Direct Proofs

These are usually the simplest kinds of proofs; we want to show that one statement implies another (i.e. $p \to q$).

1. Show that any positive integer divisible by 4 can be written as a difference of two squares. (e.g. $20 = 5 * 4 = 6^2 - 4^2$) Write the above problem in the form of $p \to q$, then prove it.

   Let $P(x)$ be "$(x > 0) \wedge (4 \mid x)$." (The notation $4 \mid x$ means x is divisible by 4.) Let $Q(x)$ be $''\exists a \exists b (x = a^2 - b^2)$.

   Proof: One way to get started is to do a few more examples. Try: $16 = 4 * 4 = 5^2 - 3^2$, $12 = 3 * 4 = 4^2 - 2^2$, etc. Hopefully, after these, or a few more examples, you might guess the solution $x = 4k = (k+1)^2 - (k-1)^2$. To verify this guess, expand the right side: $(k+1)^2 - (k-1)^2 = k^2 + 2k + 1 - (k^2 - 2k + 1) = 4k$.

   Another proof: $x = 4k = 2 * 2k = (k+1-(k-1))(k+1+(k-1)) = (k+1)^2 - (k-1)^2$

2. A rational number (an element of $\mathbb{Q}$), is a number of the form $\frac{a}{b}$ where a and b are integers and $b \neq 0$. Prove that the sum of two rational numbers is another rational number. (State the problem in the form $p \to q$.)

   Let $P(x, y)$ be "$(x \in \mathbb{Q}) \wedge (y \in \mathbb{Q})$." Let $Q(x, y)$ be "$x + y \in \mathbb{Q}$."

   Proof: If $x = \frac{a}{b}$ and $y = \frac{c}{d}$, then $x + y = \frac{ad+bc}{bd}$.

Proof by Contraposition

Often times, in order to show $p \to q$, it will be easier to prove $\neg q \to \neg p$, the contrapositive. This works because $p \to q \equiv \neg q \to \neg p$. The purpose of this technique is often to get a starting situation to work with.

1. Let x, y be two integers. Suppose $x^2(y^2 - 2y)$ is odd. Prove that x and y are odd. State the contrapositive, and then prove it.

   The contrapositive is: If x or y is even, then $x^2(y^2 - 2y)$ is even.

   Proof: If $x = 2c$, then $x^2(y^2 - 2y) = (2c)^2(y^2 - 2y) = 4c^2(y^2 - 2y)$. This is even because it is divisible by 2, since 2 divides 4.

   If $y = 2c$, then $x^2(y^2 - 2y) = x^2((2c)^2 - 2(2c)) = x^2(4c^2 - 4c) = 4x^2(c^2 - c)$. This is even because it is divisible by 2, since 2 divides 4.

2. Let x and y be integers. Suppose xy is not divisible by 5. Then show that x and y are not divisible by 5. As before, state the contrapositive and prove it.

   The contrapositive is: If x or y is divisible by 5, then xy is divisible by 5.

   Proof: (Note: in this case, we could say "without loss of generality, let x be divisible by 5" because the roles of x and y in this problem are symmetric.) If $x = 5c$, then $xy = 5cy$ is divisible by 5. If $y = 5c$, then $xy = 5cx$ is divisible by 5.

Proof by Contradiction

Sometimes, when the above techniques fail, it can be useful to assume that q is false. Then derive a contradictionusing the starting information (p) and the assumption ($\neg q$). This means that your assumption could not have been true.

1. Show that $\sqrt[3]{2}$ is irrational.

   Suppose $\sqrt[3]{2}$ is rational, so $\sqrt[3]{2} = \frac{a}{b}$ for integers a, b with no common factors. Then cube both sides, so $2 = \frac{a^3}{b^3}$, and thus $2b^3 = a^3$. Thus a is even (since a^3 is divisible by 2). Let $a = 2c$. Then $a^3 = 8c^3$. Then we have $2b^3 = 8c^3 \implies b^3 = 4c^3$. Thus b is even (since b^3 is divisible by 2). But if a and b are both even, then they have 2 as a common factor, contradicting our assumption.

2. Let x, y be positive integers. Show that $x^2 - y^2 \neq 1$.

   Suppose $x^2 - y^2 = 1$. Factor the left side: $(x + y)(x - y) = 1$. Since x and y are both positive, then $x \geq 1$ and $y \geq 1$, so $x + y \geq 2$. Divide both sides by $x + y$, and then we get $(x - y) = \frac{1}{x+y}$. However, the left side is an integer, but the right side is not an integer (since $x + y > 1$), so this is a contradiction.

Proofs of Equivalence

To prove statements of the form $p \leftrightarrow q$, you must show both $p \to q$ (the statement) and $q \to p$ (the converse).

State the converses of the statements on the previous side. Are any of them true?

Direct Proofs:

1. The converse is: "if an integer can be written as a difference of two squares, then it is divisible by 4." This is false. $3 = 2^2 - 1^2 = 4 - 1 = 3$, but 3 is not divisible by 4.

2. The converse is: "if the sum of two numbers is rational, then both of those numbers must be rational." This is false. $\frac{1}{2} + \pi$ and $-\pi$ are not rational, but their sum is $\frac{1}{2}$ which is rational.

Contraposition:

1. The converse is: if x and y are odd, then so is $x^2(y^2 - 2y)$. This is true. Let $x = 2k+1$ and $y = 2l+1$. Then $(2k+1)^2((2l+1)^2-2(2l+1)) = (4k^2+4k+1)(4l^2-1)$. Expanding gives: $(4k^2 + 4k + 1)(4l^2 - 1) = (16k^2l^2 - 4k^2 + 14kl^2 - 4k + 4l^2) - 1$. The first number is even and -1 is odd, so this is not divisible by 2.

2. The converse is: if x, y are not divisible by 5, then xy is not divisible by 5. This is true. We don't have the tools to prove this yet, but this is a consequence of prime factorizations.

Proof by cases

It is often useful to break up a problem into cases to give yourself more structure.

1. Let n be a positive integer. Prove that if the remainder when dividing n by 3 is 2, that n is not a square.

   Proof: Work with the contrapositive: If n is a square, then the remainder when dividing n by 3 is not 2. First, since n is a square, write $n = k^2$. Consider the following:

   $k = 3l$: $n = k^2 = (3l)^2 = 9l^2$ is divisible by 3.

   $k = 3l + 1$: $n = k^2 = (3l + 1)^2 = 9l^2 + 6l + 1$ has remainder 1 when divided by 3

   $k = 3l + 2$: $n = k^2 = (3l + 2)^2 = 9l^2 + 12l + 4$ has remainder 1 when divided by 3.

   (Why are these three cases enough?)

   These cases are enough because the only possible remainders when performing division by 3 are $0, 1, 2$.