

Proofs problems

Joshua Morton

September 11, 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 $\{1, 2, 3, \dots, 2n\}$, 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 $\{1, 2, \dots, 2n\}$, then two of the selected numbers will sum to $2n + 1$.

Proof. TODO

Quick maths

Proposition

If one chooses 31 numbers from the set $\{1, 2, 3, \dots, 60\}$, 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 initials.

TODO

Chapter 2

Direct proofs

Fact 2.0.1

The sum of integers is 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 divisibility 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*