

**Problem**

Prove that for all positive integers  $a$  and  $b$ ,  $a \mid b$  if, and only if,  $\gcd(a, b) = a$ .

**Solution****Part (a)**

Assume that  $a \mid b$ . We know that  $a \mid a$  and there can be no larger number than  $a$  that divides  $a$ . So  $a = \gcd(a, b)$ .

**Part (b)**

Assume that  $\gcd(a, b) = a$ . By definition of the gcd,  $a \mid b$ .

**Problem**

Prove the following statement. For all integers  $a, b$  and  $c$ , if  $a \mid b$  and  $a \mid c$  then  $a \mid (b - c)$  and  $a \mid (b + c)$ .

**Solution**

There exist integers  $n, m$  such that  $b = na$  and  $c = ma$ . Then

$$\begin{aligned} b - c &= na - ma \\ &= a(n - m) \end{aligned} \tag{1}$$

So  $a \mid (b - c)$ .

$$\begin{aligned} b + c &= na + ma \\ &= a(n + m) \end{aligned} \tag{2}$$

So  $a \mid (b + c)$ .

**Problem**

Prove that for ANY 4 digit nonnegative integer  $n$ , if the sum of the digits of  $n$  is divisible by 3, then  $n$  is divisible by 3.

**Solution**

Let the digits of some 4 digit number  $n$  be represented by  $a, b, c, d$ . Then

$$\begin{aligned} n &= a(1000) + b(100) + c(10) + d \\ &= a(999 + 1) + b(99 + 1) + c(9 + 1) + d \\ &= a(999) + b(99) + c(9) + a + b + c + d \\ &= (3(a(333) + b(33) + c(3)) + (a + b + c + d) \end{aligned} \tag{3}$$

The left component of the sum is divisible by three and thus for the entire sum to be divisible by 3 the right side,  $a + b + c + d$  (the sum of the digits of  $n$ ), must also be divisible by three.

## Problem

When an integer  $b$  is divided by 12, the remainder is 7. What is the remainder when  $8b$  is divided by 12?

## Solution

$$b = n(12) + 7 \tag{4}$$

$$\begin{aligned} 8b &= 8(n(12) + 7) \\ &= 8n(12) + 56 \\ &= (8n + 4)(12) + 8 \end{aligned} \tag{5}$$

So the remainder is 8.

## Problem

Prove that 3, 5, and 7 are the only prime numbers of the form  $p, p + 2$  and  $p + 4$ .

## Solution

Assume that there are 3 other primes of this form. Then  $3 \nmid p, 3 \nmid p + 2, 3 \nmid p + 4$ . If  $3 \nmid p$  then 3 must divide either  $p + 1$  or  $p + 2$ . We know that it doesn't divide  $p + 2$  so therefore it must divide  $p + 1$ . However, if  $p$  divides  $p + 1$  then it also divides  $p + 4$ . So the only way that these three numbers can be prime is if one of them is equal to 3. This is not the case when  $p + 2 = 3$  or when  $p + 4 = 3$  so the only situation that works is the one that was provided.

## Problem

Prove that  $\sqrt{5}$  is irrational.

## Solution

### Part (a)

Begin with the proposition that if  $5 \mid n^2$  then  $5 \mid n$ . This can be seen from Euclid's Lemma. If  $5 \mid n \cdot n$  then  $5 \mid n$ .

### Part (b)

Assume that  $\sqrt{5}$  is rational. Then it can be written in the form  $a/b$  for integers  $a$  and  $b$ . We can state that  $a$  and  $b$  have no common factors without loss of generality. Then

$$5 = (a/b)^2 \tag{6}$$

$$5 = (a^2/b^2) \tag{7}$$

$$5b^2 = a^2 \tag{8}$$

So 5 divides  $a^2$  and from our earlier proposition we know 5 divides  $a$ . This means that  $a$  can be written as  $5k$  for some integer  $k$ . Plugging it into the above equations we get

$$5b^2 = a^2 \tag{9}$$

$$5b^2 = (5k)^2 \tag{10}$$

$$5b^2 = 25k^2 \tag{11}$$

$$b^2 = 5k^2 \tag{12}$$

Thus 5 divides  $b^2$  and again by our earlier proposition we can say that 5 divides  $b$ . However, this contradicts our assertion that  $a$  and  $b$  had no common factors. Thus  $\sqrt{5}$  is irrational.

## Problem

Suppose  $((A \cap C) \subseteq (B \cap C))$  and  $((A \cup C) \subseteq (B \cup C))$ . Prove using a proof by cases that  $A \subseteq B$ . Be sure to state your assumptions and what you are proving, and to give a step-by-step proof with rules of inference, laws of equivalence, algebraic truths and/or other justifications required to make the logic of your proof perfectly clear.

## Solution

We are attempting to prove that every element  $a$  in  $A$  is also an element of  $B$ . In order to prove this we will consider two cases, when  $a$  is in  $C$  and when  $a$  is not in  $C$ .

(a) Case 1: Assume  $a \in C$

We know that  $a$  is in  $A$  and we have assumed that it is also in  $C$ . Then it is also in  $(A \cap C)$ . We are told  $(A \cap C)$  is a subset of  $(B \cap C)$  so every element of the former is an element of the latter. So  $a$  is an element of  $(B \cap C)$  and by the definition of set intersection it must be in  $B$ .

(b) Case 2: Assume  $a \notin C$

$a$  is an element of  $A$  so it is an element of  $(A \cup C)$ . We are told this set is a subset of  $(B \cup C)$ . This means that  $a$  is an element of  $(B \cup C)$ . By definition of set unions, every element of  $(B \cup C)$  is either a member of  $B$  or a member of  $C$ . We have assumed that  $a \notin C$  so therefore  $a$  must be in  $B$ .

We have shown that in all cases, for any arbitrary element  $a \in A$ ,  $a \in B$ . Therefore  $A$  is a subset of  $B$ .

## Problem

Prove by contradiction:

$$\text{If } (A \cap C) \subseteq B \wedge a \in C \text{ then } a \notin (A - B)$$

Be sure you justify every step of your proof with a rule of inference or law of equivalence or set definition. Rules of inference should be used when possible.

**Solution**

Assume that  $a \in (A - B)$ . By the definition of set difference  $a \in A$  and  $a \notin B$ . We are told that  $a \in C$ . Therefore, because it is in both  $A$  and  $C$  we know that  $a \in A \cap C$ . We are told that  $(A \cap C) \subseteq B$ . This means that every element of  $(A \cap C)$  is also an element of  $B$ .  $a$  is one such an element so  $a$  must be in  $B$ . This means that  $a \in B$ . This is a contradiction. Therefore  $a \notin (A - B)$  and the statement is proved.

**Problem**

What conclusion(s) can you draw from the following set of premises? Explain the rules of inference you apply in obtaining the conclusion(s).

$$(a) \neg p \implies r \wedge s$$

$$(b) t \implies s$$

$$(c) u \implies \neg p$$

$$(d) \neg w$$

$$(e) u \vee w$$

**Solution**

List of conclusions:

- |                      |  |
|----------------------|--|
| 1) $u$               | from d) and e) using conjunctive syllogism |
| 2) $\neg p$          | from 1) and c) using modus ponens          |
| 3) $r \wedge \neg s$ | from 2) and a) using modus ponens          |
| 4) $\neg s$          | from 3) using simplification               |
| 5) $r$               | from 3) using simplification               |
| 6) $\neg t$          | from 4) and b) using modus tollens         |

**Problem**

Use truth tables to determine which one of the following is a tautology and which one is a contradiction.

$$(a) (p \wedge q) \vee (\neg p \vee (p \wedge \neg q))$$

$$(b) (p \wedge \neg q) \wedge (\neg p \vee q)$$

**Solution****Part (a)**

$p$	$q$	$\neg q$	$\neg p$	$p \wedge q$	$p \wedge \neg q$	$\neg p \vee (p \wedge \neg q)$	$(p \wedge q) \vee (\neg p \vee (p \wedge \neg q))$
$F$	$F$	$T$	$T$	$F$	$F$	$T$	$T$
$F$	$T$	$F$	$T$	$F$	$F$	$T$	$T$
$T$	$F$	$T$	$F$	$F$	$T$	$T$	$T$
$T$	$T$	$F$	$F$	$T$	$F$	$F$	$T$

Regardless of the values of  $p$  and  $q$ ,  $(p \wedge q) \vee (\neg p \vee (p \wedge \neg q))$  is always true so it is a tautology.

**Part (b)**

$p$	$q$	$\neg p$	$\neg q$	$p \wedge \neg q$	$\neg p \vee q$	$(p \wedge \neg q) \wedge (\neg p \vee q)$
$F$	$F$	$T$	$T$	$F$	$T$	$F$
$F$	$T$	$T$	$F$	$F$	$T$	$F$
$T$	$F$	$F$	$T$	$T$	$F$	$F$
$T$	$T$	$F$	$F$	$F$	$T$	$F$

Regardless of the values of  $p$  and  $q$ ,  $(p \wedge \neg q) \wedge (\neg p \vee q)$  is always false so it is a contradiction.

**Problem**

Using existential instantiation, universal instantiation and existential generalization (and any other inference rules necessary), prove

$$\forall x P(x) \wedge \exists x Q(x) \implies \exists x (P(x) \wedge Q(x))$$

**Solution**

By existential instantiation we can say that  $\forall x P(x)$  there is a  $c$  such that  $Q(c)$ . By universal instantiation we can say that for any arbitrary  $y \in U$   $P(y)$ .  $c$  is a possible value of  $y$  and so we can say that  $P(c) \wedge Q(c)$ . By existential generalization we can conclude that  $\exists x (P(x) \wedge Q(x))$ .

**Problem**

"Do you mean that you think you can find out the answer to it" said the March Hare. "Exactly so," said Alice. "Then you should say what you mean," the March Hare went on. "I do," Alice hastily replied; "at least-at least I mean what I say-that's the same thing, you know." "Not the same thing a bit!" said the Hatter. "Why you might just as well say that 'I see what I eat' is the same thing as 'I eat what I see'!"

-from "A Mad Tea-Party" in *Alice in Wonderland*, by Lewis Carroll

The Hatter is correct. "I say what I mean" is not the same thing as "I mean what I say." Rewrite each of these two sentences in if-then form and explain the logical relation between them. Also, write the negation of each if-then statement.

**Solution**

(a) “I say what I mean.” = If I mean something then I say it.”

(b) “I mean what I say.” = If I say something then I mean it.”

They are converses of each other. The inverse of a) is “If I don’t mean something then I don’t say it.” The inverse of b) is “If I don’t say something then I don’t mean it.”