Section 4.6

Sterling Jeppson

October 24, 2020

Problem 1

Theorem: There is no least positive real number.

Proof. Suppose not. That is, suppose that there is a least positive real number x. We must deduce a contradiction. Consider the number $x/2$. Since x is a positive real number, $x/2$ is also a positive real number. In addition, we can deduce that $x/2 < x$ by multiplying both sides of the inequality 1 ¡ 2 by x and dividing by 2. Hence $x/2$ is a real number that is less than the least positive real number. This is a contradiction. Thus the supposition is false and so there is no least positive real number. □

Problem 2

Is $\frac{1}{0}$ an irrational number? Explain.

Solution

No. Suppose that $\frac{1}{0} = x$ such that x is a real number. x cannot be a rational number as it is a quotient of two integers with the denominator equal to 0. Thus if x is a real number and x is not rational then x must be rational. Now $0 \cdot x = 0 = 1$. This is a contradiction. Hence $\frac{1}{0}$ is not an irrational number.

Problem 3

Use proof by contradiction to show that for all integers n, $3n+2$ is not divisible by 3.

Theorem: For all integers n, $3n+2$ is not divisible by 3.

Proof. Suppose not. That is suppose that there exists an integer n such that $3 \mid (3n+2)$. Then $3n+2 = 3k$. for some integer k.

$$\begin{aligned} 3n+2 &= 3k \\ 2 &= 3n-3k \\ 2 &= 3(n-k) \end{aligned}$$

It follows that $3 \mid 2$. But theorem 4.3.1 states that if a and b are positive integers and $a \mid b$ then $a \leq b$. This is a contradiction. Thus the supposition is false and the theorem is true. $\square$

Problem 4

Use proof by contradiction to show that for all integers m, $7m+4$ is not divisible by 7.

Theorem: For all integers m, $7m + 4$ is not divisible by 7.

Proof. Suppose not. That is suppose that there exists an integer m such that $7 \mid (7m + 4)$. Then $7m + 4 = 7k$ for some integer k.

$$
\begin{aligned}
7m + 4 &= 7k \\
4 &= 7k - 7m \\
4 &= 7(k - m)
\end{aligned}
$$

It follows that $7 \mid 4$. But theorem 4.3.1 states that if a and b are positive integers and $a \mid b$ then $a \leq b$. This is a contradiction. Thus the supposition is false and the theorem is true. $\square$

Problem 5

Prove that there is no greatest even integer.

Theorem: There is no greatest even integer.

Proof. Suppose not. That is suppose that there exists an integer n such that n is even and n is the largest even integer. It follows from definition of even that $n = 2k$ for some integer k. Let $m = n + 2$. Now m is an integer as it is a sum of integers. By substitution,

$$
\begin{aligned}
m &= n + 2 \\
&= 2k + 2 \\
&= 2(k + 1)
\end{aligned}
$$

It follows that m is even as $m = 2(k+1)$ and $k+1$ is an integer as $k+1$ is a sum of integers. Now m is even and $m > n$, but n is the greatest even integer. This is a contradiction. Thus the supposition is false and the theorem is true. $\square$

Problem 6

Prove that there is no greatest negative real number.

Theorem: There is no greatest negative real number.

Proof. Suppose not. That is suppose that there exists a greatest negative real number x. We must deduce a contradiction. Consider the negative real number, $x/2$. Since x is a negative real number, $x/2$ is also a negative real number. In addition, we can deduce that $x/2 > x$ by multiplying both sides of the inequality $1 < 2$ by x and dividing by 2. Hence $x/2$ is a negative real number that is greater than the greatest negative real number. This is a contradiction. Thus the supposition is false and the theorem is true. □

Problem 7

Prove that there is no least positive rational number.

Theorem: There is no least positive rational number.

Proof. Suppose not. That is suppose that there exists a least positive rational number r. We must deduce a contradiction. Since r is rational $r = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Consider the positive rational number $r/2$. Since r is a positive rational number, $r/2$ is also a positive rational number as $\frac{r}{2} = \frac{a/b}{2} = \frac{a}{2b}$ which are both integers with $2b \neq 0$ by the zero product property. In addition we can deduce that $r/2 < r$ by multiplying both sides of the inequality $1 < 2$ by r and dividing by 2. Hence $r/2$ is a positive number that is less than less than the least positive rational number. This is a contradiction. Thus the supposition is false and the theorem is true. □

Problem 8

Theorem: The difference of any rational number and any irrational number is irrational.

Proof. Suppose not. That is suppose that there exists a rational number x and and irrational number y such that $x - y$ is rational. By definition of rational, there exists integers a, b, c, and d with $b \neq 0$ and $d \neq 0$ so that $x = \frac{a}{b}$ and $x - y = \frac{c}{d}$. By substitution,

$$\frac{a}{b} - y = \frac{c}{d}$$

Adding y and subtracting $\frac{c}{d}$ on both sides gives

$$\begin{aligned} y &= \frac{a}{b} - \frac{c}{d} \\ &= \frac{ad}{bd} - \frac{bc}{bd} \\ &= \frac{ad - bc}{bd} \end{aligned}$$

Now both $ad - bc$ and bd are integers because products and differences of integers are integers. And $bd \neq 0$ by the zero product property. Hence y is a ratio of integers with a nonzero denominator, and thus y is rational by the definition of rational. We therefore have that y is irrational and that y is rational, which is a contradiction. Thus the supposition is false and the theorem is true. □

Problem 9

(a) when asked to prove that the difference of any irrational number and any rational number is irrational, a student began, "Suppose not. That is, suppose the difference of any irrational number and any rational number is rational." What is wrong with beginning the proof in this way?

(b) Prove that the difference of any irrational number and any rational number is irrational.

Solution

(a) Beginning a proof by contradiction requires that you take the logical negation of the statement to be proved. However the student did perform the logical negation correctly. The correct logical negation of a universal statement is an existential statement. Thus the logical negation should be, there exists an irrational number and a rational number such that their difference is rational.

(b) *Theorem*: The difference of any irrational number and any rational number is irrational.

Proof. Suppose not. That is suppose that there exists an irrational number x and a rational number y such that $x - y$ is rational. By definition of rational, there exists integers a, b, c, and d with $b \neq 0$ and $d \neq 0$ so that $y = \frac{a}{b}$ and $x - y = \frac{c}{d}$. By substitution,

$$x - \frac{a}{b} = \frac{c}{d}$$

Adding $\frac{a}{b}$ to both sides gives

$$\begin{aligned} x &= \frac{a}{b} + \frac{c}{d} \\ &= \frac{ad}{bd} + \frac{bc}{bd} \\ &= \frac{ad + bc}{bd} \end{aligned}$$

Now both $ad+bc$ and bd are integers because products and sums of integers are integers. And $bd \neq 0$ by the zero product property. Hence x is a ratio of two integers with a nonzero denominator, and thus x is rational by the definition of rational. We therefore have that x is rational and that x is irrational, which is a contradiction. Thus the supposition is false and the theorem is true. □

Problem 10

Prove that the square root of any irrational number is irrational.

Theorem: The square root of any irrational number is irrational.

Proof. Suppose not. That is suppose that there exists an irrational number x such that $\sqrt{x}$ is rational. By definition of rational $\sqrt{x} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. By substitution,

$$\begin{aligned} x &= (\sqrt{x})^2 \\ &= \left(\frac{a}{b}\right)^2 \\ &= \left(\frac{a^2}{b^2}\right) \end{aligned}$$

Now both a^2 and b^2 are integer with $b^2 \neq 0$ by the zero product property. Hence x is a ratio of two integers with a nonzero denominator, and thus x is rational by the definition of rational. We therefore have x is irrational and x is rational which is a contradiction. Thus the supposition is false and the theorem is true. □

Problem 11

Prove that the product of any nonzero rational number and any irrational number is irrational.

Theorem: The product of any nonzero rational number and any irrational number is irrational.

Proof. Suppose not. That is suppose that there exists a nonzero rational number x and an irrational number y such that xy is rational. By definition of rational, $x = \frac{c}{d}$ with $d \neq 0$ and $xy = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Furthermore since $x \neq 0$, $c \neq 0$. By substitution,

$$\begin{aligned} \frac{a}{b} &= \frac{c}{d} \cdot y \\ y &= \frac{ad}{bc} \end{aligned}$$

Now ad and bc are both integers as products of integers are integers. Furthermore, by the zero product property $bc \neq 0$. Hence y is a ratio of two integers with a nonzero denominator, and thus y is rational. We therefore have that y is rational and y is irrational which is a contradiction. Thus the supposition is false and the theorem true. □

Problem 12

Prove that if a and b are rational numbers, $b \neq 0$, and r is any irrational number, then $a + br$ is irrational.

Theorem: If a and b are rational numbers, $b \neq 0$, and r is any irrational number, then $a + br$ is irrational.

Proof. Suppose not. That is suppose that there exists rational number a and b with $b \neq 0$, and an irrational number r, such that $a + br$ is rational. Then there exists integers c, d, e, and f such that $a = \frac{c}{d}$, and $b = \frac{e}{f}$ with $d \neq 0$, $f \neq 0$, and $e \neq 0$. Also $a + br = \frac{g}{h}$ for integers g and h with $h \neq 0$. By substitution,

$$\begin{aligned} a + br &= \frac{c}{d} + \frac{e}{f} \cdot r \\ \frac{g}{h} &= \frac{c}{d} + \frac{e}{f} \cdot r \\ r &= \frac{f(\frac{g}{h} - \frac{c}{d})}{e} \\ r &= \frac{fgd - fhc}{hde} \end{aligned}$$

Now $fgd - fhc$ and hde are both integers as products and differences of integers are integers. Furthermore, by the zero product property $hde \neq 0$. Hence r is a ratio of two integers with a nonzero denominator, and thus r is rational. We therefore have that r is rational and r is irrational which is a contradiction. Thus the supposition is false and theorem true. □

Problem 13

Prove that for any integer n, $n^2 - 2$ is not divisible by 4.

Theorem: For any integer n, $n^2 - 2$ is not divisible by 4.

Proof. Suppose not. That is suppose that there exists an integer n, such that $4 \mid (n^2 - 2)$. Then $n^2 - 2 = 4k$.

Case 1(n is even): If n is even then $n = 2p$ for some integer p. By substitution,

$$\begin{aligned} n^2 - 2 &= 4k \\ (2p)^2 - 2 &= 4k \\ 4p^2 - 2 &= 4k \\ 2 &= 4p^2 - 4k \\ 2 &= 4(p^2 - k) \end{aligned}$$

It follows then that $4 \mid 2$, but theorem 4.3.1 states that if a and b are positive integers and $a \mid b$ then $a \leq b$. This is a contradiction.

Case 2(n is odd): If n is odd then $n = 2p + 1$ for some integer p. By substitution,

$$\begin{aligned} n^2 - 2 &= 4k \\ (2p+1)^2 - 2 &= 4k \\ 4p^2 + 4p + 1 - 2 &= 4k \\ 4p^2 + 4p - 1 &= 4k \\ 1 &= 4(p^2 + p - k) \end{aligned}$$

It follows then that $4 \mid 1$, but theorem 4.3.1 states that if a and b are positive integers and $a \mid b$ then $a \leq b$. This is a contradiction.

Since a contradiction is reached in the case that n is even or odd and since all integers are either even or odd a contradiction will always be reached for every n. Thus the supposition is false and the theorem is true. □

Problem 14

Prove that for all prime numbers a, b, and c, $a^2 + b^2 \neq c^2$.

Theorem: Prove that for all prime numbers a, b, and c, $a^2 + b^2 \neq c^2$.

Proof. Suppose not. That is suppose that there exists prime numbers a, b, and c such that $a^2 + b^2 = c^2$.

$$\begin{aligned} a^2 + b^2 &= c^2 \\ a^2 &= c^2 - b^2 \\ a^2 &= (c-b)(c+b) \end{aligned}$$

Since a is a prime number, a is a positive integer. It follows that a^2 must also be a positive integer. Thus $c - b = 1$ or $c - b > 1$.

Case 1($c - b = 1$): If $c - b = 1$ then $c = b + 1$ but the only two prime numbers that fulfill this requirement are 2 and 3. Therefore $c = 2$ and $b = 3$.

$$a^2 = 1 \cdot (2 + 3) = 5$$

This is a contradiction as a is prime but $\sqrt{5}$ is not and integer and therefore not prime.

Case 2($c - b > 1$): If $c - b > 1$ then $c + b > 1$. Since a is prime a^2 can only be factored as $1 \cdot a^2$ or $a \cdot a$. Since both $c-b$ and $c+b$ are greater than 1 both of the factors of a^2 must be a.

$$c - b = a = c + b$$

Thus $c - b = c + b$ which means that $2b = 0$. By the zero product property $b = 0$. This is a contradiction as b is a prime and 0 is not prime.

Since a contradiction is always reached the supposition is false and the proposition is true. □

Problem 15

Prove that if a, b, and c are integers and $a^2+b^2 = c^2$, then at least one of a is odd.

Theorem: If a, b, and c are integers and $a^2 + b^2 = c^2$, then at least one of a and b is even.

Proof. Suppose not. That is suppose that there exists some integers a, b, and c such that $a^2 + b^2 = c^2$ and neither a nor b is even. By definition of odd $a = 2n + 1$ and $b = 2m + 1$ for some integers n and m. By substitution,

$$\begin{aligned} c^2 &= a^2 + b^2 \\ &= (2n+1)^2 + (2m+1)^2 \\ &= 4n^2 + 4n + 1 + 4m^2 + 4m + 1 \\ &= 4n^2 + 4n + 4m^2 + 4m + 2 \\ &= 4(n^2 + n + m^2 + m) + 2 \end{aligned}$$

It follows from closure under multiplication and addition that $n^2 + n + m^2 + m$ is an integer. Let that integer be t. Then $c^2 = 4t + 2 = 2(2t + 1)$. It follows that c^2 is an even integer. Since c^2 is an even integer c must also be an even integer. Thus $c = 2p$ for some integer p. It follows that

$$\begin{aligned} c^2 &= (2p)^2 \\ 2(2t+1) &= 4p^2 \\ 2t+1 &= 2p^2 \end{aligned}$$

This is a contradiction as an even integer cannot equal an odd integer. Thus the supposition is false and the theorem is true. □

Problem 16

Prove that for all odd integers a, b, and c, if z is a solution of $ax^2 + bx + c = 0$ then x is irrational.

Theorem: For all odd integers a, b, and c, if z is a solution of $ax^2 + bx + c = 0$ then z is irrational.

Proof. Suppose not. That is suppose that there exists odd integers a, b, and c, such that z is a solution of $ax^2 + bx + c = 0$ and z is rational. By definition of rational $z = \frac{p}{q}$ for some integers p and q such that $q \neq 0$. If z is a solution of $ax^2 + bx + c = 0$ then by substitution,

$$a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c = 0$$

Multiply both sides of the equation by q^2 to obtain

$$ap^2 + bpq + cq^2 = 0$$

Case 1(p and q are both odd): If p and q are both odd then we have

$$\begin{aligned} 0 &= ap^2 + bpq + cq^2 \\ &= \text{odd} \cdot \text{odd}^2 + \text{odd} \cdot \text{odd} \cdot \text{odd} + \text{odd} \cdot \text{odd}^2 \\ &= (\text{odd} + \text{odd}) + \text{odd} \\ &= \text{even} + \text{odd} \\ &= \text{odd} \end{aligned}$$

This is a contradiction as 0 is even.

Case 2(p is odd and q is even): If p is odd and q is even then we have

$$\begin{aligned} 0 &= ap^2 + bpq + cq^2 \\ &= \text{odd} \cdot \text{odd}^2 + \text{odd} \cdot \text{odd} \cdot \text{even} + \text{odd} \cdot \text{even}^2 \\ &= (\text{odd} + \text{even}) + \text{even} \\ &= \text{odd} + \text{even} \\ &= \text{odd} \end{aligned}$$

This is a contradiction as 0 is even.

Case 3(p even and q is odd): If p is even and q is odd then we have

$$\begin{aligned} 0 &= ap^2 + bpq + cq^2 \\ &= \text{odd} \cdot \text{even}^2 + \text{odd} \cdot \text{even} \cdot \text{odd} + \text{odd} \cdot \text{odd}^2 \\ &= (\text{even} + \text{even}) + \text{odd} \\ &= \text{even} + \text{odd} \\ &= \text{odd} \end{aligned}$$

This is a contradiction as 0 is even

We do not need to check the case that q and p are both even. This is because if p and q are both even then $p = 2m$ and $q = 2n$ for some integers m and

n. Thus $\frac{p}{q} = \frac{2m}{2n} = \frac{m}{n}$. If m and n are both even then repeat the process until m is not even, or n is not even, or m and n are both not even. Then this case will match either case 1, 2, or 3.

Since we reach a contradiction in all cases and since every rational number matches either case 1, 2, or 3 we can conclude that the supposition is false and the theorem is true. □

Problem 17

Prove that for all integers a, if $a \ mod \ 6 = 3$, then $a \ mod \ 3 \neq 2$.

Theorem: For all integers a, if $a \ mod \ 6 = 3$, then $a \ mod \ 3 \neq 2$.

Proof. Suppose not. That is suppose that there exists an integer a such that $a \ mod \ 6 = 3$ and $a \ mod \ 3 = 2$. It follows from the definition of *mod* that $a = 6q + 3$ for some integer q and $a = 3p + 2$ for some integer p.

$$\begin{aligned} 6q + 3 &= 3p + 2 \\ 3p - 6q &= 3 - 2 \\ 3(p - 2q) &= 1 \end{aligned}$$

It follows that $3 \mid 1$. This is a contradiction as theorem 4.3.1 states that if a and b are positive integers and $a \mid b$ then $a \leq b$ but $3 \not\leq 1$. Thus the supposition is false and the proposition is true. □

Problem 18

Theorem: For all integers n, if $5 \nmid n^2$ then $5 \nmid n$.

Proof. Suppose that n is any integer such that $5 \mid n$. We must show that $5 \mid n^2$. By definition of divisibility, $n = 5k$ for some integer k. By substitution, $n^2 = (5k)^2 = 5(5k^2)$. But $5k^2$ is an integer as it is a product of integers. Hence $n^2 = 5 \cdot \text{(an integer)}$, and so $5 \mid n^2$. □

Problem 19

Prove that if a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Theorem: If a product of two positive real numbers is greater than 100, then at least one of the numbers is greater than 10.

Proof. Suppose that x and y are any two positive real numbers such that $x \leq 10$ and $y \leq 10$.

$$xy \leq 10 \cdot 10 = 100$$

□

Problem 20

Prove that if a sum of two real numbers is less than 50, then at least one of the numbers is less than 25.

Theorem: If a sum of two real numbers is less than 50, then at least one of the numbers is less than 25.

Proof. Suppose that x and y are any two real numbers such that $x \geq 25$ and $y \geq 25$.

$$x + y \geq 25 + 25 = 50$$

$\square$

Problem 21

consider the statement "For all integers n, if n^2 is odd then n is odd."

(a) Write what you would suppose and what you would need to show to prove this statement by contradiction.

(b) Write what you would suppose and what you would need to show to prove this statement by contraposition.

Solution

(a) You would need to suppose that there exists an integer n such that n^2 is odd and n is even. You would need to show that this supposition leads to a contradiction.

(b) You would need to suppose that n is any integer such that n is not odd. You would need to show that n^2 is not odd.

Problem 22

Consider the statement "For all real numbers r, if r^2 is irrational then r is irrational."

(a) Write what you would suppose and what you would need to show to prove this statement by contradiction.

(b) Write what you would suppose and what you would need to show to prove this statement by contraposition.

Solution

(a) You would need to suppose that there exists a real number r such that r^2 is irrational and r is rational. You would need to show that this supposition leads to a contradiction.

(b) You would need to suppose that r is any real number such that r is not rational. You would need to show that r^2 is not rational.

Problem 23

Prove that the negative of any irrational number is irrational by contradiction and contraposition.

Theorem The negative of any irrational number is irrational.

Proof. Suppose not. That is suppose that there exists an irrational number x such that $-x$ is rational. By definition of rational, $-x = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Since $-1 \cdot -x = x$ it follows that

$$-1 \cdot \frac{a}{b} = -\frac{a}{b} = x$$

Now x is a ratio of two integers with a nonzero denominator, and thus x is rational. We therefore have that x is rational and x is irrational which is a contradiction. Thus the supposition is false and the theorem is true. □

Proof. Suppose that x is any rational number. By definition of rational $x = \frac{a}{b}$ for some integers a and b with $b \neq 0$. It follows that $-x = -\frac{a}{b}$. Now $-x$ is a rational number as it is a ratio of two integers with a nonnegative denominator. □

Problem 24

Prove by contradiction and contraposition that the reciprocal of any irrational number is irrational.

Theorem: The reciprocal of any irrational number is irrational.

Proof. Suppose not. That is suppose that there exists an irrational number x such that $\frac{1}{x}$ is rational. By the definition of rational $\frac{1}{x} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Solving for x gives

$$x = \frac{b}{a}$$

By the zero product property $a \neq 0$ as $b = ax$ and $b \neq 0$. Now x is a ratio of two integers with a nonzero denominator. We therefore have that x is rational and x is irrational which is a contradiction. Thus the supposition is false and the theorem is true. □

Proof. Suppose that $\frac{1}{x}$ is a rational number. Then $\frac{1}{x} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. It follows that $x = \frac{b}{a}$. By the zero product property $a \neq 0$ as $b = ax$ and $b \neq 0$. Now x is a ratio of two integers with a nonzero denominator. We therefore have that x is rational. $\square$

Problem 25

Prove by contradiction and contraposition that for all integers n, if n^2 is odd then n is odd.

Theorem: For all integers n, if n^2 is odd then n is odd.

Proof. Suppose not. That is suppose that there exists an integer n such that n^2 is odd and n is even. By definition of even $n = 2k$ for some integer k. Thus $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. We therefore have that n^2 is even and n^2 is odd which is a contradiction. Thus the supposition is false and the theorem is true. $\square$

Proof. Suppose that n is any integer such that n is even. By definition of even $n = 2k$ for some integer k. Thus $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$. It follows that n^2 is even. $\square$

Problem 26

Prove by contradiction and contraposition that for all integers a, b, and c, if $a \nmid bc$ then $a \nmid b$.

Theorem: For all integers a, b, and c, if $a \nmid bc$ then $a \nmid b$.

Proof. Suppose not. That is suppose that there exists some integers a, b, and c, such that $a \nmid bc$ and $a \mid b$. It follows from the definition of divide that $b = ak$ for some integer k. Multiply both sides by c to obtain $bc = akc = a(kc)$. It follows from closure under multiplication that kc is an integer. Let that integer be t. Then $bc = at$. It follows from the definition of divides that $a \mid bc$. We therefore have that $a \mid bc$ and $a \nmid bc$ which is a contradiction. Thus the supposition is false and the theorem is true. $\square$

Proof. Suppose that a, b, and c, are any integers such that $a \mid b$. It follows from the definition of divides that $b = ak$ for some integer k. Multiply both sides by c to obtain $bc = akc = at$ for some integer $t = kc$. It now follows from the definition of divides that $a \mid bc$. $\square$

Problem 27

Prove by contradiction and contraposition that for all integers m and n, if $m+n$ is even then m and n are both even or m and n are both odd.

Theorem: For all integers m and n, if $m+n$ is even then m and n are both even or m and n are both odd.

Proof. Suppose not. That is suppose that there exists integers m and n such that $m+n$ is even and m and n have opposite parity.

Case 1(m is even): If m is even then n must be odd. Thus $m = 2k$ and $n = 2j+1$ for some integers k and j.

$$m + n = 2k + 2j + 1 = 2(k + j) + 1$$

It follows that $m+n$ is odd. We therefore have that $m+n$ is even and $m+n$ is odd which is a contradiction.

Case 2(m is odd): If m is odd then n must be even. Thus $m = 2k+1$ and $n = 2j$ for some integers k and j.

$$m + n = 2k + 1 + 2j = 2(k + j) + 1$$

It follows that $m+n$ is odd. We therefore have that $m+n$ is even and $m+n$ is odd which is a contradiction.

Since we reach a contradiction in both of the only two possible cases we conclude that the supposition is false and the theorem is true. □

Proof. Suppose that m and n are any integers such that they have opposite parity.

Case 1(m is even): If m is even then n must be odd. Thus $m = 2k$ and $n = 2j+1$ for some integers k and j.

$$m + n = 2k + 2j + 1 = 2(k + j) + 1$$

It follows that $m+n$ is odd.

Case 2(m is odd): If m is odd then n must be even. Thus $m = 2k+1$ and $n = 2j$ for some integers k and j.

$$m + n = 2k + 1 + 2j = 2(k + j) + 1$$

It follows that $m+n$ is odd. □

Problem 28

Prove by contradiction and contraposition that for all integers m and n, if mn is even then m is even or n is even.

Theorem: For all integers m and n, if mn is even then m is even or n is even.

Proof. Suppose not. That is suppose that there exists integers m and n such that mn is even and m and n are both odd. By definition of odd $m = 2k + 1$ and $n = 2j + 1$ for some integers k and j. By substitution,

$$\begin{aligned} mn &= (2k+1)(2j+1) \\ &= 4kj + 2j + 2k + 1 \\ &= 2(2kj + j + k) + 1 \end{aligned}$$

It follows that mn is odd. We therefore have that mn is even and mn is odd which is a contradiction. Thus the supposition is false and the theorem is true. □

Proof. Suppose that m and n are any integers such that m and n are both odd. By definition of odd $m = 2k + 1$ and $n = 2j + 1$ for some integers k and j. By substitution,

$$\begin{aligned} mn &= (2k+1)(2j+1) \\ &= 4kj + 2j + 2k + 1 \\ &= 2(2kj + j + k) + 1 \end{aligned}$$

It follows that mn is odd. □

Problem 29

Prove by contradiction and contraposition that for all integers a, b, and c, if $a \mid b$ and $a \nmid c$, then $a \nmid (b + c)$.

Theorem: For all integers a, b, and c, if $a \mid b$ and $a \nmid c$, then $a \nmid (b + c)$.

Proof. Suppose not. That is suppose that there exists integers a, b, and c, such that $a \mid b$ and $a \nmid c$ and $a \mid (b + c)$. It follows from the definition of divides that $b + c = ak$ for some integer k and $b = aj$ for some integer j. By substitution,

$$\begin{aligned} b + c &= ak \\ aj + c &= ak \\ c &= a(k - j) \end{aligned}$$

It follows that $a \mid c$. We therefore have that $a \nmid c$ and $a \mid c$ which is a contradiction. Thus the supposition is false and the theorem is true. □

Let $P \equiv a \nmid (b + c)$, $Q \equiv a \mid b$, and $R \equiv a \nmid c$. The theorem that we need to prove is

$$\forall a, b, c \in \mathbb{Z},\ Q \wedge R \implies P$$

The contrapositive of this statement is

$$\forall a, b, c \in \mathbb{Z},\ \neg P \implies \neg Q \vee \neg R$$

It is easily verifiable by truth table that

$$\neg P \implies \neg Q \vee \neg R \equiv \neg P \wedge Q \implies \neg R$$

Therefore, we will prove a statement which is logically equivalent to the contrapositive of the theorem to be proved and in so doing prove the theorem. We will prove that

$$\forall a, b, c \in \mathbb{Z},\ \ \neg P \wedge Q \implies \neg R$$

Proof. Suppose that a, b, and c, are any integers such that $a \mid (b+c)$ and $a \mid b$. It follows that $b+c = ak$ and $b = aj$ for some integers k and j. By substitution,

$$\begin{aligned} b + c &= ak \\ aj + c &= ak \\ c &= a(k-j) \end{aligned}$$

It follows from the definition of divides that $a \mid c$. The theorem is proved. □

Problem 30

The following proof that every integer is rational is incorrect. Find the mistake.

proof: Suppose not. Suppose every integer is irrational. Then the integer 1 is irrational. But $1 = 1/1$, which is rational. This is a contradiction.

Solution

This proof by contradiction failed to correctly logically negate the statement to be proved. The correct logical negation is "there exists an integer x such that x is irrational", not that every integer is irrational. Therefore the discovery of a specific case of an integer that is rational does not constitute a contradiction and the proof fails.

Problem 31

(a) Prove by contraposition: For all positive integers n, r, and s, if $rs \leq n$, then $r \leq \sqrt{n}$ or $s \leq \sqrt{n}$.

(b) Prove: For all integers $n > 1$, if n is not prime, then there exists a prime number p, such that $p \leq \sqrt{n}$ and n is divisible by p.

(c) State the contrapositive of the result of part (b). The results of exercise 31 provide a way to test whether an integer is prime.

Solution

(a) *Theorem*: For all positive integers n, r, and s, if $rs \leq n$, then $r \leq \sqrt{n}$ or $s \leq \sqrt{n}$.

Proof. Suppose that n, r, and s, are any positive integers such that $r > \sqrt{n}$ and $s > \sqrt{n}$.

$$\begin{aligned} r &> \sqrt{n} \\ rs &> s\sqrt{n}, \qquad \text{but since } s > \sqrt{n} \\ rs &> \sqrt{n}\sqrt{n} \\ rs &> n \end{aligned}$$

□

(b) *Theorem*: For all integers $n > 1$, if n is not prime, then there exists a prime number p, such that $p \leq \sqrt{n}$ and n is divisible by p.

Proof. Let n be any integer such that $n > 1$ and n is not prime. It follows from theorem 4.3.4 which states that every integer $n > 1$ is divisible by a prime number that $p \mid n$ for some prime number p. It follows from the definition of divisibility that $n = pk$ for some integer k.

$$\begin{aligned} &n = pk \\ &n \geq pk \\ &p \leq \sqrt{n} \ \text{ or } \ k \leq \sqrt{n}, \quad \text{by part (a)} \end{aligned}$$

If $p \leq \sqrt{n}$ then this particular n is consistent with the theorem. If $k \leq \sqrt{n}$ then k is either prime or composite. If k is prime then this particular n is consistent with the theorem. Since n is not prime and $n = pk$ we can conclude that $k > 1$ because if $k = 1$ then $n = p$ which is prime. Therefore if k is composite use theorem 4.3.4 which guarantees a prime number m such that $m \mid k$. It follows from the transitivity of divisibility that since $m \mid k$ and $k \mid n$, $m \mid n$. It follows from theorem 4.3.1 that since $m \mid k$ $m \leq k$. It follows that $m \leq \sqrt{n}$ as $m \leq k \leq \sqrt{n}$. □

(c) For all integers $n > 1$, if there does not exist a prime number p such that $p \leq \sqrt{n}$ and $p \mid n$, then n is prime.

Problem 32 and solution

Use the test for primality to determine whether the following numbers are prime or not.

(a) $\sqrt{667} \approx 25.83 > 23$. $23 \mid 667$ so 667 is not prime.

(b) $\sqrt{557} \approx 23.60$ but 557 is not divisible by 23, 19, 17, 13, 11, 7, 5, 3, or 2 and so 557 is prime.

(c) $\sqrt{527} \approx 22.96 > 17$. $17 \mid 527$ so 527 is not prime.

(d) $\sqrt{613} \approx 24.76$ but 613 is not divisible by 23, 19, 17, 13, 11, 7, 5, 3, or 2 and so 613 is prime.

Problem 33

The sieve of Eratosthenes, named after its inventor, the Greek scholar Eratosthenes, provides a way to find all prime numbers less than or equal to some fixed number n. To construct it, write out all the integers from 2 to n. Cross out all multiples of 2 except 2 itself, then all multiples of 3 except 3 itself, then all multiples of 5 except 5 itself, and so forth. Continue crossing out the multiples of each successive prime number up to $\sqrt{n}$. The numbers that are not crossed out are all the prime numbers for 2 to n. Use the sieve of Eratosthenes to find all prime numbers less than 100.

Solution

$2, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11, \cancel{12}, 13, \cancel{14}, \cancel{15}, \cancel{16}, 17, \cancel{18}, 19, \cancel{20}, \cancel{21}, \cancel{22}, 23, \cancel{24}, \cancel{25}, \cancel{26}, \cancel{27}, \cancel{28}, 29, \cancel{30}, 31, \cancel{32}, \cancel{33}, \cancel{34}, \cancel{35}, \cancel{36}, 37, \cancel{39}, \cancel{39}, \cancel{40}, 41, \cancel{42}, 43, \cancel{44}, \cancel{45}, \cancel{46}, 47, \cancel{48}, \cancel{49}, \cancel{50}, \cancel{51}, \cancel{52}, 53, \cancel{54}, \cancel{55}, \cancel{56}, \cancel{57}, \cancel{58}, 59, \cancel{60}, 61, \cancel{62}, \cancel{63}, \cancel{64}, \cancel{65}, \cancel{66}, 67, \cancel{68}, \cancel{69}, \cancel{70}, 71, \cancel{72}, 73, \cancel{74}, \cancel{75}, \cancel{76}, \cancel{77}, \cancel{78}, 79, \cancel{80}, \cancel{81}, \cancel{82}, 83\ \cancel{84}, \cancel{85}, \cancel{86}, \cancel{87}, \cancel{88}, 89, \cancel{90}, \cancel{91}, \cancel{92}, \cancel{93}, \cancel{94}, \cancel{95}, \cancel{96}, 97, \cancel{98}, \cancel{99}.$

Therefore the prime numbers less than 100 are

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Problem 34 and solution

Use the test for primality and the results of exercise 33 to determine whether the following numbers are prime.

(a) $\sqrt{9,269} \approx 96.3$. Checking all the prime factors less than 96.3 found in exercise 33 shows that 9,269 is not prime as $13 \mid 9,269$.

(b) $\sqrt{9,103} \approx 95.4$ but none of the prime numbers less than 95.4 found in exercise 33 divide 9,103 and so 9,103 is prime.

(c) $\sqrt{8,623} \approx 92.9$ but none of the prime numbers less than 92.9 found in exercise 33 divide 8,623 and so 8,623 is prime.

(d) $\sqrt{7,917} \approx 88.97$. Checking all the prime factors less than 88.97 found in exercise 33 shows that 7,917 is not prime as $3 \mid 7,917$.

Problem 35

Use proof by contradiction to show that every integer greater than 11 is a sum of two composite numbers.

Theorem: Every integer greater than 11 is a sum of two composite numbers.

Proof. Suppose not. That is suppose there exists an integer n such that $n > 11$ and n is not a sum of two composite numbers.

Case 1 (n is even): If n is even then $n = 2k$ for some integer k.

$$\begin{aligned} n &> 11 \\ n &\geq 12 \\ 2k &\geq 12 \\ k &\geq 6 \end{aligned}$$

Now $n = (n-4) + 4 = (2k-4) + 4 = 2(k-2) + 4$. Since $k \geq 6$, $2(k-2) \geq 8$. It follows that $1 < 2 < 2(k-2)$. Also, since $k-2$ is an integer $2 \mid (2(k-2))$. It now follows from definition of composite that $2(k-2) = n-4$ is composite. Finally $1 < 2 < 4$ and $2 \mid 4$ and so 4 is composite. Since $n = (n-4) + 4$ and both $n-4$ and 4 are composite, it follows that n is a sum of two composite numbers. We therefore have that n is not a sum of two composite numbers and n is a sum of two composite numbers which is a contradiction.

Case 2 (n is odd): If n is odd then $n = 2k+1$ for some integer k.

$$\begin{aligned} n &> 11 \\ n &\geq 12 \\ 2k+1 &\geq 12 \\ k &\geq 6 \end{aligned}$$

Now $n = (n-9) + 9 = (2k+8) + 9 = 2(k+4) + 9$. Since $k \geq 6$, $1 < 2 < 2k+8$. Furthermore, $2 \mid (2(k+4))$. Thus $2k+8$ is a composite number. Finally $1 < 3 < 9$ and $3 \mid 9$. Thus 9 is a composite number. Since $n = (2k+8) + 9$ and both $2k+8$ and 9 are composite, it follows that n is a sum of two composite numbers. We therefore have that n is not a sum of two composite numbers and n is a sum of two composite numbers which is a contradiction.

Since we reach a contradiction in the case that n is even and in the case that n is odd and since all integers are either even or odd we can conclude that the supposition is false and the theorem is true. $\square$