Homework 5

Mark Petersen

Sections 8 and 9

8. Proof By Cases

Exercise 8.1. Let $x, y \in \mathbb{Z}$. Prove that if x and y have the same parity, then $x^2 + xy$ is even.

Proof: We directly suppose that x and y have the same parity, and prove this for the case of even and odd parity.

Case 1. Suppose x and y are even such that $x = 2k$ and $y = 2l$ for some $k, l \in \mathbb{Z}$. Then,

$$\begin{aligned} x^2 + xy &= 4k^2 + 4kl \\ &= 2\left(2k^2 + 2kl\right), \end{aligned}$$

which is even.

Case 2. Suppose x and y are odd such that $x = 2k+1$ and $y = 2l+1$ for some $k, l \in \mathbb{Z}$. Then

$$\begin{aligned} x^2 + xy &= 4k^2 + 4k + 1 + 4kl + 2k + 2l + 1 \\ &= 2\left(2k^2 + 4k + 4l + 2kl + 1\right), \end{aligned}$$

which is even.

Therefore, if x and y have the same parity, then $x^2 + xy$ is even.

■

Exercise 8.2. Let $a, b, c \in \mathbb{Z}$. Prove that if $a \nmid bc$, then $a \nmid b$ and $a \nmid c$.

Proof: We contrapositively suppose that if $a \mid b$ or $a \mid c$ then $a \mid bc$. We break this down into two cases.

Case 1. Suppose that $a \mid b$ then by definition $b = am$ for some $m \in \mathbb{Z}$, then $bc = amc$ which a is a divisor of.

Case 2. Suppose that $a \mid c$. This case is similar to the first.

Since the statement $a \mid b$ or $a \mid c$ then $a \mid bc$ is true, the original statement is true.

■

Exercise 8.3. Prove that given $x \in \mathbb{Z}$, either $x^2 \equiv 0 \mod 4$ or $x^2 \equiv 1 \mod 4$. Using this, prove that for any integer x we have $4 \mid \left(x^4 - x^2\right)$.

Proof: The value of x can be written as $4k$, $4k+1$, $4k+2$, or $4k+3$ for some $k \in \mathbb{Z}$. We prove the statement directly by proving the following four cases.

Case 1. Suppose $x = 4k$, then $x^2 = 16k^2$. Since $4 \mid 16k^2 - 0$, $x^2 \equiv 0 \mod 4$.

Case 2. Suppose $x = 4k+1$, then $x^2 = 16k^2 + 8k + 1$. Since $4 \mid 16k^2 + 8k + 1 - 1$, $x^2 \equiv 1 \mod 4$.

Case 3. Suppose $x = 4k+2$, then $x^2 = 16k^2 + 16k + 4$. Since $4 \mid 16k^2 + 16k + 4 - 0$, $x^2 \equiv 0 \mod 4$.

Case 4. Suppose $x = 4k+3$, then $x^3 = 16k + 24k + 9$. Since $4 \mid 16k + 24k + 9 - 1$, $x^2 \equiv 1 \mod 4$.

Since all four cases hold, the statement is true.

■

The second portion of this problem is to prove that given $x \in \mathbb{Z}$, then $4 \mid \left(x^4 - x^2\right)$.

Proof: We directly suppose that $x \in \mathbb{Z}$. Using the information from the previous proof we know that either $x^2 \equiv 0 \mod 4$ or $x^2 \equiv 1 \mod 4$. This gives us two cases that we can prove separately.

Case 1. Suppose directly that $x^2 \equiv 0 \mod 4$. This means that $4 \mid x^2$, in other words $x^2 = 4a$ for some $a \in \mathbb{Z}$. Let us simplify the expression $4 \mid \left(x^4 - x^2\right)$ which can be written as $4 \mid x^2\left(x^2 - 1\right)$ and is equivalent to saying $x^2\left(x^2 - 1\right) = 4c$ for some $c \in \mathbb{Z}$. Using the fact that $x^2 = 4a$ we get $4a\left(x^2 - 1\right) = 4c$ which is true.

Case 2. Suppose directly that $x^2 \equiv 1 \mod 4$. This indicates that $4 \mid x^2 - 1$, in other words $x^2 - 1 = 4a$ for some $a \in \mathbb{Z}$. We showed earlier that the statement $4 \mid \left(x^4 - x^2\right)$ can be written as $4 \mid x^2\left(x^2 - 1\right)$ and is equivalent to saying $x^2\left(x^2 - 1\right) = 4c$ for some $c \in \mathbb{Z}$. Using the fact that $x^2 - 1 = 4a$ we get $x^2 4a = 4c$ which is true.

Since both cases are true, given $x \in \mathbb{Z}$, then $4 \mid \left(x^4 - x^2\right)$.

■

Exercise 8.4. Let $a, b, c, n \in \mathbb{Z}$. If $a \equiv b \mod n$ and $b \equiv c \mod n$, show that $a \equiv c \mod n$. If we know $11 \equiv -3 \mod 7$ and $-3 \equiv 4 \mod 7$, can we say that $11 \equiv 4 \mod 7$?

Proof: We suppose directly that $a \equiv b \mod n$ which implies $n \mid (a - b)$ which is equivalent to saying that $a - b = ng$ for some $g \in \mathbb{Z}$. Solving for b we get $b = a - ng$. We can use this identity in the statement $b \equiv c \mod n$ by writing the equivalent form $b - c = nl$ for some $l \in \mathbb{Z}$, and substituting in $a - ng$ for b to get

$$\begin{aligned} b - c &= nl \\ a - ng - c &= nl \\ a - c &= nl + ng \\ a - c &= n\left(l + g\right), \end{aligned}$$

which implies $n \mid a - c$ or equivalently $a \equiv c \mod n$. And of course this proof shows that the answer to the question is yes. ■

Exercise 8.5. Prove, for any $n \in \mathbb{Z}$, that $3 \mid n$ if and only if $3 \mid n^2$.

Proof: This is a biconditional, so we will prove both direction.

$(\implies)$: We begin by showing directly that if $3 \mid n$ then $3 \mid n^2$. $3 \mid n$ is equivalent to saying $n = 3c$ for some $c \in \mathbb{N}$. Substituting this in for n^2 yields $n^2 = 3\left(3c^2\right)$ which shows that $3 \mid n^2$.

$(\impliedby)$: Next we show directly by cases that if $3 \mid n^2$ then $3 \mid n$. An integer n can be written as either $3k$, $3k + 1$, or $3k + 2$ for some $k \in \mathbb{N}$. Only in the case $n = 3k$ is $3 \mid n$. Thus we need to show that in the other two cases, that $3 \mid n^2$ is false.

Case 1. Suppose $n = 3k$, substituting this into the statement $3 \mid n^2$ yields $3 \mid 3\left(3k^2\right)$. Which is true.

Case 2. Suppose $n = 3k+1$, substituting this into the statement $3 \mid n^2$ yields $3 \mid \left(3\left(3k^2 + 2k\right) + 1\right)$ which is false since 3 does not divide 1.

Case 3. Suppose $n = 3k + 2$, substituting this into the statement $3 \mid n^2$ yields $3 \mid \left(3\left(3k^2 + 4k\right) + 2\right)$ which is false since 3 does not divide 2.

Therefore if $3 \mid n^2$, then $3 \mid n$, which completes the proof.

■

Exercise 8.6. Prove $3 \mid \left(2n^2+1\right)$ if and only if $3 \nmid n$, for $n \in \mathbb{Z}$.

Proof: This is a biconditional, so we will prove both direction.
$(\implies)$: We suppose contrapositively that $3 \mid n$ such that $n = 3a$ for some $a \in \mathbb{Z}$. Substituting this into $2n^2+1$ yields

$$\begin{aligned} 2n^2+1 &= 18a^2+1 \\ &= 3\left(6a^2\right)+1, \end{aligned}$$

which does not divide by 3 since 1 does not divide by 3. Therefore if $3 \mid \left(2n^2+1\right)$, then $3 \nmid n$.
$(\impliedby)$: We suppose directly that $3 \nmid n$. This means that the integer n can be written as either $n = 3k+1$ or $3k+2$ for some $k \in \mathbb{N}$. If the statement holds for both cases, then it is true.

Case 1. We assume that $n = 3k+1$. Substituting this into $2n^2+1$ yields

$$\begin{aligned} 2n^2+1 &= 2\left(9k^2+6k+1\right)+1 \\ &= 18k^2+12k+3 \\ &= 3\left(6k^2+4k+1\right), \end{aligned}$$

which does divide by 3.

Case 2. We assume that $n = 3k+2$. Substituting the value of n into $2n^2+1$ yields

$$\begin{aligned} 2n^2+1 &= 2\left(9k^2+12k+4\right)+1 \\ &= 18k^2+24k+9 \\ &= 3\left(6k^2+8k+3\right), \end{aligned}$$

which does divide by 3.

Since both cases hold, if $3 \nmid n$ then $3 \mid \left(2n^2+1\right)$.

■

Exercise 8.7. Let $a, b, c, d, n \in \mathbb{Z}$. If $a \equiv b \mod n$ and $c \equiv d \mod n$, prove that $ac \equiv bd \mod n$. What does this statement say if we take $c = a$ and $d = b$? We know that $19 \equiv 5 \mod 7$. Do we then know $19^2 \equiv 5^2 \mod 7$. How about $19^3 \equiv 5^3 \mod 7$?.

Proof: We suppose directly that $a \equiv b \mod n$ and $c \equiv d \mod n$, which is equivalent to supposing $a - b = ng$ and $c - d = nk$ for some $k, g \in \mathbb{Z}$. Solving for a and c gives us $a = ng + b$ and $c = nk + d$. Multiplying a and c yields

$$ac = ngnk - dng - bnk + bd,$$

which can be written as

$$\begin{aligned} ad - bd &= ngnk - dng - bnk \\ &= n\left(ngk - dg - bk\right). \end{aligned}$$

This shows that $n \mid ad - bd$, or equivalently $ac \equiv bd \mod n$. ■

Under the conditions that $c = a$ and $d = b$, the statement that we proves says that $a^2 \equiv b^2 \mod n$. This means that if $19 \equiv 5 \mod 7$ then $19^2 \equiv 5^2 \mod 7$. To show that $19^3 \equiv 5^3 \mod 7$, suppose $a - b = ng$ for some $g \in \mathbb{Z}$. Then

$$\begin{aligned} a^3 &= n^3g^3 + n^2g^2b + 2n^2g^2b + 2ngb^2 + ngb^2 + b^3 \\ &= n\left(n^2g^3 + 3ng^2b + 3gb^2\right) + b^3, \end{aligned}$$

which can be written as

$$a^3 - b^3 = n\left(n^2g^3 + 3ng^2b + 3gb^2\right).$$

This shows that if $a \equiv b \mod n$, then $a^3 \equiv b^3 \mod n$, thus $19^3 \equiv 5^3 \mod 7$.

Exercise 8.8. Prove Theorem 8.22 for any $x, y \in \mathbb{R}$, we have $|xy| = |x|\,|y|$.

Proof: We show this directly by considering the four case.

Case 1. Suppose that $x \geq 0$ and $y \geq 0$, then $xy \geq 0$, $xy = |xy|$, $|x| = x$, and $|y| = y$, thus showing that$|xy| = |x|\,|y|$.

Case 2. Suppose that $x < 0$ and $y < 0$, then $xy > 0$, $xy = |xy|$, $|x| = -x$, and $|y| = -y$. Therefore we have

$$\begin{aligned} xy &= -|x|\left(-|y|\right) \\ &= |x|\,|y|, \end{aligned}$$

thus showing that $|xy| = |x|\,|y|$.

Case 3. Suppose that $x \geq 0$ and $y < 0$, then $xy \leq 0$, $xy = -|xy|$, $|x| = x$, and $|y| = -y$. Therefore $xy = -|x|\,|y|$, which shows that $|x|\,|y| = |xy|$.

Case 4. Suppose that $x < 0$ and $y \geq 0$. This case is similar to the previous one.

Since all four cases hold, we have shown that $|xy| = |x|\,|y|$.

■

Exercise 8.9. Let $a \in \mathbb{R}$. Prove that $a^2 \leq 1$ if and only if $-1 \leq a \leq 1$.

Proof: This is biconditional so we show both ways.

$(\implies)$: We assume directly that $a^2 \leq 1$. Taking the square root of both sides gives us $|a| \leq 1$. We have two cases to show.

Case 1. Suppose that $a \geq 0$, then $|a| = a$ and $a \leq 1$.

Case 2. Suppose that $a \leq 0$, then $|a| = -1$ and $a \geq -1$.

Regardless of the case, $-1 \leq a \leq 1$. This shows that if $a^2 \leq 1$, then $-1 \leq a \leq 1$.

$(\impliedby)$: We assume contrapositively that if $a^2 > 1$, then $a > 1$ or $a < -1$. Taking the square root of both side of $a^2 > 1$ gives us $|a| > 1$. We have two cases to show.

Case 1. Suppose that $a \geq 0$, then $|a| = 1$ and $a > 1$.

Case 2. Suppose that $a \leq 0$, then $|a| = -1$ and $a < -1$.

Regardless of the case, $a > 1$ or $a < -1$ if $a^2 > 1$, thus proving contrapositively that if $a^2 \leq 1$, then $-1 \leq a \leq 1$. This completes the proof.

■

9. Proof by Contradiction

Exercise 9.1. Let R and S be statements. Draw a truth table with columns labeled R, S, $\neg R$ and $(\neg R) \implies S$. Verify that the only row where S is false and $(\neg R) \implies S$ is true occurs when R is true.

R	S	$\neg R$	$\neg R \implies S$
T	T	F	T
T	F	F	T
F	T	T	T
F	F	T	F

Exercise 9.2. Prove the following statement directly, contrapositively, and by contradiction. Give $x \in \mathbb{Z}$, if $3x + 1$ is even, then $5x + 2$ is odd.

Before we show the main proof, we begin with the following lemma.

Lemma 9.3. *If $3x + 1$ is even then x is odd.*

Proof: We suppose contrapositively that x is even such that $x = 2k$ for some $k \in \mathbb{Z}$. Substituting this into $3x + 1$ gives us

$$\begin{aligned} 3x + 1 &= 6k + 1 \\ &= 2(3k) + 1, \end{aligned}$$

which is odd. Thus if $3x + 1$ is even then x is odd. ■

Lemma 9.4. *If $5x + 2$ is even, then x is even.*

Proof: We suppose contrapositively that x is odd such that $x = 2k + 1$ for some $k \in \mathbb{Z}$. Substituting this into $5x + 1$ gives us

$$\begin{aligned} 5x + 2 &= 10k + 7 \\ &= 2(5k + 3) + 1, \end{aligned}$$

which is odd. Thus if $5x + 2$ is even, then x is even. ■

a) **Directly**
Proof: We suppose directly that $3x + 1$ is even. According to lemma 9.3, x is odd which is equivalent to saying that $x = 2k + 1$ for some $k \in \mathbb{Z}$. Substituting this into $5x + 2$ gives

$$\begin{aligned} 5x + 2 &= 5(2k + 1) + 2 \\ &= 10k + 6 \\ &= 2(5k + 3) \end{aligned}$$

which is even. ■

b) **Contrapositively**
Proof: We suppose contrapositively that $5x+2$ is even. According to lemma 9.4, x is even which is equivalent to saying that $x = 2k$ for some $k \in \mathbb{Z}$. Substituting this into $3x + 1$ gives

$$\begin{aligned} 3x + 1 &= 6k + 1 \\ &= 2(3k) + 1, \end{aligned}$$

which is odd. Which shows that if $5x + 2$ is even, then $3x + 1$ is odd. ■

c) **Contradiction**
Proof: By contradiction we suppose that $3x + 1$ is even and $5x + 2$ is even. According to lemma 9.3, x is odd which is equivalent to saying that $x = 2k + 1$ for some $k \in \mathbb{Z}$. Substituting this into $3x + 1$ and $5x + 2$ give us

$$\begin{aligned} 3x + 1 &= 6k + 4 \\ &= 2(3k + 2), \end{aligned}$$

which is even, and

$$\begin{aligned} 5x + 2 &= 5(2k + 1) + 2 \\ &= 10k + 7 \\ &= 2(5k + 3) + 1, \end{aligned}$$

which is odd

$$\rightarrow\leftarrow$$

■

Exercise 9.5. Prove, by way of contradiction, the following statement: Given $a, b, c \in \mathbb{Z}$ with $a^2 + b^2 = c^2$, then a is even or b is even.

Proof: By contradiction we suppose that $a^2 + b^2 = c^2$, a is odd and b is odd. For some $k, l \in \mathbb{Z}$, $a = 2k + 1$ and $b = 2l + 1$. Substituting these into $a^2 + b^2 = c^2$ yields

$$\begin{aligned} a^2 + b^2 = c^2 &= 4k^2 + 4k + 1 + 4l^2 + 4l + 1 \\ &= 4\left(k^2 + l^2\right) + 4\left(k + l\right) + 2 \\ &= 4\left(k + l\right)^2 - 4\left(k + l\right) + 2 \\ &= 4x^2 - 4x + 2. \end{aligned}$$

In order for $c^2 = 4x^2 - 4x + 2$, there must exist a number $(x + y)$, where $y \in \mathbb{Z}$, such that $(x + y)^2 = x^2 - x + \frac{1}{2}$. Factoring out the term $(x + y)^2$ gives us

$$(x + y)^2 = x^2 + 2xy + y^2,$$

which creates the system of equations

$$\begin{aligned} 2xy &= -x \\ y &= -\frac{1}{2} \end{aligned}$$

and

$$\begin{aligned} y^2 &= \frac{1}{2} \\ |y| &= \frac{1}{\sqrt{2}}, \end{aligned}$$

which is contradictory. Thus there is not an integer that is the square root of $4x^2 - 4x + 2$ for all $x \in \mathbb{Z}$. In other words the statement $c^2 = 4x^2 - 4x + 2$ is false. This proves that given $a, b, c \in \mathbb{Z}$ with $a^2 + b^2 = c^2$, then a is even or b is even. ■

Exercise 9.6. Prove that $\sqrt{3}$ is irrational.

Proof: We assume by contradiction that $\sqrt{3}$ is rational, and thus can be written as $\frac{a}{b}$ where $a \in \mathbb{Z}$ and $b \in \mathbb{Z} - \{0\}$. We assume that $\frac{a}{b}$ is in lowest terms. By squaring and clearing by denominators we have $a^2 = 3b^2$. Thus $3 \mid a^2$, and hence $3 \mid a$. We can write $a = 3x$ for some $x \in \mathbb{Z}$. Plugging $a = 3x$ into the equality $a^2 = 3b^2$ yields $9a^2 = 3b^2$, or in other words $b^2 = 3a^2$ which means that $3 \mid b^2$, and hence $3 \mid b$. However, note both a and b can be divided by 3 which contradicts the fact that $\frac{a}{b}$ was assumed to be in lowest terms. Hence $\sqrt{3}$ is irrational. ■

Exercise 9.7. Prove that $\sqrt[3]{2}$ is irrational.

Proof: We assume by contradiction that $\sqrt[3]{2}$ is rational. And thus can be written as $\frac{a}{b}$ where $a \in \mathbb{Z}$ and $b \in \mathbb{Z} - \{0\}$. We assume that $\frac{a}{b}$ is in lowest terms. By cubing and clearing by denominators we have $a^3 = 2b^3$. Thus $2 \mid a^3$, and hence $2 \mid a$. We can write $a = 2x$ for some $x \in \mathbb{Z}$. Plugging $a = 2x$ into the equality $a^3 = 2b^3$ yields $8a^3 = 2b^3$, or in other words $b^3 = 2\left(2a^3\right)$ which means that $2 \mid b^3$, and hence $2 \mid b$. However, note both a and b can be divided by 2 which contradicts the fact that $\frac{a}{b}$ was assumed to be in lowest terms. Hence $\sqrt[3]{2}$ is irrational. ■

Exercise 9.8. Prove if $x \in \mathbb{Q}$ and $y \in \mathbb{R} - \mathbb{Q}$, then $x + y \in \mathbb{R} - \mathbb{Q}$.

Proof: We assume by contradiction that $x \in \mathbb{Q}$ and $y \in \mathbb{R} - \mathbb{Q}$ and $x + y \notin \mathbb{R} - \mathbb{Q}$. Since x is a rational number it can be written as $\frac{a}{b}$ for some $a \in \mathbb{Z}$ and

$b \in \mathbb{Z} - \{0\}$, and since $x + y$ is rational, it can be written as $\frac{c}{d}$ for some $c \in \mathbb{Z}$ and $d \in \mathbb{Z} - \{0\}$. We can solve for y by subtracting $\frac{a}{b}$ from $\frac{c}{d}$ which yields $\frac{cb-ad}{bd}$ which must be rational and hence $y \notin \mathbb{R} - \mathbb{Q}$. ∎

Exercise 9.9. Prove: If we are given a nonzero rational number x and an irrational number y, then the number xy is irrational.

Proof: We assume by contradiction that $x \in \mathbb{Q} - \{0\}$, $y \in \mathbb{R} - \mathbb{Q}$ and $xy \in \mathbb{Q}$. The rational number x can be written as $\frac{a}{b}$ for some $a, b \in \mathbb{Z} - \{0\}$, and the rational number xy can be written as $\frac{c}{d}$ for some $c \in \mathbb{Z}$ and $d \in \mathbb{Z} - \{0\}$. Solving for y yields

$$\begin{aligned} y &= xy/x \\ &= \frac{c}{d}\frac{b}{a} \\ &= \frac{cb}{da}, \end{aligned}$$

which is rational. This is contradictory since y was stated to be irrational. Therefore if $x \in \mathbb{Q}$ and $y \in \mathbb{R} - \mathbb{Q}$, then $x + y \in \mathbb{R} - \mathbb{Q}$. ∎

Exercise 9.10. Prove there is no smallest positive irrational number.

Proof: We suppose by contradiction that there is a smallest positive irrational number z. We know from the previous proof that given a nonzero rational number x and an irrational number y, then the number xy is irrational. Thus xz must be irrational. Let $x = \frac{1}{b}$ such that $b \in \{x \in \mathbb{Z}, x > 1\}$, then $xz > 0$, is still positive and an irrational number. In fact $xz = \frac{z}{b}$ which must be smaller than z. This is contradictory to our assumption that z was the smallest positive irrational number. Thus there is not smallest positive irrational number. ∎

Example 9.11. Given $x, y \in \mathbb{Z}$, prove that $33x + 132y \neq 57$.

Proof: We suppose by contradiction that $33x + 132y = 57$ which can be written $33\,(x + 4y) = 57$ or equivalently as

$$x + 4y = \frac{19}{11}.$$

Solving for x yields $x = \frac{19}{11} - 4y$ which is not an integer since $\frac{19}{11}$ is not an integer. Therefore $33x + 132y \neq 57$ if x and y are integers. ∎