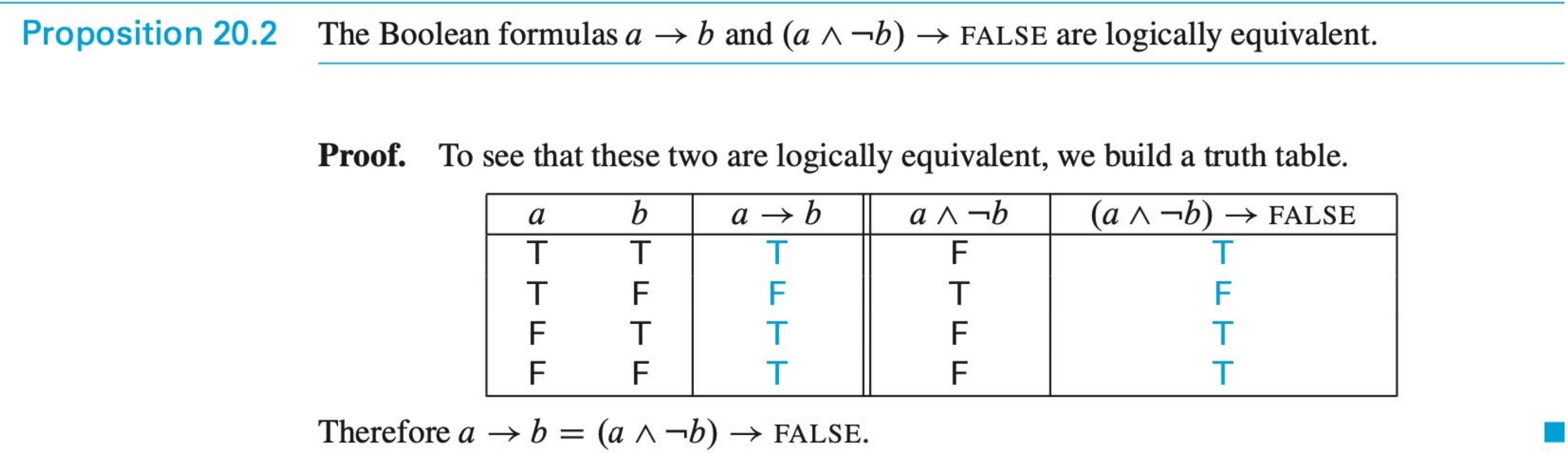
CIT 5920
Recitation 9

Shenao, Sam, Tiffany, Qianyue, Shutong

Overview for Today

- Logistics
- Proof by Contradiction and Contrapositive
- How to Negate an Implication
- Question 1 (2 minutes)
- Question 2 (3 minutes)
- Question 3 (3 minutes)
- Detour: Rational Numbers
- Question 4 (4 minutes)
- Question 5 (5 minutes)
- Question 6 (5 minutes)

Proof by Contradiction



Proposition 20.2 The Boolean formulas $a \to b$ and $(a \wedge \neg b) \to \text{FALSE}$ are logically equivalent.

Proof. To see that these two are logically equivalent, we build a truth table.

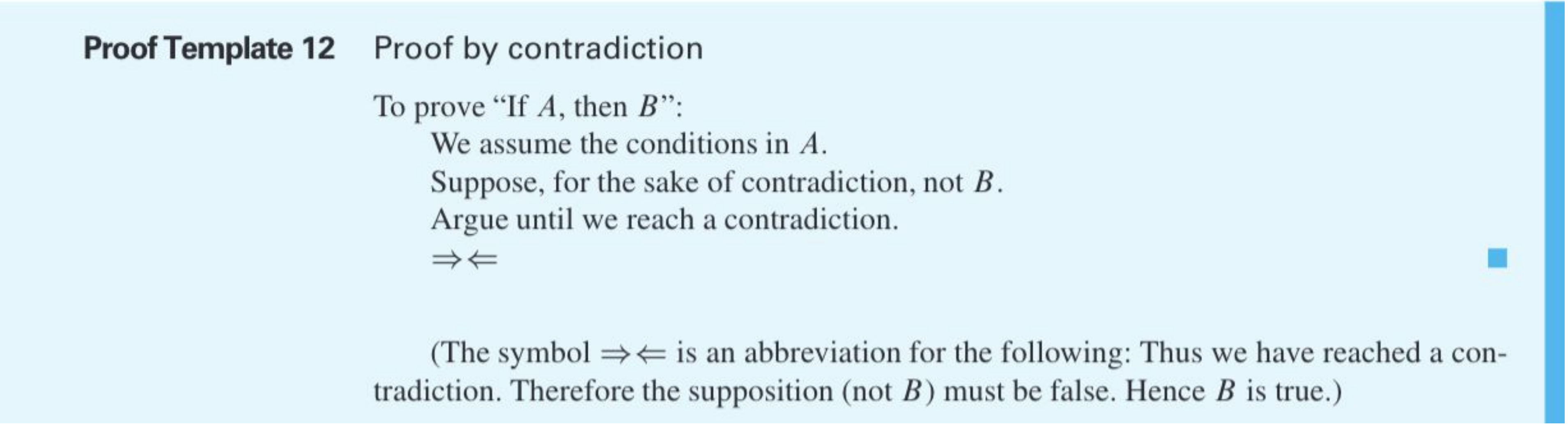
a	b	$a \to b$	$a \wedge \neg b$	$(a \wedge \neg b) \to \text{FALSE}$
T	T	T	F	T
T	F	F	T	F
F	T	T	F	T
F	F	T	F	T

Therefore $a \to b = (a \wedge \neg b) \to \text{FALSE}$. ■

Proof by Contradiction

P	Q	$\neg P$	$P \Rightarrow Q$	$\neg P \vee Q$	$\neg(P \Rightarrow Q)$	$P \wedge \neg Q$
T	T	F	T	T	F	F
F	T	T	T	T	F	F
T	F	F	F	F	T	T
F	F	T	T	T	F	F

Proof by contradiction



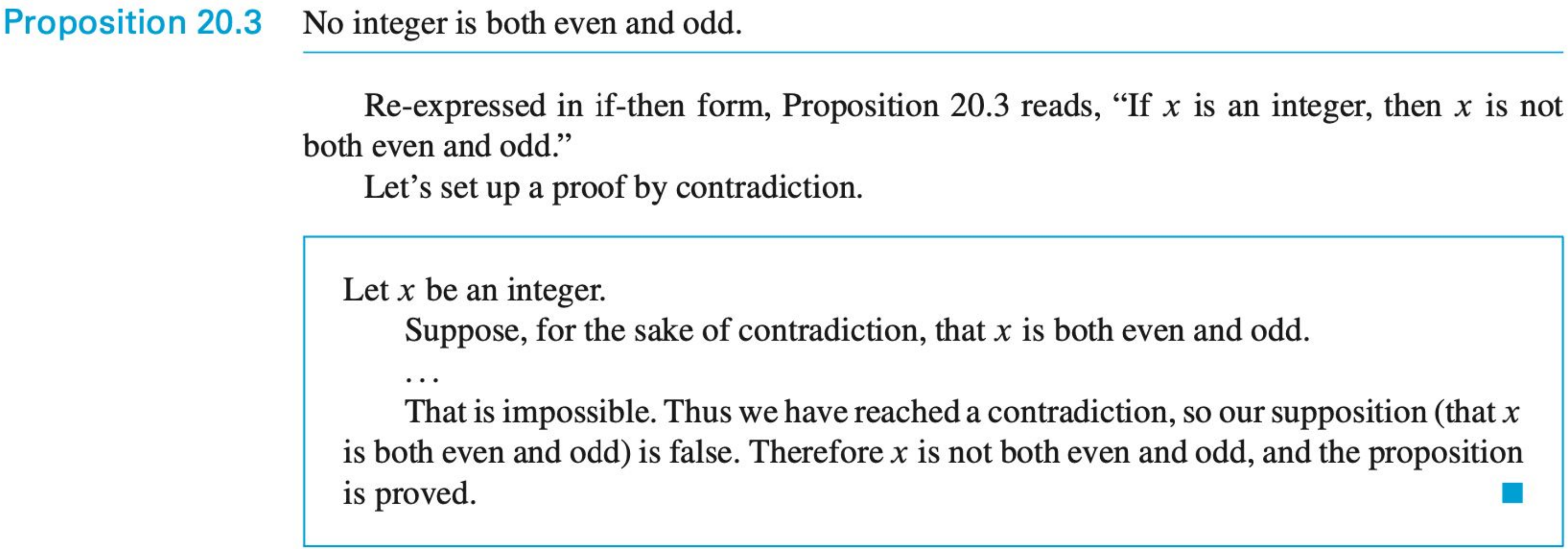
Proof Template 12 Proof by contradiction

To prove "If A, then B":

We assume the conditions in A.
Suppose, for the sake of contradiction, not B.
Argue until we reach a contradiction.
$\Rightarrow\Leftarrow$ ■

(The symbol $\Rightarrow\Leftarrow$ is an abbreviation for the following: Thus we have reached a contradiction. Therefore the supposition (not B) must be false. Hence B is true.)

Proof by Contradiction



Proposition 20.3 No integer is both even and odd.

Re-expressed in if-then form, Proposition 20.3 reads, “If x is an integer, then x is not both even and odd.”

Let’s set up a proof by contradiction.

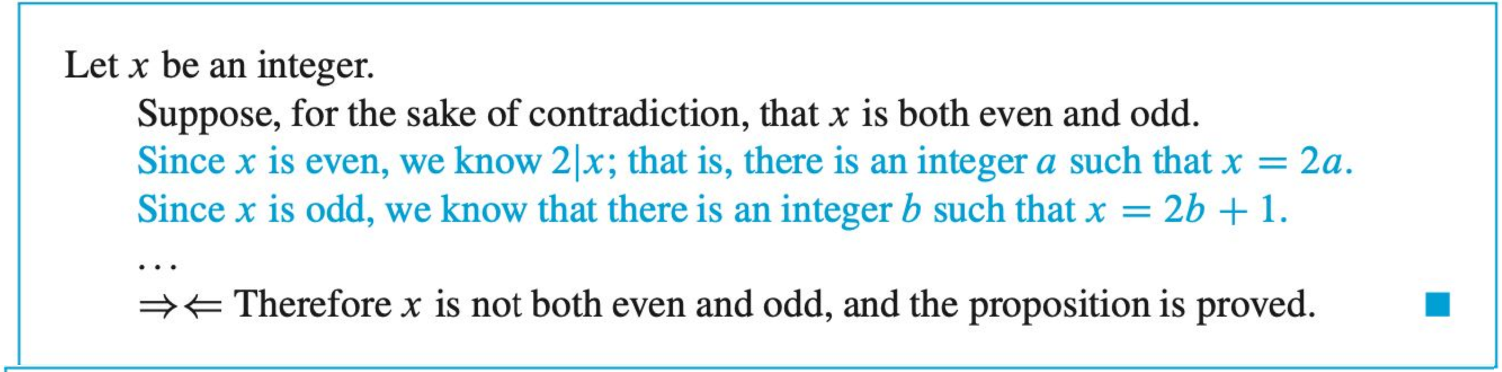
Let x be an integer.

Suppose, for the sake of contradiction, that x is both even and odd.

. . .

That is impossible. Thus we have reached a contradiction, so our supposition (that x is both even and odd) is false. Therefore x is not both even and odd, and the proposition is proved. ■

Proof by Contradiction



Let x be an integer.

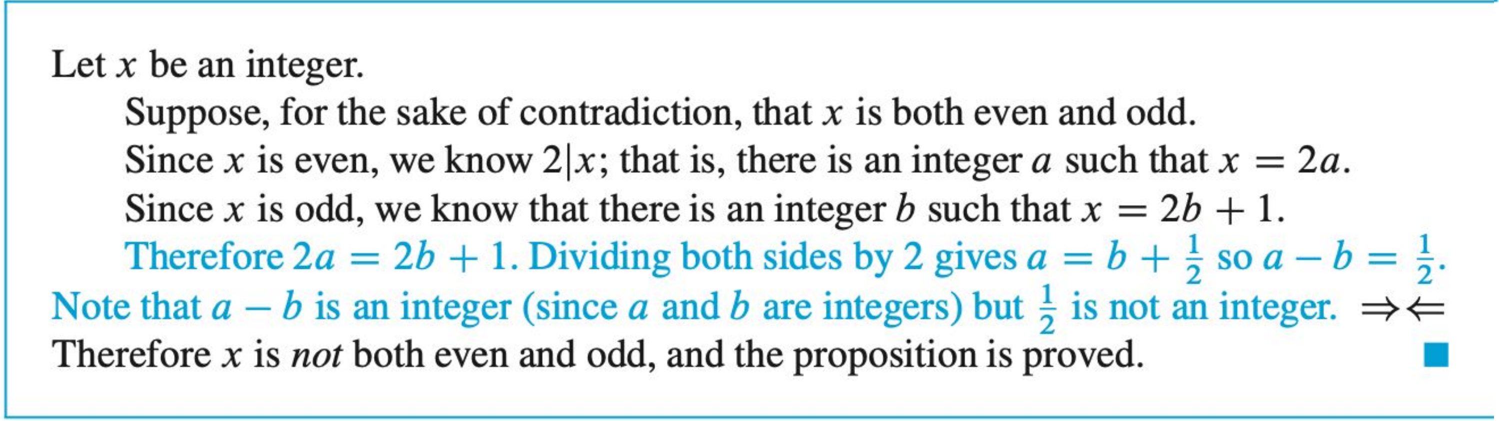
Suppose, for the sake of contradiction, that x is both even and odd.

Since x is even, we know $2|x$; that is, there is an integer a such that $x = 2a$.

Since x is odd, we know that there is an integer b such that $x = 2b + 1$.

$\dots$

$\Rightarrow\Leftarrow$ Therefore x is not both even and odd, and the proposition is proved. ■



Let x be an integer.

Suppose, for the sake of contradiction, that x is both even and odd.

Since x is even, we know $2|x$; that is, there is an integer a such that $x = 2a$.

Since x is odd, we know that there is an integer b such that $x = 2b + 1$.

Therefore $2a = 2b + 1$. Dividing both sides by 2 gives $a = b + \frac{1}{2}$ so $a - b = \frac{1}{2}$.

Note that $a - b$ is an integer (since a and b are integers) but $\frac{1}{2}$ is not an integer. $\Rightarrow\Leftarrow$

Therefore x is *not* both even and odd, and the proposition is proved. ■

Contrapositive

Suppose $x \in Z$. If $7x + 9$ is even, then x is odd

Proof by contrapositive: (recall if a then b becomes if not b then not A

Suppose x is NOT odd.

Suppose x is not odd. Thus we can write it as some $x = 2a$

Then $7x + 9 = 7(2a) + 9 = 14a + 9 = 2(7a+4) + 1$

Consequently $7x + 9$ is not even

How to Negate an Implication

Say we want to negate: $P \Rightarrow Q$

We want to make it: $\neg(P \Rightarrow Q)$

Step 1: Replace Implication Sign

Rewrite $P \Rightarrow Q$ as: $\neg P \lor Q$

With the negation:

$\neg(P \Rightarrow Q)$ becomes $\neg(\neg P \lor Q)$

Step 2: Use DeMorgan's Law

Rewrite $\neg P \lor Q$ as: $\neg(P \land \neg Q)$

With the negation:

$\neg(\neg P \lor Q)$ becomes $\neg(\neg(P \land \neg Q))$

Step 3: Cancel out Extra Negations

$\neg(\neg(P \land \neg Q))$ becomes $P \land \neg Q$

Question ?

Prove by contradiction that

if 4 divides an integer n, then n + 2 is not divisible by 4

Answer 1

We will prove this by contradiction.

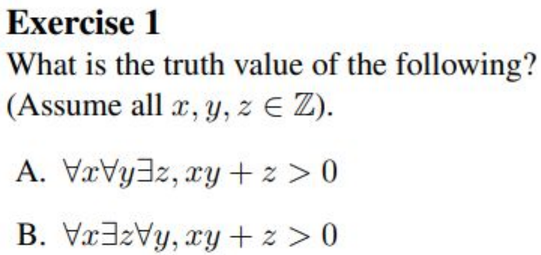
1. Assume, to the contrary, that if n is divisible by 4, then n + 2 **is divisible** by 4.
2. Since 4 divides n, then n = 4k for some integer k.
3. Since n + 2 is divisible by 4, then n + 2 = 4p for some integer p.
4. Substituting n = 4k into n + 2 = 4p:

   4k + 2 = 4p

   2 = 4(p - k)

   ½ = p - k
5. Since p, k are integers, then p - k is an integer. However, ½ is not an integer, which leads to a contradiction.
6. Therefore, we conclude that the original statement is true: if 4 divides an integer n, then n + 2 is not divisible by 4.

Question 1



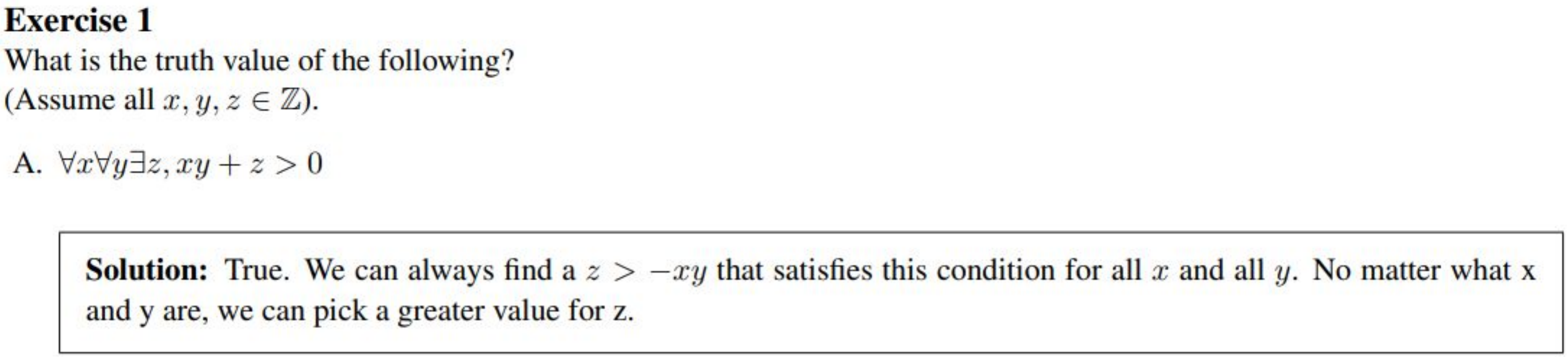
Exercise 1

What is the truth value of the following?
(Assume all $x, y, z \in \mathbb{Z}$).

A. $\forall x \forall y \exists z, xy + z > 0$

B. $\forall x \exists z \forall y, xy + z > 0$

Answer 1

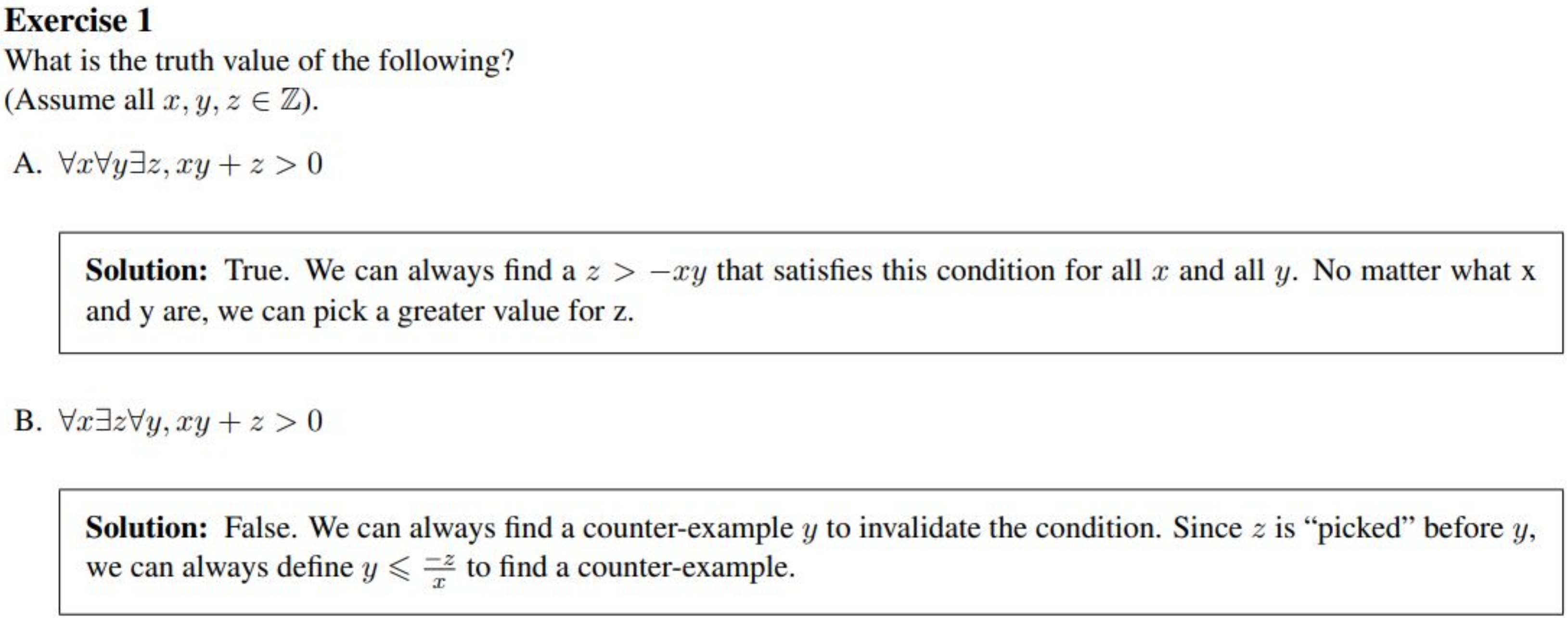


Exercise 1
What is the truth value of the following?
(Assume all $x, y, z \in \mathbb{Z}$).

A. $\forall x \forall y \exists z, xy + z > 0$

Solution: True. We can always find a $z > -xy$ that satisfies this condition for all x and all y. No matter what x and y are, we can pick a greater value for z.

Answer 1 (cont.)



Exercise 1
What is the truth value of the following?
(Assume all $x, y, z \in \mathbb{Z}$).

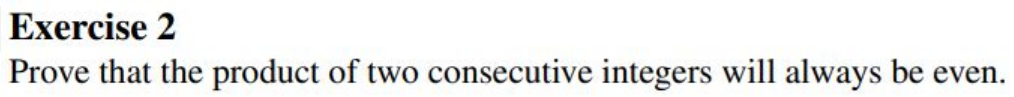
A. $\forall x \forall y \exists z, xy + z > 0$

Solution: True. We can always find a $z > -xy$ that satisfies this condition for all x and all y. No matter what x and y are, we can pick a greater value for z.

B. $\forall x \exists z \forall y, xy + z > 0$

Solution: False. We can always find a counter-example y to invalidate the condition. Since z is "picked" before y, we can always define $y \leqslant \frac{-z}{x}$ to find a counter-example.

Question 2

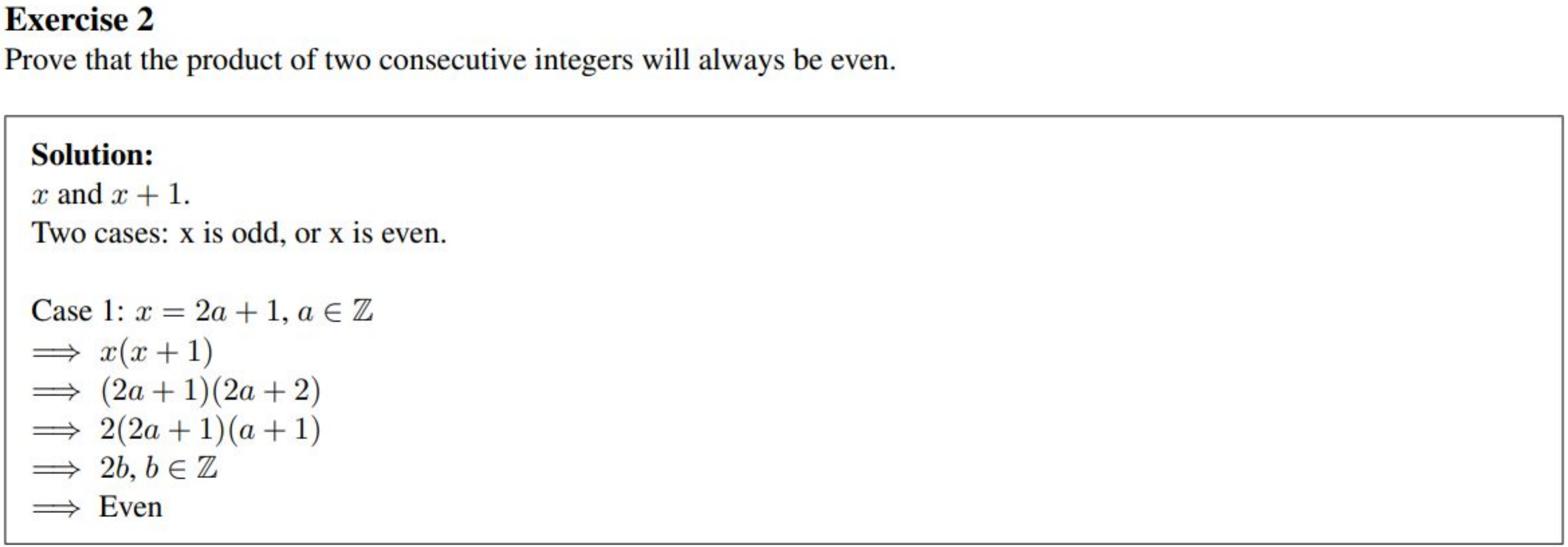


Exercise 2

Prove that the product of two consecutive integers will always be even.

Hint: cases by even and odd numbers

Answer 2



Exercise 2

Prove that the product of two consecutive integers will always be even.

Solution:

x and $x + 1$.

Two cases: x is odd, or x is even.

Case 1: $x = 2a + 1$, $a \in \mathbb{Z}$

$\implies x(x + 1)$

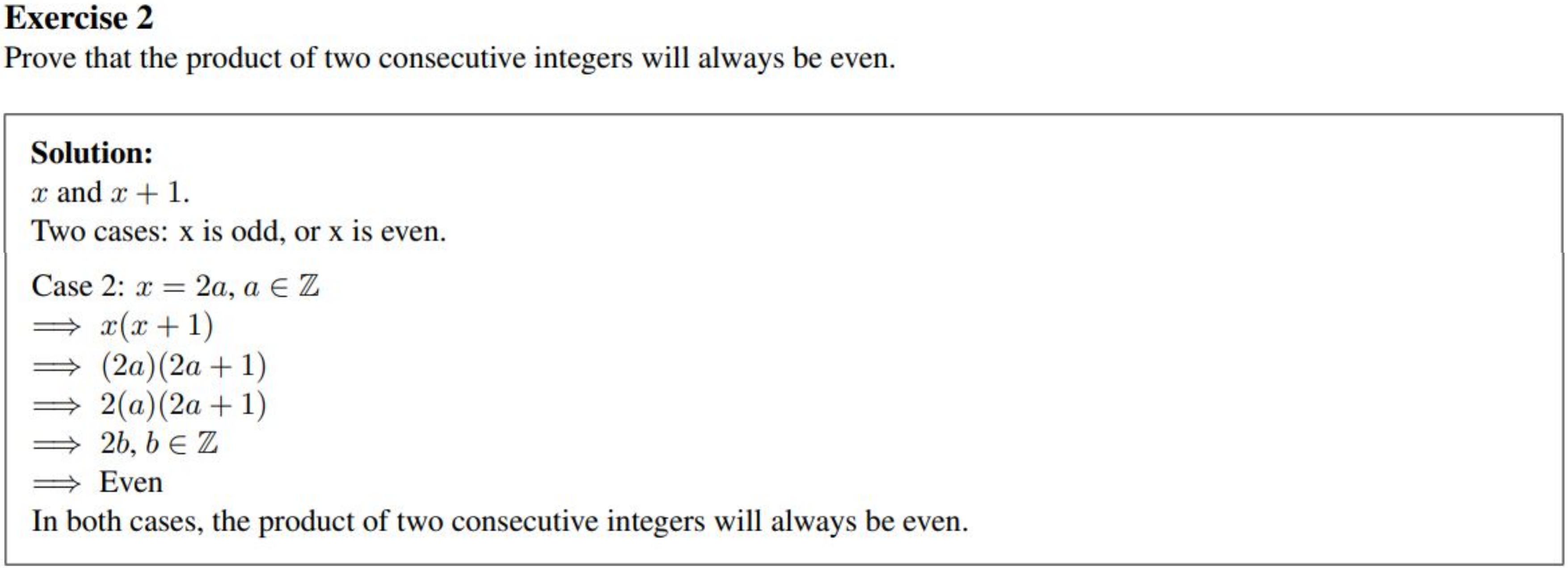
$\implies (2a + 1)(2a + 2)$

$\implies 2(2a + 1)(a + 1)$

$\implies 2b$, $b \in \mathbb{Z}$

$\implies$ Even

Answer 2 (cont.)



Exercise 2

Prove that the product of two consecutive integers will always be even.

Solution:

x and $x + 1$.

Two cases: x is odd, or x is even.

Case 2: $x = 2a$, $a \in \mathbb{Z}$

$\implies x(x+1)$

$\implies (2a)(2a+1)$

$\implies 2(a)(2a+1)$

$\implies 2b$, $b \in \mathbb{Z}$

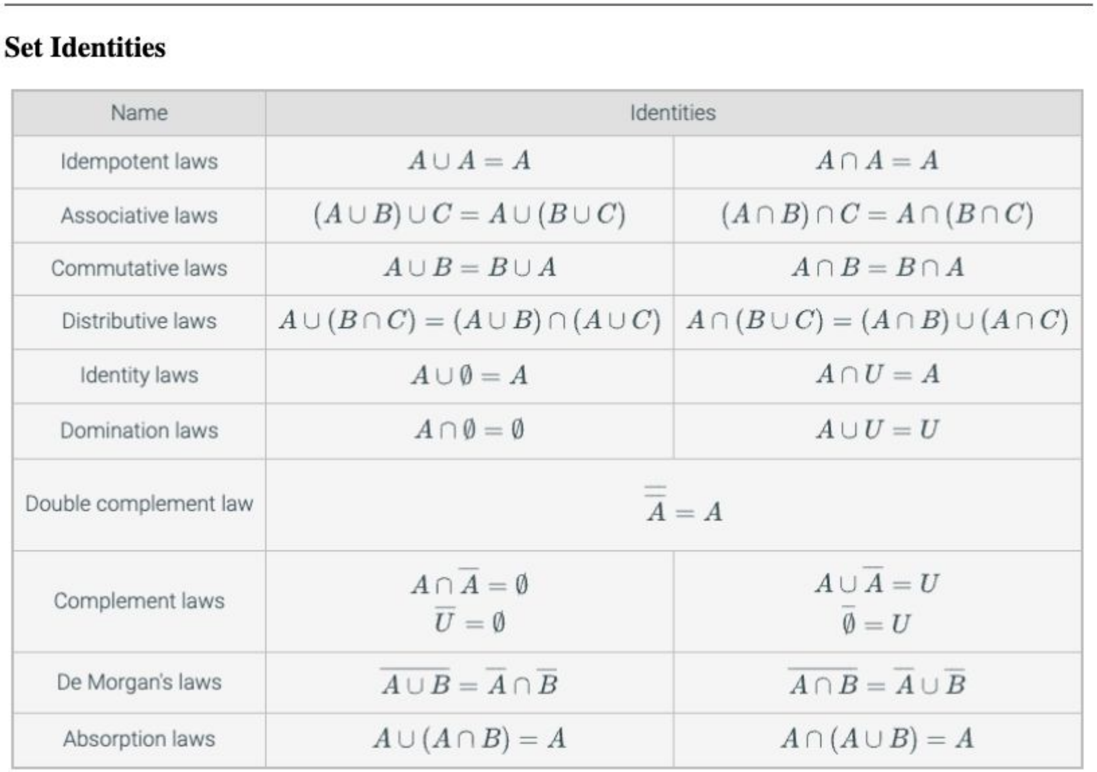
$\implies$ Even

In both cases, the product of two consecutive integers will always be even.

Question 3

Exercise 3

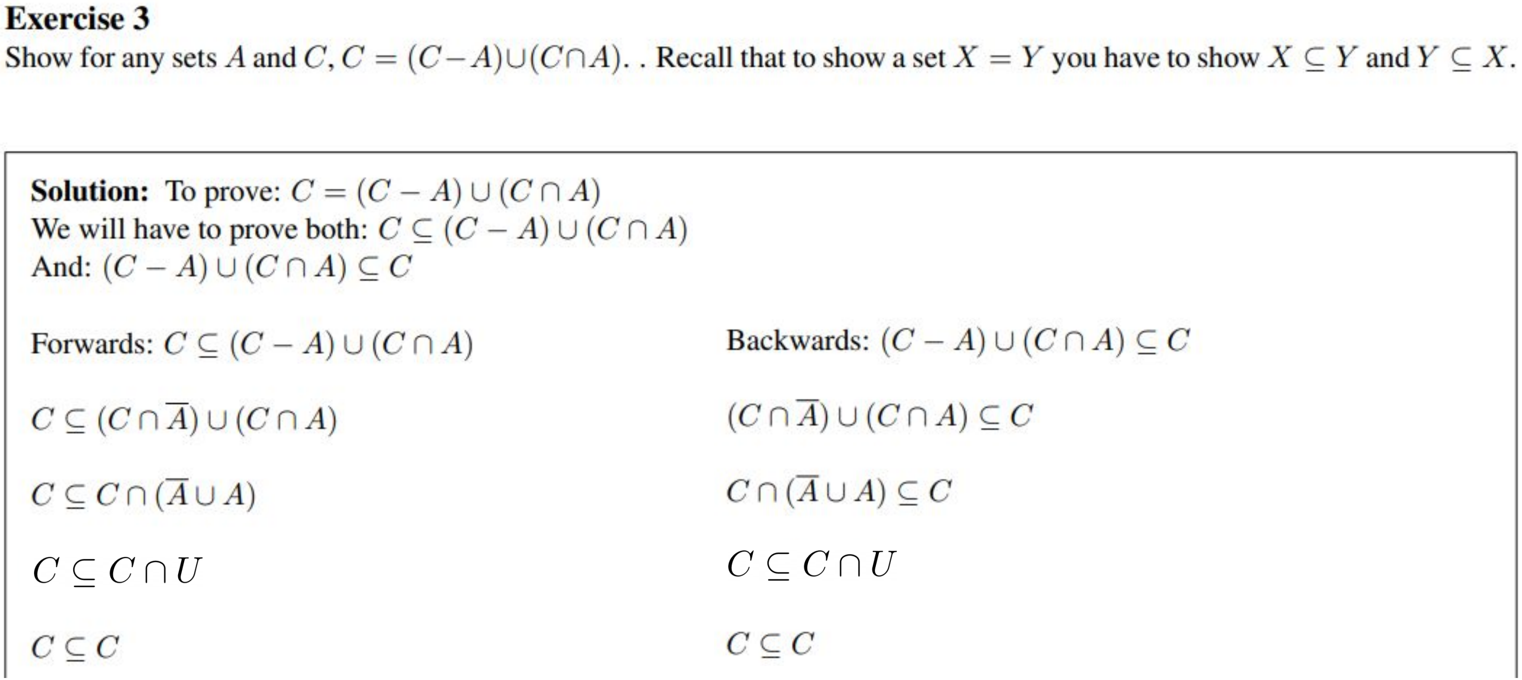
Show for any sets A and C, $C = (C - A) \cup (C \cap A)$. . Recall that to show a set $X = Y$ you have to show $X \subseteq Y$ and $Y \subseteq X$.



Set Identities

Name	Identities	
Idempotent laws	$A \cup A = A$	$A \cap A = A$
Associative laws	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
Commutative laws	$A \cup B = B \cup A$	$A \cap B = B \cap A$
Distributive laws	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
Identity laws	$A \cup \emptyset = A$	$A \cap U = A$
Domination laws	$A \cap \emptyset = \emptyset$	$A \cup U = U$
Double complement law	$\overline{\overline{A}} = A$	
Complement laws	$A \cap \overline{A} = \emptyset$ $\overline{U} = \emptyset$	$A \cup \overline{A} = U$ $\overline{\emptyset} = U$
De Morgan's laws	$\overline{A \cup B} = \overline{A} \cap \overline{B}$	$\overline{A \cap B} = \overline{A} \cup \overline{B}$
Absorption laws	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$

Answer 3



Exercise 3

Show for any sets A and C, $C = (C - A) \cup (C \cap A)$. . Recall that to show a set $X = Y$ you have to show $X \subseteq Y$ and $Y \subseteq X$.

Solution: To prove: $C = (C - A) \cup (C \cap A)$
We will have to prove both: $C \subseteq (C - A) \cup (C \cap A)$
And: $(C - A) \cup (C \cap A) \subseteq C$

Forwards: $C \subseteq (C - A) \cup (C \cap A)$

$C \subseteq (C \cap \overline{A}) \cup (C \cap A)$

$C \subseteq C \cap (\overline{A} \cup A)$

$C \subseteq C \cap U$

$C \subseteq C$

Backwards: $(C - A) \cup (C \cap A) \subseteq C$

$(C \cap \overline{A}) \cup (C \cap A) \subseteq C$

$C \cap (\overline{A} \cup A) \subseteq C$

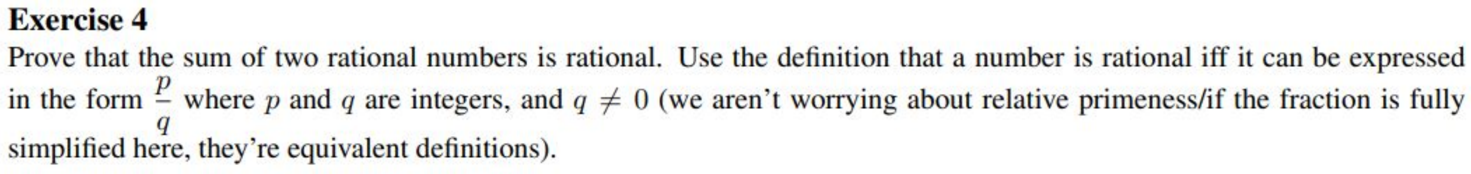
$C \subseteq C \cap U$

$C \subseteq C$

Detour: Rational Numbers

- Any rational number, x, can be expressed as a fraction:
  $\frac{p}{q}$ where p and q are integers, and q is not 0
- e.g. 0.25 can be expressed as 1/4
- A common strategy when doing a proof by contradiction involving rational numbers is to show that assuming some condition is true will lead to a situation where q is 0, or a number that has to be irrational

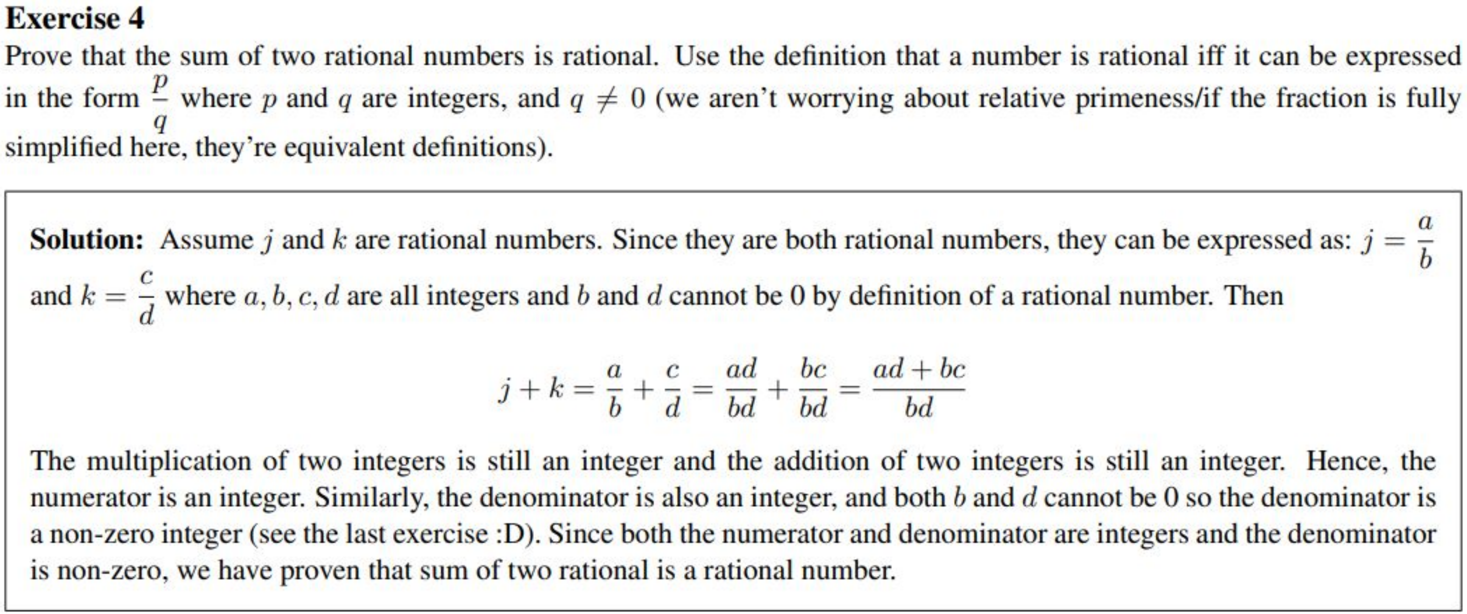
Question 4



Exercise 4

Prove that the sum of two rational numbers is rational. Use the definition that a number is rational iff it can be expressed in the form $\frac{p}{q}$ where p and q are integers, and $q \neq 0$ (we aren't worrying about relative primeness/if the fraction is fully simplified here, they're equivalent definitions).

Answer 4



Exercise 4

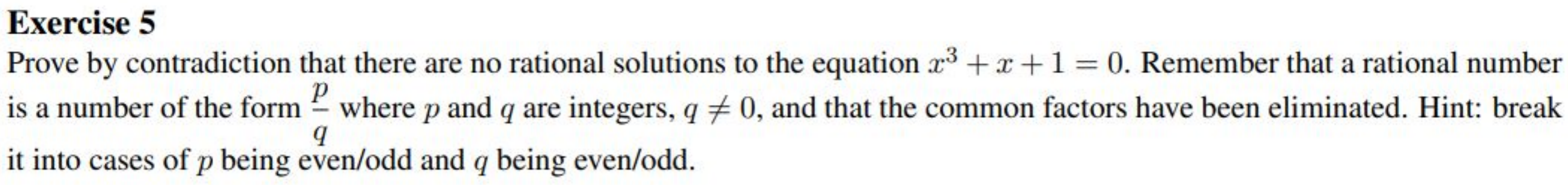
Prove that the sum of two rational numbers is rational. Use the definition that a number is rational iff it can be expressed in the form $\frac{p}{q}$ where p and q are integers, and $q \neq 0$ (we aren't worrying about relative primeness/if the fraction is fully simplified here, they're equivalent definitions).

Solution: Assume j and k are rational numbers. Since they are both rational numbers, they can be expressed as: $j = \frac{a}{b}$ and $k = \frac{c}{d}$ where a, b, c, d are all integers and b and d cannot be 0 by definition of a rational number. Then

$$j + k = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = \frac{ad + bc}{bd}$$

The multiplication of two integers is still an integer and the addition of two integers is still an integer. Hence, the numerator is an integer. Similarly, the denominator is also an integer, and both b and d cannot be 0 so the denominator is a non-zero integer (see the last exercise :D). Since both the numerator and denominator are integers and the denominator is non-zero, we have proven that sum of two rational is a rational number.

Question 5

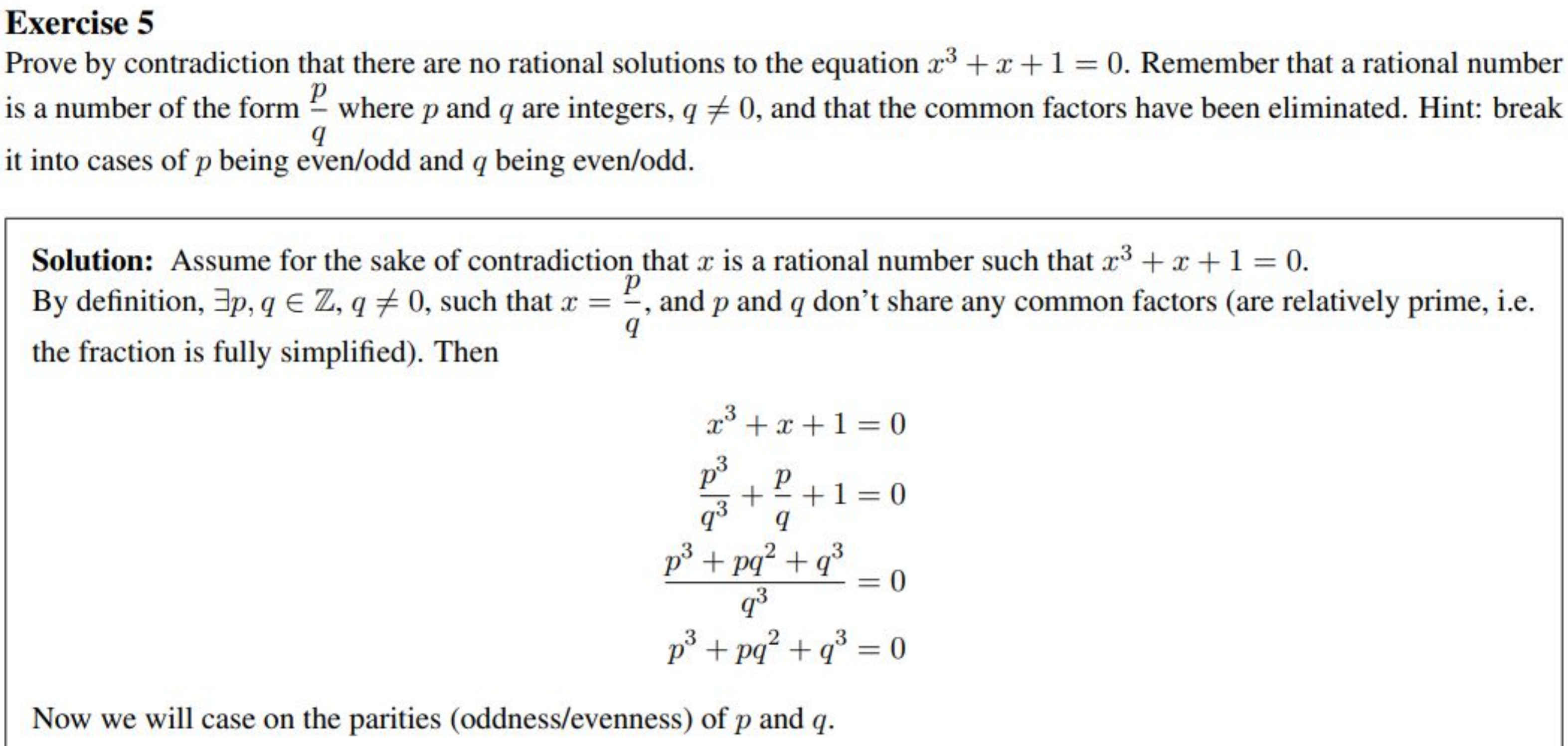


Exercise 5

Prove by contradiction that there are no rational solutions to the equation $x^3 + x + 1 = 0$. Remember that a rational number is a number of the form $\frac{p}{q}$ where p and q are integers, $q \neq 0$, and that the common factors have been eliminated. Hint: break it into cases of p being even/odd and q being even/odd.

Odd + Odd	= Even
Even + Even	= Even
Odd + Even	= Odd
Odd × Odd	= Odd
Even * Even	= Even
Odd * Even	= Even

Answer 5



Exercise 5

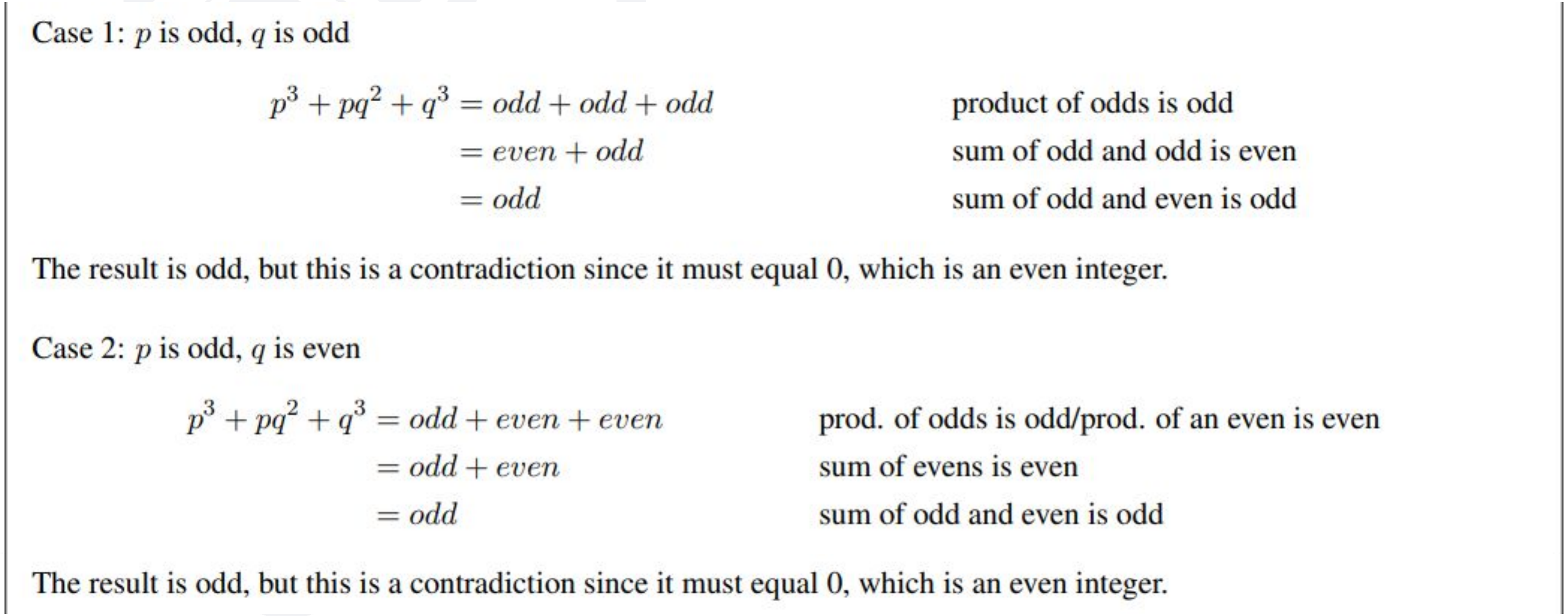
Prove by contradiction that there are no rational solutions to the equation $x^3 + x + 1 = 0$. Remember that a rational number is a number of the form $\frac{p}{q}$ where p and q are integers, $q \neq 0$, and that the common factors have been eliminated. Hint: break it into cases of p being even/odd and q being even/odd.

Solution: Assume for the sake of contradiction that x is a rational number such that $x^3 + x + 1 = 0$. By definition, $\exists p, q \in \mathbb{Z}$, $q \neq 0$, such that $x = \frac{p}{q}$, and p and q don't share any common factors (are relatively prime, i.e. the fraction is fully simplified). Then

$$\begin{aligned} x^3 + x + 1 &= 0 \\ \frac{p^3}{q^3} + \frac{p}{q} + 1 &= 0 \\ \frac{p^3 + pq^2 + q^3}{q^3} &= 0 \\ p^3 + pq^2 + q^3 &= 0 \end{aligned}$$

Now we will case on the parities (oddness/evenness) of p and q.

Answer 5 (cont.)



Case 1: p is odd, q is odd

$$\begin{aligned} p^3 + pq^2 + q^3 &= odd + odd + odd && \text{product of odds is odd} \\ &= even + odd && \text{sum of odd and odd is even} \\ &= odd && \text{sum of odd and even is odd} \end{aligned}$$

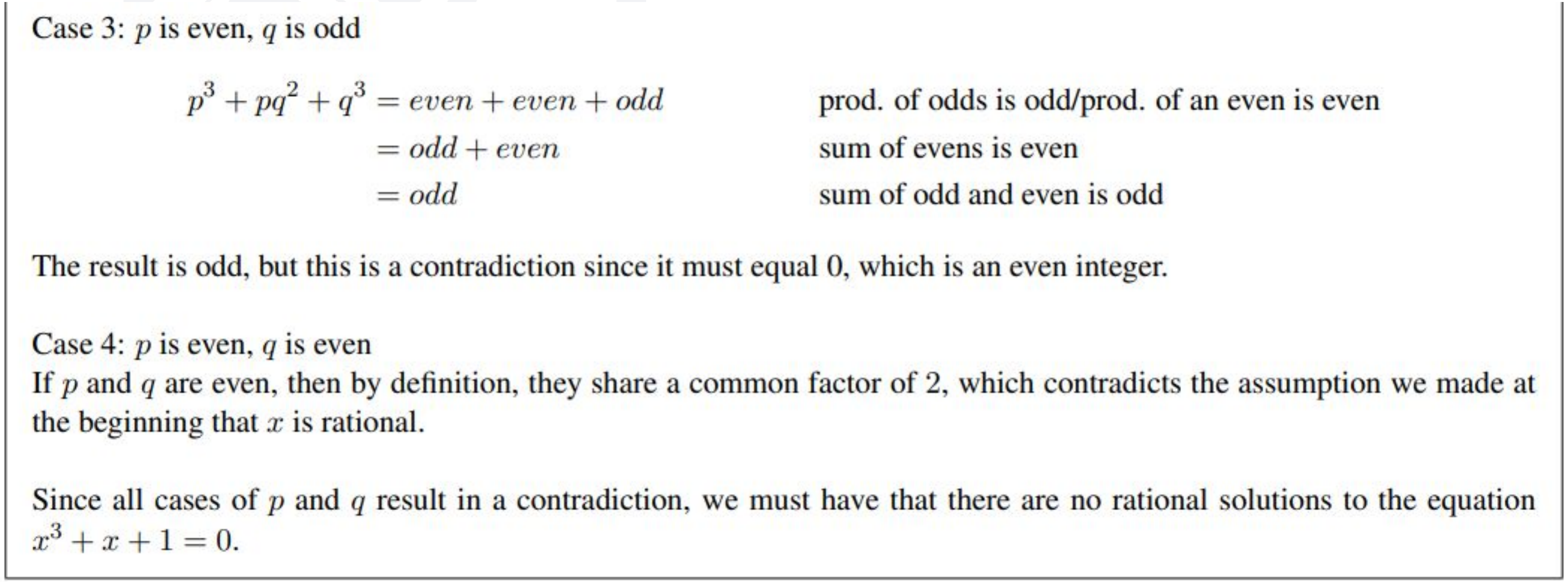
The result is odd, but this is a contradiction since it must equal 0, which is an even integer.

Case 2: p is odd, q is even

$$\begin{aligned} p^3 + pq^2 + q^3 &= odd + even + even && \text{prod. of odds is odd/prod. of an even is even} \\ &= odd + even && \text{sum of evens is even} \\ &= odd && \text{sum of odd and even is odd} \end{aligned}$$

The result is odd, but this is a contradiction since it must equal 0, which is an even integer.

Answer 5 (cont.)



Case 3: p is even, q is odd

$$\begin{aligned} p^3 + pq^2 + q^3 &= even + even + odd && \text{prod. of odds is odd/prod. of an even is even} \\ &= odd + even && \text{sum of evens is even} \\ &= odd && \text{sum of odd and even is odd} \end{aligned}$$

The result is odd, but this is a contradiction since it must equal 0, which is an even integer.

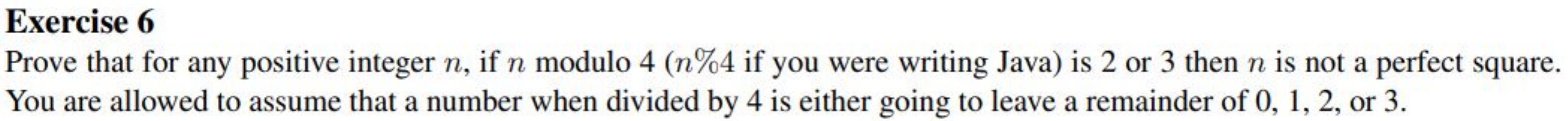
Case 4: p is even, q is even
If p and q are even, then by definition, they share a common factor of 2, which contradicts the assumption we made at the beginning that x is rational.

Since all cases of p and q result in a contradiction, we must have that there are no rational solutions to the equation $x^3 + x + 1 = 0$.

Detour: Modulo

- "Modulo" is the remainder in a division by something
- **n ≡ m [mod p]** is the same thing as saying there is a k such that **n = kp + m**
- For example: **11 ≡ 3 [mod 4]** can be thought of as **7 = (2)(4) + 3**
- When we have a division by p, for instance here, p = 3, then we consider a case for each of the possible remainders:
    - n ≡ 0 [mod 3]
    - n ≡ 1 [mod 3]
    - n ≡ 2 [mod 3]
- The possible remainders will span from **0 to p - 1**
- **We couldn't have n ≡ 3 [mod 3]**, because 3 divides 3 with no remainder, so that's the same case as n ≡ 0 [mod 3]; we can never have a remainder of 3 when dividing by 3 since we could just increment k to deal with that
- This can be a handy tool to use in many cases: for example to denote that a number, **x, is even we can say x ≡ 0 [mod 2]**, i.e. that x can be divided by 2 with no remainder

Question 6

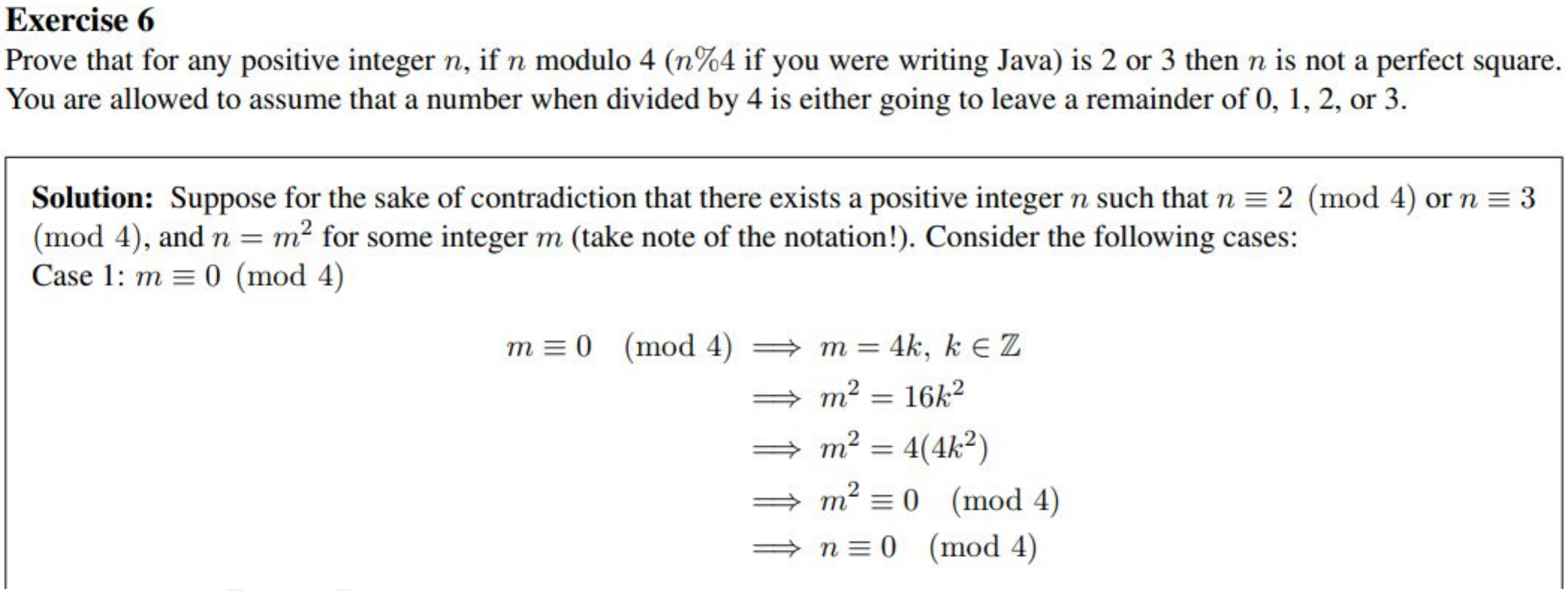


Exercise 6

Prove that for any positive integer n, if n modulo 4 ($n\%4$ if you were writing Java) is 2 or 3 then n is not a perfect square. You are allowed to assume that a number when divided by 4 is either going to leave a remainder of 0, 1, 2, or 3.

Use Contradiction

Answer 6



Exercise 6

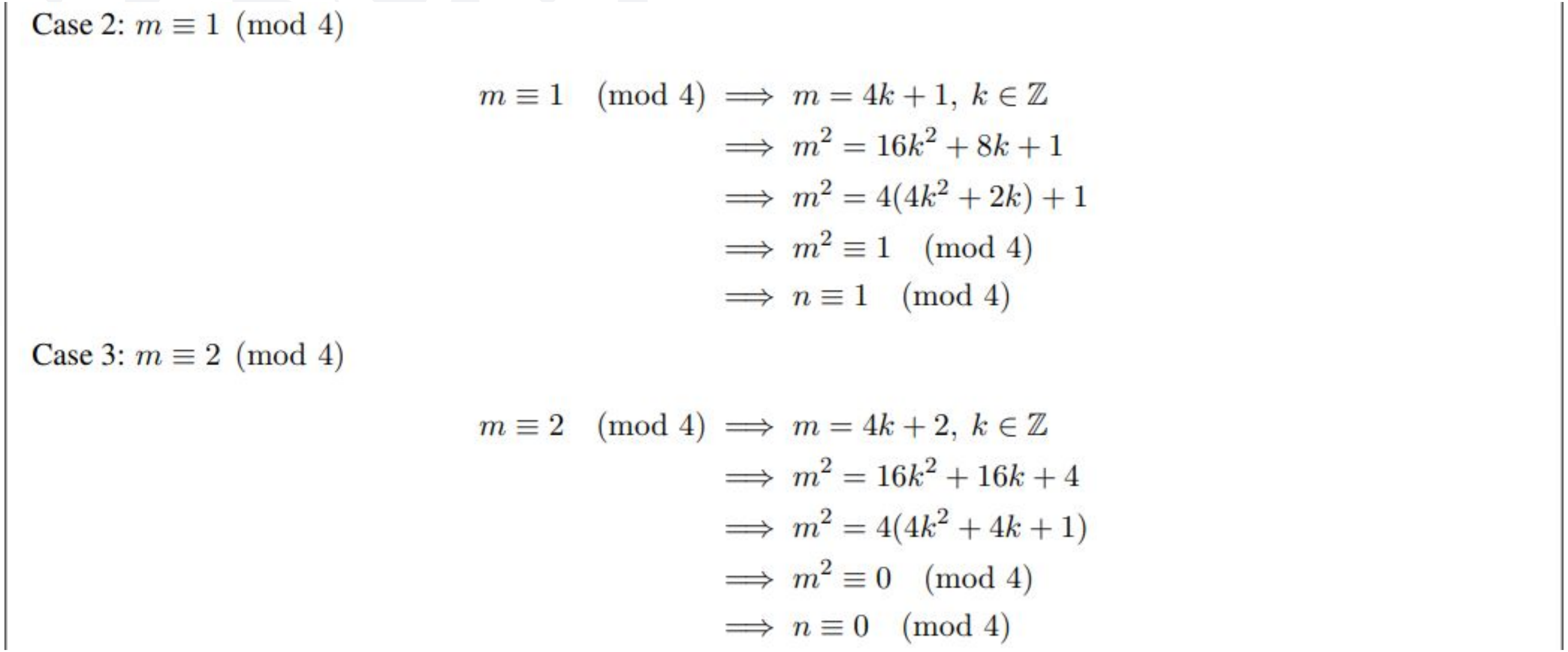
Prove that for any positive integer n, if n modulo 4 ($n\%4$ if you were writing Java) is 2 or 3 then n is not a perfect square. You are allowed to assume that a number when divided by 4 is either going to leave a remainder of 0, 1, 2, or 3.

Solution: Suppose for the sake of contradiction that there exists a positive integer n such that $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$, and $n = m^2$ for some integer m (take note of the notation!). Consider the following cases:

Case 1: $m \equiv 0 \pmod 4$

$$\begin{aligned} m \equiv 0 \pmod 4 &\implies m = 4k,\ k \in \mathbb{Z} \\ &\implies m^2 = 16k^2 \\ &\implies m^2 = 4(4k^2) \\ &\implies m^2 \equiv 0 \pmod 4 \\ &\implies n \equiv 0 \pmod 4 \end{aligned}$$

Answer 6 (cont.)



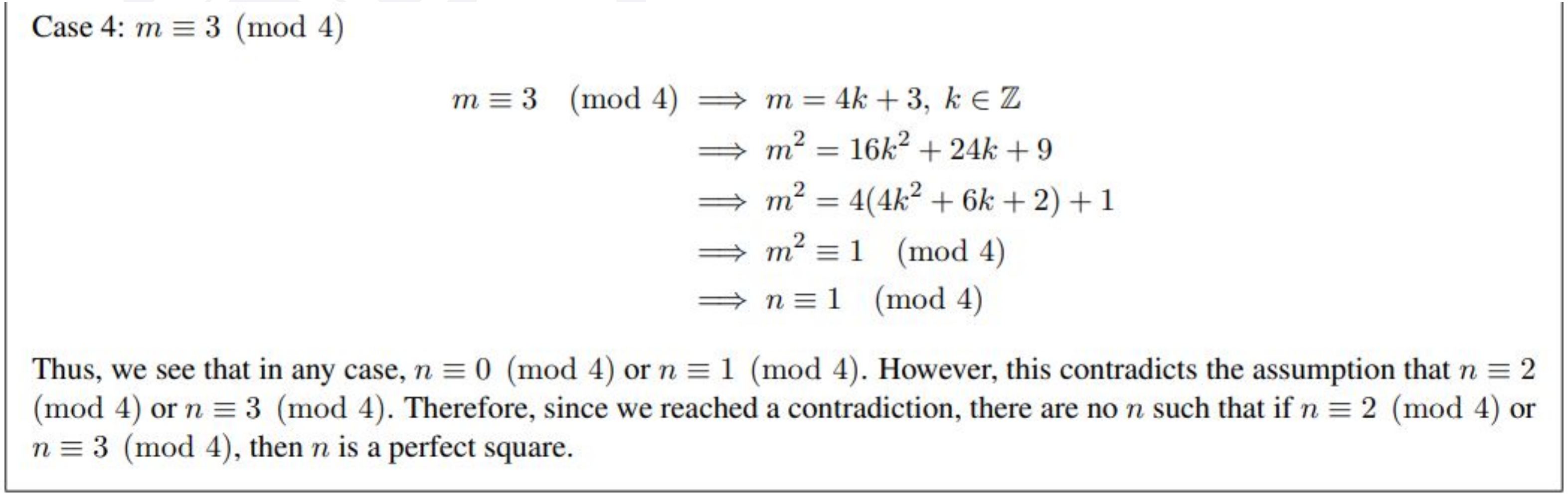
Case 2: $m \equiv 1 \pmod 4$

$$\begin{aligned} m \equiv 1 \pmod 4 &\implies m = 4k + 1,\ k \in \mathbb{Z} \\ &\implies m^2 = 16k^2 + 8k + 1 \\ &\implies m^2 = 4(4k^2 + 2k) + 1 \\ &\implies m^2 \equiv 1 \pmod 4 \\ &\implies n \equiv 1 \pmod 4 \end{aligned}$$

Case 3: $m \equiv 2 \pmod 4$

$$\begin{aligned} m \equiv 2 \pmod 4 &\implies m = 4k + 2,\ k \in \mathbb{Z} \\ &\implies m^2 = 16k^2 + 16k + 4 \\ &\implies m^2 = 4(4k^2 + 4k + 1) \\ &\implies m^2 \equiv 0 \pmod 4 \\ &\implies n \equiv 0 \pmod 4 \end{aligned}$$

Answer 6 (cont.)

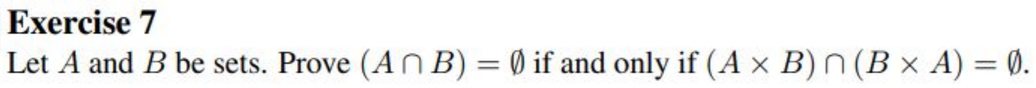


Case 4: $m \equiv 3 \pmod 4$

$$\begin{aligned} m \equiv 3 \pmod 4 &\implies m = 4k+3,\ k \in \mathbb{Z} \\ &\implies m^2 = 16k^2 + 24k + 9 \\ &\implies m^2 = 4(4k^2 + 6k + 2) + 1 \\ &\implies m^2 \equiv 1 \pmod 4 \\ &\implies n \equiv 1 \pmod 4 \end{aligned}$$

Thus, we see that in any case, $n \equiv 0 \pmod 4$ or $n \equiv 1 \pmod 4$. However, this contradicts the assumption that $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$. Therefore, since we reached a contradiction, there are no n such that if $n \equiv 2 \pmod 4$ or $n \equiv 3 \pmod 4$, then n is a perfect square.

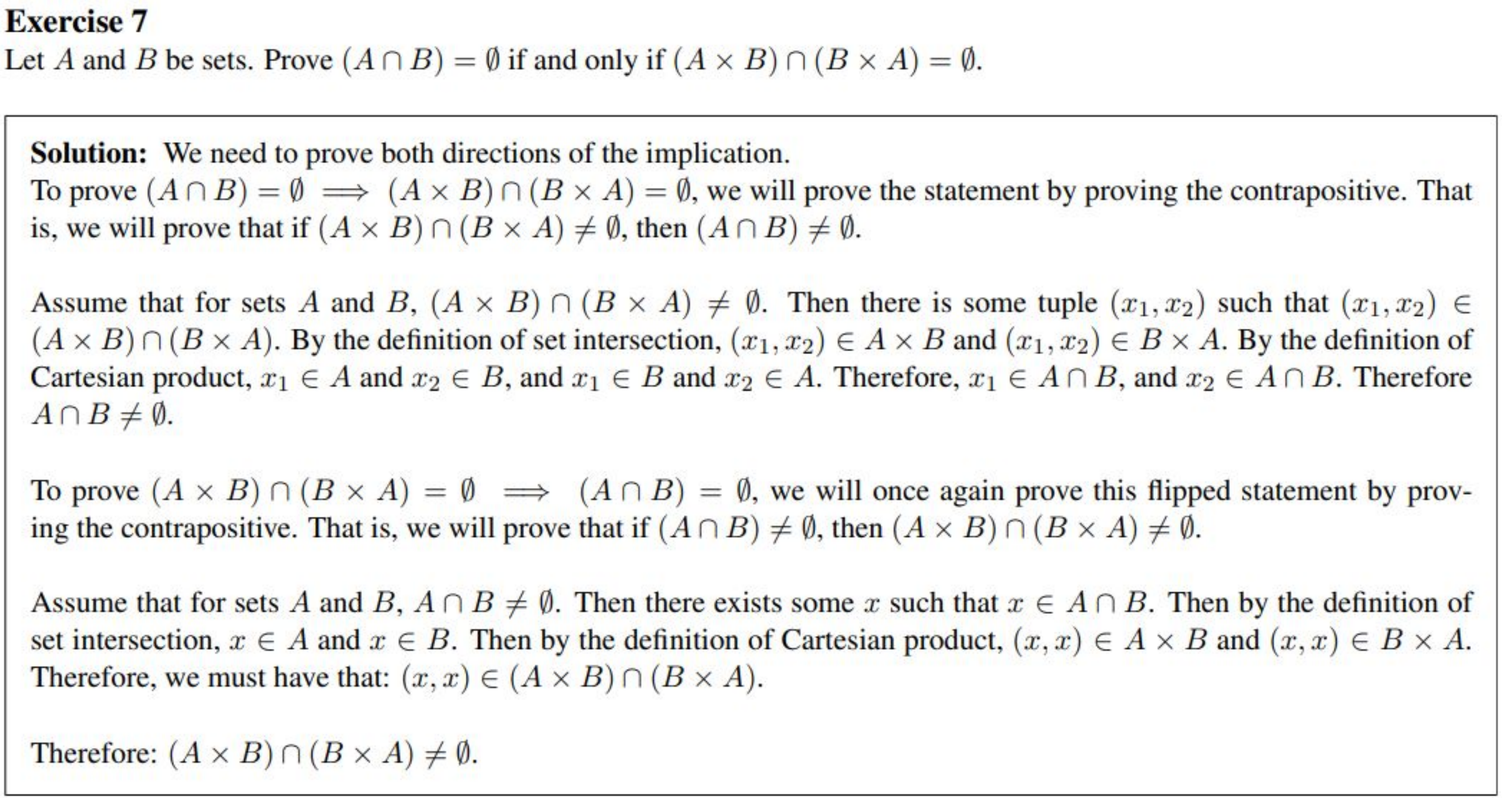
Question 6



Exercise 7

Let A and B be sets. Prove $(A \cap B) = \emptyset$ if and only if $(A \times B) \cap (B \times A) = \emptyset$.

Answer 6



Exercise 7

Let A and B be sets. Prove $(A \cap B) = \emptyset$ if and only if $(A \times B) \cap (B \times A) = \emptyset$.

Solution: We need to prove both directions of the implication.
To prove $(A \cap B) = \emptyset \implies (A \times B) \cap (B \times A) = \emptyset$, we will prove the statement by proving the contrapositive. That is, we will prove that if $(A \times B) \cap (B \times A) \neq \emptyset$, then $(A \cap B) \neq \emptyset$.

Assume that for sets A and B, $(A \times B) \cap (B \times A) \neq \emptyset$. Then there is some tuple (x_1, x_2) such that $(x_1, x_2) \in (A \times B) \cap (B \times A)$. By the definition of set intersection, $(x_1, x_2) \in A \times B$ and $(x_1, x_2) \in B \times A$. By the definition of Cartesian product, $x_1 \in A$ and $x_2 \in B$, and $x_1 \in B$ and $x_2 \in A$. Therefore, $x_1 \in A \cap B$, and $x_2 \in A \cap B$. Therefore $A \cap B \neq \emptyset$.

To prove $(A \times B) \cap (B \times A) = \emptyset \implies (A \cap B) = \emptyset$, we will once again prove this flipped statement by proving the contrapositive. That is, we will prove that if $(A \cap B) \neq \emptyset$, then $(A \times B) \cap (B \times A) \neq \emptyset$.

Assume that for sets A and B, $A \cap B \neq \emptyset$. Then there exists some x such that $x \in A \cap B$. Then by the definition of set intersection, $x \in A$ and $x \in B$. Then by the definition of Cartesian product, $(x, x) \in A \times B$ and $(x, x) \in B \times A$. Therefore, we must have that: $(x, x) \in (A \times B) \cap (B \times A)$.

Therefore: $(A \times B) \cap (B \times A) \neq \emptyset$.

See you next week!

Penn Engineering