.

    $x > y \Rightarrow f(x) > f(y) \Rightarrow g(f(x)) < g(f(y))$, so $g \circ f$ is also decreasing.

    $x > y \Rightarrow g(x) < g(y) \Rightarrow g(g(x)) > g(g(y))$, so $g \circ g$ is increasing.

13. If f is increasing, show that $g(x) = f(-x)$ is decreasing (1) directly, and (2) by applying a result from the previous problem.

    $x > y \Rightarrow -x < -y \Rightarrow f(-x) < f(-y) \Rightarrow g(x) < g(y)$, so g is decreasing.

    Alternately, $h(x) = -x$ is decreasing, so $g = f \circ h$ is also decreasing.

3.1 From Lectures and Homework

1. Find the formulas for $\cos(\sin^{-1}(x)), \tan(\sin^{-1}(x)), \sin(\cos^{-1}(x)), \tan(\cos^{-1}(x)), \sin(\tan^{-1}(x))$, and $\cos(\tan^{-1}(x))$. Draw triangles.

2. Suppose we decide in advance that we want all exponentiation to obey the rule $a^{x+y} = a^x \cdot a^y$. Why does this force $a^0 = 1$? Why does this force $a^{-x} = 1/a^x$?

   $a^0 \cdot a^n = a^{0+n} = a^n$, so $a^0 = 1$.

   $a^{-x} \cdot a^x = a^{-x+x} = a^0 = 1$, so $a^{-x} = 1/a^x$.

   Similarly, $a^1 = a$ is a result of the rule $(a^x)^y = a^{xy}$ because $(a^1)^n = a^{1\cdot n} = a^n$ for all n, so $a^1 = a$.

3. Define $\ln(x)$ as the inverse of e^x, so that $x = \ln(e^x)$, $e^{\ln(x)} = x$ (for $x > 0$), and $\ln(x) = a \Leftrightarrow e^a = x$. Prove that $\ln(xy) = \ln(x) + \ln(y)$, $\ln(x/y) = \ln(x) - \ln(y)$, and $\ln(x^r) = r\ln(x)$.

   See the other packet, "Summary of Proofs for Logs and Exponents."

4 Bootstrapping

Once we prove that some relation holds for two numbers/functions/etc., we can use previous results to more easily work our way up to larger cases.

1. (Example) Prove that odd + odd + odd = odd.

   Proof: *We know that odd + odd = even and odd + even = odd.*

   Therefore, odd + (odd + odd) = odd + even = odd.

2. If f, g, and h are 1-1, prove that $f \circ g \circ h$ is 1-1.

   Let $k = g \circ h$. k is 1-1, so $f \circ g \circ h = f \circ k$ is 1-1.

3. If f, g, h are increasing, prove that $f \circ g \circ f \circ h \circ g$ is increasing.

   $inc \circ inc \circ inc \circ (inc \circ inc) = inc \circ inc \circ (inc \circ inc) = inc \circ (inc \circ inc) = inc \circ inc = inc.$

4. If $(fg)' = f'g + fg'$, find a formula for $(fgh)'$.

   Let $k = gh$. Then $(fgh)' = (fk)' = f'k + fk' = f'gh + f(gh)' = f'gh + f(g'h + gh') = f'gh + fg'h + fgh'$.

5 Proof by Contradiction

"Once you eliminate the impossible, whatever remains, however improbable, must be the truth." -Sherlock Holmes

1. Prove that $\log_2 5$ is irrational. Do this by assuming that it is rational, and show that the assumption leads to a contradiction.

   Suppose that $\log_2 5 = a/b$. Then $2^{a/b} = 5$, so $2^a = 5^b$. This is impossible since 2^a is even and 5^b is odd, thus our assumption that a/b existed was false.

2. Prove that $\sqrt{2}$ is irrational.

   Suppose that $\sqrt{2} = a/b$. Since a/b is a fraction, we can reduce it to lowest terms, and so can assume that a and b have no common factor. Then $a^2/b^2 = 2$, so $a^2 = 2b^2$.

   This implies that a is even, so say $a = 2n$. Then $2b^2 = (2n)^2 = 4n^2$, so $b^2 = 2n^2$. This now implies that b is even, which contradicts our assumption that a and b had no common factor. Therefore no such fraction a/b exists.