Proofs problems

Joshua Morton

November 19, 2023

Chapter 1

Intuitive Proofs

Fact 1.0.1: The pigeonhole principle

Simple form: If $n+1$ objects are placed into n boxes, then at least one box has at least two objects in it.
General form: If $kn+1$ objects are placed into n boxes, then at least one box has at least $k+1$ objects in it.

Proposition

If one chooses $n+1$ numbers from $\{1, 2, 3, \ldots, 2n\}$, it is guaranteed that two of the numbers they chose are consecutive.

Proof. TODO *Quick maths*

Proposition

If one selects any $n+1$ numbers from the set $\{1, 2, \ldots, 2n\}$, then two of the selected numbers will sum to $2n+1$.

Proof. TODO *Quick maths*

Proposition

If one chooses 31 numbers from the set $\{1, 2, 3, \ldots, 60\}$, then two of the numbers must be relatively prime.

Proof. TODO *Quick maths*

Problem

Determine whether or not the pigeonhole principle guarantees that two students at your school have the same 3-letter initals.

TODO

Chapter 2

Direct proofs

Fact 2.0.1

The sum of integers in an integer, the difference of integers is an integer, and the product of integers is an integer.

Definition 2.0.1: Even and odd integers

- An integer n is even if $n = 2k$ for some integer k;
- An integer n is odd if $n = 2k + 1$ for some integer k.

Fact: Any integer is either even or odd.

Proposition

The sum of an even integer and an odd integer is odd.

Proof. Assume that n is an even integer and that m is an odd integer. By the definition of even and odd numbers $n = 2a$ and $m = 2b + 1$ for some integers a and b. Then,

$$n + m = (2a) + (2b + 1) = 2a + 2b + 1 = 2(a + b) + 1.$$

And since $a+b$ is an integer by Fact 2.0.1, we have shown that $n+m = 2k+1$ where $k = a+b$. Therefore, by the definition of an odd integer this means that $a + b$ is odd. *Quick maths*

Proposition

The product of two even integers is even.

Proof. Assume that n and m are even integers. By the definition of an even integer $n = 2a$ and $m = 2b$ for some integers a and b. Then,

$$nm = (2a)(2b) = 4ab = 2(2ab).$$

And since $2ab$ is an integer by Fact 2.0.1, we have shown that $nm = 2k$ where $k = 2ab$. Therefore, by the definition of an even integer this means that nm is even. *Quick maths*

Proposition

The product of two odd integers is odd.

Proof. Assume that n and m are odd integers. By the definition of an odd integer this means that $n = 2a + 1$ and $m = 2b + 1$ for some integers a and b. Then,

$$nm = (2a + 1)(2b + 1) = 4ab + 2a + 2b + 1 = 2(2ab + a + b) + 1.$$

And since $2ab + a + b$ is an integer by Fact 2.0.1, we have shown that $nm = 2k + 1$ where $k = 2ab + a + b$. Therefore, by the definition of an odd integer this means that nm is odd. *Quick maths*

Proposition

The product of an even integer and an odd integer is even.

Proof. Assume that n is an even integer and m is an odd integer. By the definition of an even and odd integer this means that $n = 2a$ and $m = 2b + 1$ for some integers a and b. Then,

$$nm = (2a)(2b + 1) = 4ab + 2a = 2(2ab + a).$$

Since $2ab + a$ is an integer by Fact 2.0.1, we have shown that $nm = 2k$ where $k = 2ab + a$. Therefore, by the definition of an even integer this means that nm is even. *Quick maths*

Proposition

An even integer squared is an even integer.

Proof. Assume that n is an even integer. By the definition of an even integer $n = 2a$ for some integer a. Then,

$$n^2 = (2a)^2 = 4a^2 = 2(2a^2).$$

Since $2a^2$ is an integer by Fact 2.0.1, we have shown that $n^2 = 2k$ where $k = 2a^2$. Therefore, by the definition of an even integer this means that n^2 is even. *Quick maths*

Definition 2.0.2

A nonzero integer a is said to *divide* an integer b if $b = ak$ for some integer k. When a does divide b, we write "$a \mid b$" and when a does not divide b we write "$a \nmid b$."

Proposition 2.0.1

If $d \mid a$ and $d \mid b$ then $d \mid a + b$.

Proof. Assume that $d \mid a$ and $d \mid b$. By the definition of divisibility $a = dk$ and $b = dl$ for some integers k and l. Then,

$$a + b = dk + dl = d(k + l).$$

Since $k + l$ is an integer by Fact 2.0.1, we have shown that $a + b = dq$ where $q = k + l$. Therefore, by the definition of divisibility this means that $d \mid a + b$. *Quick maths*

Proposition 2.0.2

If $d \mid b$ then $d \mid -b$.

Proof. Assume that $d \mid b$. By the definition of divisibility $dk = b$ for some integer k. Then,

$$-b = -(dk) = d(-k).$$

Since $-k$ is an integer by Fact 2.0.1, we have shown that $-b = dq$ where $q = -k$. Therefore, by the definition of divisibility this means that $d \mid -b$. *Quick maths*

Proposition 2.0.3

If $d \mid b$ then $-d \mid b$.

Proof. Assume that $d \mid b$. By the definition of divisibility $dk = b$ for some integer k. Then,

$$b = dk = - - dk = -d(-k)$$

Since $-k$ is an integer by Fact 2.0.1, we have shown that $b = -dq$ where $q = -k$. Therefore, by the definition of divisibility this means that $-d \mid b$. *Quick maths*

Definition 2.0.3: Modular Congruence

For integers a, r and m, we say that a is *congruent* to r *modulo* m, and we write $a \equiv r \pmod{m}$, if $m \mid (a - r)$.

Proposition 2.0.4

If a, b, c, d and m are integers, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then, $a+c \equiv b+d \pmod{m}$.

Proof. Assume that a, b, c, d and m are integers, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By the definition of modular congruence this means that $m \mid (a-b)$ and $m \mid (c-d)$. Applying the definition of divisibility we get $mk = a - b$ and $ml = c - d$ for some integers k and l. Then,

$$(a + c) - (b + d) = (a - b) + (c - d) = mk + ml = m(k + l).$$

Since by Fact 2.0.1 $k + l$ is an integer, we have shown that $(a + c) - (b + d) = mq$ where $q = k + l$. Therefore, by the definition of divisibility $m \mid (a+c)-(b+d)$. Furthermore, by the definition of modular congruence $a + c \equiv b + d \pmod{m}$. *Quick maths*

Proposition 2.0.5

If a, b, c, d and m are integers, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then, $a-c \equiv b-d \pmod{m}$.

Proof. Assume that a, b, c, d and m are integers, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. By the definition of modular congruence this means that $m \mid (a-b)$ and $m \mid (c-d)$. Applying the definition of divisibility we get $mk = a - b$ and $ml = c - d$ for some integers k and l. Then,

$$(a - c) - (b - d) = (a - b) - (c - d) = mk - ml = m(k - l).$$

Since by Fact 2.0.1 $k - l$ is an integer, we have shown that $(a - c) - (b - d) = mq$ where $q = k - l$. Therefore, by the definition of divisibility $m \mid (a-c)-(b-d)$. Furthermore, by the definition of modular congruence $a - c \equiv b - d \pmod{m}$. *Quick maths*

Proposition 2.0.6

If a, b, c, d and m are integers, $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then, $ac \equiv bd \pmod{m}$.

I was unable to do this problem in a reasonable amount of time :/ I ended up looking at the answer.

Proposition 2.0.7

Prove that for every integer n, either $n^2 \equiv 0 \pmod{4}$ or $n^2 \equiv 1 \pmod{4}$.

Proof. Assume that n is an integer. By definition 2.0.1, n is either even or odd.

First consider the case when n is even. By the definition of an even integer $n = 2k$ for some integer k. Then,

$$n^2 = (2k)^2 = 4k^2 = 4(k^2).$$

Since by Fact 2.0.1 k^2 is an integer, we have shown that $n^2 = 4p$ where $p = k^2$. Therefore, by the definition of divisibility $4 \mid n^2$. Furthermore, by the definition of modular congruence $n^2 \equiv 0 \pmod 4$. Based on that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Now consider the case when n is odd. By the definition of an odd integer $n = 2k+1$ for some integer k. Then,

$$n^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k = 4(k^2 + k).$$

Since by Fact 2.0.1 $k^2 + k$ is an integer, we have shown that $n^2 - 1 = 4p$ where $p = k^2 + k$. Therefore, by the definition of divisibility $4 \mid n^2 - 1$. Furthermore, by the definition of modular congruence $n^2 \equiv 1 \pmod 4$. Based on that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

Since $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$ both when n is even and when n is odd, we have proven that $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$ for all integers n. *Quick maths*

Definition 2.0.4: Greatest common divisor

Given two integers a and b, the *greatest common divisor* of a and b is the largest integer d, such that $d \mid a$ and $d \mid b$. We say that the $\gcd(a, b) = d$.

Lemma 2.0.1

If a, b are integers then $\gcd(a, b) = \gcd(b, a)$.

Proof. TODO *Quick maths*

Chapter 3

Sets

Definition 3.0.1: Subsets

Suppose A and B are sets. If every element in A is also in B, then A is a *subset* of B, denoted $A \subseteq B$.

Definition 3.0.2: Union

The *union* of sets A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$. Furthermore, if $\mathscr{A}$ is a set of sets, then $\bigcup_{S \in \mathscr{A}} S$ is the *union* between all subsets of $\mathscr{A}$.

Definition 3.0.3: Intersection

The *intersection* of sets A and B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$. Furthermore, if $\mathscr{A}$ is a set of sets, then $\bigcap_{S \in \mathscr{A}} S$ is the *intersection* between all subsets of $\mathscr{A}$.

Definition 3.0.4: Set subtraction

The *subtraction* of sets B from A is the set $A \setminus B = \{x : x \in A \text{ and } x \notin B\}$.

Definition 3.0.5: Complement of a set

If $A \subseteq U$, then U is called a *universal set* of A. The *complement* of A in U is $A^c = U \setminus A$.

Proposition 3.0.1

Suppose A, B and C are sets. Prove that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Proof. Assume A, B and C are sets. We wish to show that $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Notice that this is equivalent to proving $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

To begin we will prove that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Assume that $x \in A \cup (B \cap C)$. By the definition of the union between sets,

$$x \in A \quad \text{or} \quad x \in B \cap C.$$

We will first consider the case when $x \in A$. It is clear to the see that $x \in A \cup B$ and $x \in A \cup C$ by the definition of union between sets. Furthermore, by the definition of intersection between sets $x \in (A \cup B) \cap (A \cup C)$. Now consider the case when $x \in B \cap C$. By the definition of intersections between sets,

$$x \in B \quad \text{and} \quad x \in C.$$

Using the definition of union between sets we get $x \in A \cup B$ and $x \in A \cup C$. Additionally, applying the definition of intersections between sets we get $x \in (A \cup B) \cap (A \cup C)$. Since in either case $x \in (A \cup B) \cap (A \cup C)$ this shows that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Now we will prove that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. Assume that $x \in (A \cup B) \cap (A \cup C)$. By the definition of intersections between sets.

$$x \in A \cup B \quad \text{and} \quad x \in A \cup C.$$

First consider the case when $x \in A$. By the definition of unions between sets $x \in A \cup (B \cap B)$. Now, consider the case when $x \notin A$. Since $x \in A \cup B$, $x \in A \cup C$ and $x \notin A$, $x \in B$ and $x \in C$. Applying the definition of intersections between sets we get $x \in B \cap C$. Additionally, applying the definition of unions between sets we get $x \in A \cup (B \cap C)$. Since in either case $x \in A \cup (B \cap C)$ we have shown that $(A \cap B) \cup (A \cap C) \subseteq A \cup (B \cap C)$.

Both $A \cup (B \cap C)$ and $(A \cup B) \cap (A \cup C)$ are subsets of each other, this shows that they must be equal, completing the proof. *Quick maths*