Chris Hunt DP3 MTH231

3.2 Proofs

Proofs require foundational techniques.

Ex. Theorem: There are infinitely many primes

Proof by Contradiction

Proof. Suppose this were not the case. That is suppose there are only finitely many primes. Then there must be a last, largest prime, call it p. Consider the number:

$$N = p! + 1 = (p \cdot (p-1) \cdots 3 \cdot 2 \cdot 1) + 1$$

Now N is certainly larger than p. Also, N is not divisible by any number less than or equal to p, since every number less than or equal to p divides p!. Thus the prime factorization of N contains prime numbers (possibly just N itself) all greater than p. So p is not the largest prime, a contradiction. Therefore there are infinitely many primes.

- Direct Proof →

- useful when proving implications.

Assume P. Explain, explain, ..., explain. Therefore Q.

$\forall x (P(x) \to Q(x))$: Assume $P(x)$ is true and deduce $Q(x)$
Fix x to be an arbitrary element.

$\forall x \in \mathbb{Z} (P(x) \to Q(x))$ $P(x)$: x is even $Q(x)$: x^2 is even

Assume x is even we can rewrite x as 2y, where y is any integer. $x^2 = x \cdot x = 2y \cdot 2y = 2(2y \cdot y)$. Since any integer multiplied by two is even. We can conclude that if $P(x)$, then $Q(x)$ is true for all cases.

$\forall x, y, z \in \mathbb{Z} (P(x,y,z) \to Q(x,z))$ $P(x)$: $x|y \wedge y|z$ $Q(x)$: $x|z$

Let x, y, z be integers. Assume $x|y$ and $y|z$

3.2 Proofs

- Proof by contrapositive

Since $P \to Q \equiv \neg Q \to \neg P$ if we can prove the contrapositive we can prove the original implication.

Assume $\neg Q$ .... therefore $\neg P$

– $\forall x \in \mathbb{Z}(P(x) \to Q(x))$ $P(x) = x^2$ is even $Q(x) = x$ is even

Prove $\forall x \in \mathbb{Z}(\neg Q \to \neg P)$

Assume x is odd. We can rewrite x as $2k+1$ where k is any integer in $\mathbb{Z}$. Squaring x gives us:

$$x^2 = (2k+1)^2 = (2k+1)(2k+1) = 4k^2 + 4k + 1$$

$$4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Since k is an integer we know $2k^2 + 2k$ is an integer.
Since For all integers $2(\text{integer}) + 1$ is odd. The statement
$P(x) \to Q(x)$ is true

- Proof by Contradiction

If you can prove the negation of a statement is False then you prove the statement as true.

Prove that $\sqrt{2}$ is irrational

$P = \sqrt{2}$ is irrational
$\neg P = \sqrt{2}$ is rational

Suppose not. Then $\sqrt{2}$ is rational so it equals some value $\frac{a}{b}$, assume a/b is in lowest terms.

$$2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} \to 2b^2 = a^2$$

Thus a^2 is even. so $a = 2k$ For some int k and $a^2 = 4k^2$.

$$2b^2 = 4k^2 \to b^2 = 2k^2$$

Thus b^2 is even, and as such b is even. Since a is also even, we see that a/b is not in lowest terms, a contradiction. Thus $\sqrt{2}$ is irrational

Chris Hurst DP3 MTH231

3.2 Proofs

- Proof by (counter) example

It is almost never okay to prove a statement with just an example

YOU CANNOT PROVE A STATEMENT OF THE FORM $\forall x P(x)$ WITH AN EXAMPLE

However existential statements can be!

- Proof by case

Used when proving a statement by considering multiple cases

Break the problem into cases $(P1, P2, \ldots, Pn)$ Prove the statement for each case

For any integer n, the number $(n^3 - n)$ is even

$P(x) = (x^3 - x)$ is even

$\forall x \in \mathbb{Z}(P(x))$ → There are two possible case

$Q_1(x)$ = x is even

$Q_2(x)$ = x is odd

Case 1: $\forall x \in \mathbb{Z}(Q_1(x) \rightarrow P(x))$

Assume $Q_1(x)$ is true. Then x can be expressed as $x = 2k$

$x^3 - x = (2k)^3 - 2k = 2k \cdot 2k \cdot 2k - 2k$

$2k \cdot 2k \cdot 2k - 2k = 2(4k^3 - k)$

since k is any int and any int multiplied by 2 is even $P(x)$ is true

Chris Hunt DP3 MTH 231

3.2 Proofs

- Proof by cases cont.

Case 2: $\forall x \in \mathbb{Z}(Q_2(x) \rightarrow P(x))$

Assume $Q_2(x)$ is true. X can then be expressed as $x = 2k+1$.

$$x^3 - x = (2k+1)^3 - (2k+1) = (2k+1)(2k+1)(2k+1) - 2k - 1$$

$$8k^3 + 16k^2 + 8k + 1 - 2k - 1 = 8k^3 + 16k^2 + 6k = 2(4k^3 + 8k^2 + 3k)$$

Any int multiplied by 2 is even, therefore case 2 is true.

Since both cases are always true then the statement $\forall x \in \mathbb{Z}(P(x))$ is true.

Chris Hunt DP3 MTH 231

5) Prove that for all integers n, it is the case that n is even if and only if $3n$ is even. That is, prove both implications: if n is even, then $3n$ is even, and if $3n$ is even, then n is even.

Let: $P(n)$ = "n is even" $Q(n)$ = "$3n$ is even"

Claim: $\forall_n \in \mathbb{Z}\,(P(n) \leftrightarrow Q(n))$ $\equiv$ $\forall n \in \mathbb{Z}\,(P(n) \rightarrow Q(n) \wedge Q(n) \rightarrow P(n))$

Proof: Case 1: Suppose n is even. Since n is even we know that $n = 2a$ where a is any integer. Now consider $3n$:

$$3n = 3(2a) = 2(3a)$$

Since we know that a is an integer, we know that $3a$ is an integer, so $2(3a)$ is even. Therefore, if $P(n)$, then $Q(n)$ is true.

Case 2: Consider the contrapositive of $Q(n) \rightarrow P(n)$, if n is odd, then $3n$ is odd. Suppose n is odd. Since n is odd we know that $n = 2k+1$ where k is any integer. Now consider $3n$:

$$3n = 3(2k+1) = 6k + 3 = 2(3k+1) + 1$$

Since we know that k is an integer, we know that $3k+1$ is an integer, so $2(3k+1)+1$ is odd. The contrapositive is true, therefore the original statement is true

Since both cases are always true so is the complete claim.

//

Chris Hunt DP3 MTH231

7) Consider the statement: For all integers a and b, if a is even and b is a multiple of 3, then ab is a multiple of 6.

a. Prove the statement. What sort of proof are you using?

$a, b, n, m \in \mathbb{Z}$ Let: $P: a = 2n$ $Q: 3 \mid b = m$ $R: 6 \mid ab = nm$

Claim: $\forall a \forall b \in \mathbb{Z}(P \wedge Q \rightarrow R)$ $b = 3m$ $ab = 6(nm)$

Proof: Suppose P and Q.

$$ab = (2n)(3m) = 6(nm)$$

Since nm is an integer we can conclude that $6 \mid ab = nm$
Therefore the statement is true.

//

Direct Proof

SQ.2) "If k is any odd integer and m is any even integer, then $k^2 + m^2$ is odd"

Let: $k, m \in \mathbb{Z}$ $P =$ "k is odd" $Q =$ "m is even"

$R =$ "$k^2 + m^2$ is odd"

Claim: $\forall k, m \in \mathbb{Z}(P \wedge Q \rightarrow R)$ | $\forall k, m \in \mathbb{Z}(\neg R \rightarrow \neg P \vee \neg Q$

Proof: Suppose P and Q are true.

Let: $a, b \in \mathbb{Z}$ $k = 2a + 1$ $m = 2b$

$$k^2 + m^2 = (2a+1)^2 + (2b)^2 = 4a^2 + 4a + 1 + 4b^2$$

$$4a^2 + 4b^2 + 4a + 1 = 2(2a^2 + 2b^2 + 2a) + 1$$

Since a and b are integers and they are closed under + and ×, $k^2 + m^2 =$ odd. Therefore the statement is true.

//