Section 4.7

Sterling Jeppson

October 26, 2020

Problem 1

A calculator display shows that $\sqrt{2} = 1.414213562$, and $1.414213562 = \frac{1.414213562}{1000000000}$. This suggests that $\sqrt{2}$ is a rational number, which contradicts Theorem 4.7.1. Explain the discrepancy.

Solution

The number displayed by the calculator is an approximation of $\sqrt{2}$. Any decimal number which has a finite number of digits is rational. This means that in order for a number to be irrational it needs to have an infinite number of digits. This is not possible to display in a finite amount of space, for example a calculator screen, and so the calculator must use an approximation.

Problem 2

Example 4.2.1(h) illustrates a technique for showing that any repeating decimal number is rational. A calculator display shows that the result of a certain calculation as 40.72727272727. Can you be sure that the result of the calculation is a rational number? Explain.

Solution

No. The correct result of the calculation may not be a rational number as $40.72727272727 + \frac{\sqrt{2}}{100^{100}}$ will show the same result and yet it is not a rational number.

Problem 3

Determine if $6 - 7\sqrt{2}$ is irrational.

Theorem: $6 - 7\sqrt{2}$ is irrational.

Proof. Suppose not. That is suppose that $6-7\sqrt{2}$ is rational. Then $6-7\sqrt{2} = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

$$\begin{aligned} 6 - 7\sqrt{2} &= \frac{a}{b} \\ 7\sqrt{2} &= \frac{a}{b} + 6 \\ 7\sqrt{2} &= \frac{6b + a}{b} \\ \sqrt{2} &= \frac{6b + a}{7b} \end{aligned}$$

It follows from closure under multiplication and addition that $6b + a$ and $7b$ are integers. Furthermore, by the zero product property $7b \neq 0$. Now $\sqrt{2}$ is a ratio of two integers with a nonzero denominator and so $\sqrt{2}$ is rational. But this is a contradiction as $\sqrt{2}$ is irrational. Hence the supposition is false and the theorem is true. □

Problem 4

Determine if $3\sqrt{2} - 7$ is irrational.

Theorem: $3\sqrt{2} - 7$ is irrational.

Proof. Suppose not. That is suppose that $3\sqrt{2}-7$ is rational. Then $3\sqrt{2}-7 = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

$$\begin{aligned} 3\sqrt{2} - 7 &= \frac{a}{b} \\ 3\sqrt{2} &= \frac{a}{b} + 7 \\ \sqrt{2} &= \frac{a + 7b}{3b} \end{aligned}$$

it now follows from closure under multiplication and addition that $a + 7b$ and $3b$ are integers. Furthermore, by the zero product property $3b \neq 0$. Now $\sqrt{2}$ is a ratio of two integers with a nonzero denominator and so $\sqrt{2}$ is rational. But this is a contradiction as $\sqrt{2}$ is irrational. Hence the supposition is false and the theorem is true. □

Problem 5

Determine if $\sqrt{4}$ is irrational.

Contradiction: $\sqrt{4} = 2 = \frac{2}{1}$. It follows from definition that $\sqrt{4}$ is rational.

Problem 6

Determine if $\sqrt{2}/6$ is rational.

Contradiction: Suppose that $\sqrt{2}/6$ is rational. Then $\sqrt{2}/6 = \frac{a}{b}$ for some integers a and b with $b \neq 0$. But then $\sqrt{2} = \frac{6a}{b}$ which is a ratio of two integers with a nonzero denominator. However $\sqrt{2}$ is irrational and so this is a contradiction. Thus $\sqrt{2}/6$ is not rational.

Problem 7

Determine if the sum of any two irrational numbers is irrational.

Counterexample: Let $x = \sqrt{2}$ and let $y = -\sqrt{2}$. Then x and y are both irrational but $\sqrt{x} + \sqrt{y} = \sqrt{2} + (-\sqrt{2}) = 0$ which is rational.

Problem 8

Determine if the difference of any two irrational numbers is irrational.

Counterexample: Let $x = \sqrt{2}$ and let $y = \sqrt{2}$. Then x and y are irrational but $x - y = \sqrt{2} - \sqrt{2} = 0$ which is rational.

Problem 9

Determine if the positive square root of a positive irrational number is irrational.

Theorem: $\forall x \in \mathbb{R}^+,\ x \in \mathbb{Q}' \implies \sqrt{x} \in \mathbb{Q}'$.

Proof. Suppose that $\sqrt{x} \in \mathbb{Q}^+$. Then $\sqrt{x} = \frac{a}{b}$ for some integers a and b with $b \neq 0$ and $\frac{a}{b} > 0$.

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

It follows from closure under multiplication that a^2 and b^2 are integers. Furthermore, it follows from the zero product property that $b^2 \neq 0$. Now x is a ratio of two integers with a nonzero denominator and so $x \in \mathbb{Q}$. □

Problem 10

If r is any rational number and s is any irrational number, is r/s irrational?

Counterexample: Let $r = 0$ and let s be any irrational number. Then $r/s = 0/s = 0$ which is rational. However if $r \neq 0$ then

Theorem: $\forall r, s \in \mathbb{R}$, if r is any nonzero rational number and s is any irrational number then r/s is irrational.

Proof. Suppose not. That is suppose that r is any nonzero rational number and s is any irrational number such that r/s is rational. It follows from definition of rational that $\frac{r}{s} = \frac{a}{b}$ and $r = \frac{c}{d}$ for some integers a, b, c, and d, with $b \neq 0$ and $d \neq 0$. Also, Since $r \neq 0$, $a \neq 0$ and $c \neq 0$.

$$\frac{r}{s} = \frac{a}{b}$$
$$s = \frac{rb}{a}$$
$$s = \frac{bc}{ad}$$

It now follows that s is a ratio of two integers with a nonzero denominator and so s is rational. This is a contradiction and so the supposition is false and the theorem true. □

Problem 11

Determine if the sum of any two positive irrational numbers is irrational.

Counterexample: Let $x = \sqrt{2}$ and let $y = 3 - \sqrt{2}$. Then x and y are both positive irrational numbers but

$$x + y = \sqrt{2} + (3 - \sqrt{2}) = 3$$

which is a rational number.

Problem 12

Determine if the product of any two irrational numbers is irrational.

Counterexample: Let $x = y = \sqrt{2}$. Then x and y are both irrational but

$$xy = \sqrt{2} \cdot \sqrt{2} = 2$$

which is a rational number.

Problem 13

If an integer greater than 1 is a perfect square, it its cube root rational?

Counterexample: Let $x = 64$. Then x is an integer and x is a perfect square as $x = 8 \cdot 8$. But $\sqrt[3]{64} = 4$ which is rational.

Problem 14

Consider the following sentence: If x is rational then $\sqrt{x}$ is irrational. Is this sentence always true, sometimes true and sometimes false, or always false? Justify your answer.

Solution

Sometimes true and sometimes false. For example, let $x = 4$. Then x is rational and $\sqrt{x} = \sqrt{4} = 2$ is rational. However if $x = 2$ then x is rational but $\sqrt{x}$ is irrational.

Problem 15

(a) Prove that for all integers a, if a^3 is even then a is even.

(b) Prove that $\sqrt[3]{2}$ is irrational.

Solution

(a) *Theorem*: For all integers a, if a^3 is even then a is even.

Proof. Suppose not. That is suppose that there exists an integer a such that a^3 is even but a is odd. By definition of add $a = 2k + 1$ for some integer k.

$$\begin{aligned} a^3 &= (2k+1)^3 \\ &= 8k^3 + 12k^2 + 6k + 1 \\ &= 2(2k^3 + 6k^2 + 3k) + 1 \end{aligned}$$

It follows from closure under multiplication and addition that $2k^3+6k^2+3k$ is an integer. Let that integer be t. Then $a^3 = 2t + 1$. It follows that a^3 is odd which is a contradiction. Hence the supposition is false and the theorem is true. □

(b) *Theorem*: $\sqrt[3]{2}$ is irrational.

Proof. Suppose not. That is suppose that $\sqrt[3]{2}$ is rational. Then there exists integers a and b with no common factors so that $\sqrt[3]{2} = \frac{a}{b}$

$$\begin{aligned} \sqrt[3]{2} &= \frac{a}{b} \\ 2 &= \left(\frac{a}{b}\right)^3 = \frac{a^3}{b^3} \\ a^3 &= 2 \cdot b^3 \end{aligned}$$

It follows that a^3 is even and so by part(a), a is even and so $a = 2k$ for some integer k. By substitution

$$a^3 = (2k)^3 = 8k^3 = 2 \cdot b^3$$

Dividing both sides by 2 gives

$$b^3 = 4k^3 = 2 \cdot 2k^3$$

Consequently, b^3 is even, and so b is even by part(a). But we also know that a is even. Hence a and b have a common factor of 2. But this contradicts the supposition that a and b have no common factors. Hence the supposition is false and the theorem is true. □

Problem 16

(a) Use proof by contradiction to show that for any integer n, it is impossible for n to equal both $3q_1 + r_1$ and $3q_2 + r_2$, where q_1, q_2, r_1, and r_2, are integers, $0 \leq r_1 < 3$, $0 \leq r_2 < 3$, and $r_1 \neq r_2$.

(b) Use proof by contradiction, the quotient-remainder theorem, division into cases, and the result of part (a) to prove that for all integer n, if n^2 is divisible by 3 then n is divisible by 3.

(c) Prove that $\sqrt{3}$ is irrational.

Problem 16

(a) *Theorem*: For any integer n, it is impossible for n to equal both $3q_1 + r_1$ and $3q_2 + r_2$, where q_1, q_2, r_1, and r_2, are integers, $0 \leq r_1 < 3$, $0 \leq r_2 < 3$, and $r_1 \neq r_2$.

Proof. Suppose not. That is suppose that there exists an integer n such that $n = 3q_1 + r_1 = 3q_2 + r_2$ where q_1, q_2, r_1, and r_2, are integers, $0 \leq r_1 < 3$, $0 \leq r_2 < 3$, and $r_1 \neq r_2$. Without loss of generality assume that $r_1 < r_2$.

$$\begin{aligned} n = 3q_1 + r_1 &= 3q_2 + r_2 \\ 3q_1 - 3q_2 &= r_2 - r_1 \\ 3(q_1 - q_2) &= r_2 - r_1 \end{aligned}$$

Since $r_2 \neq r_1$ and $r_2 > r_1$, $r_2 - r_1$ can only be 1 if $r_2 = 2$ and $r_1 = 1$ or if $r_2 = 1$ and $r_1 = 0$ or 2 if $r_2 = 2$ and $r_1 = 0$. If $r_2 - r_1 = 1$ then we have

$$3(q_1 - q_2) = 1$$

This implies that $3 \mid 1$ and hence, by theorem 4.3.1, $3 \leq 1$ which is a contradiction. Alternatively if $r_2 - r_1 = 2$ then we have

$$3(q_1 - q_2) = 2$$

This implies that $3 \mid 2$ and hence, by theorem 4.3.1, $3 \leq 2$ which is a contradiction. Since a contradiction is reached in every possible case we can conclude that the supposition is false and the theorem is true. $\square$

(b) *Theorem*: For all integers n, if n^2 is divisible by 3 then n is divisible by 3.

Proof. Suppose not. That is suppose that there exists an integer n such that n^2 is divisible by 3 and $3 \nmid n$. It follows from the definition of divisible that $n^2 = 3q$ for some integer q. It follows from the quotient remainder theorem and the supposition that $3 \nmid n$ that $n = 3k+1$ or $n = 3k+2$. For some integer k.

Case 1 $(n = 3k + 1)$:

$$n^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$$

Let $s = 3k^2+2k$. Then s is an integer as it is a sum of products of integers. It follows that there exists an integer $t = n^2$ such that $t = 3q+0 = 3s+1$ which contradicts the results of part (a).

Case 2 $(n = 3k + 2)$:

$$n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$$

Let $s = 3k^2 + 4k + 1$. Then s is an integer as integers are closed under multiplication and addition. It follows that there exists an integer $t = n^2$ such that $t = 3q + 0 = 3s + 1$ which contradicts the results of part (a).

Since a contradiction is reached in all possible cases we can conclude that the supposition is false and the theorem is true. $\square$

(c) *Theorem*: $\sqrt{3}$ is irrational.

Proof. Suppose not. That is suppose that $\sqrt{3}$ is rational. Then there exist integers a and b with no common factors such that $\sqrt{3} = \frac{a}{b}$ and $b \neq 0$.

$$\begin{aligned} \sqrt{3} &= \frac{a}{b} \\ (\sqrt{3})^2 &= \left(\frac{a}{b}\right)^2 \\ 3 &= \frac{a^2}{b^2} \\ a^2 &= 3 \cdot b^2 \end{aligned}$$

It follows that $3 \mid a^2$ and so by part (b) $3 \mid a$. It follows then from the definition of divisibility that $a = 3k$ for some integer k.

$$a^2 = (3k)^2 = 9k^2 = 3b^2$$

Dividing both sides of the equation by 3 gives $3k^2 = b^2$. It now follows from the definition of divisibility that $3 \mid b^2$ and so by part (b) $3 \mid b$. Consequently a and b are both divisible by 3 which contradicts the assumption that a and b have no common factor. Thus the supposition is false and the theorem is true. □

Problem 17

Give an example to show that if d is not prime and n^2 is divisible by d, then n need not be divisible by d.

Solution

Let $d = 4$ and let $n = 2$. Then d is not prime and $d \mid n^2$ but $d \nmid n$.

Problem 18

The quotient-remainder theorem says not only that there exist quotients and remainders but also that the quotient and remainder of a division are unique. Prove the uniqueness. That is, prove that if a and d are integers with $d > 0$ and if q_1, r_1, q_2, and r_2 are integers such that

$$a = dq_1 + r_1 \quad \text{where } 0 \le r_1 < d \quad \text{and}$$

$$a = dq_2 + r_2 \quad \text{where } 0 \le r_2 < d, \quad \text{then}$$

$$q_1 = q_2 \quad \text{and} \quad r_1 = r_2$$

Proof. It follows from the transitive property of equality that

$$\begin{aligned} a = dq_1 + r_1 &= dq_2 + r_2 \\ r_1 - r_2 &= dq_2 - dq_1 \\ r_1 - r_2 &= d(q_2 - q_1) \quad (1) \end{aligned}$$

Now consider the minimum and maximum values of $r_1 - r_2$. The maximum value occurs when $r_1 = d - 1$ and $r_2 = 0$ and the minimum value occurs when $r_1 = 0$ and $r_2 = d - 1$. It follows that the maximum value is $d - 1$ and the minimum value is $-d + 1$. Hence

$$\begin{aligned} -d < r_1 - r_2 &< d \\ -d < d(q_2 - q_1) &< d \\ -1 < q_2 - q_1 &< 1 \end{aligned}$$

Since q_1 and q_2 are integers and $-1 < q_2 - q_1 < 1$ it follows that $q_2 - q_1 = 0$. Hence $q_1 = q_2$. Substituting 0 for $q_2 - q_1$ in (1) gives

$$\begin{aligned} r_1 - r_2 &= d \cdot 0 \\ r_1 - r_2 &= 0 \end{aligned}$$

Hence $r_1 = r_2$ and the proof is complete. □

Problem 19

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

Solution

Lemma 1: $\forall n \in \mathbb{Z},\ 5 \mid n^2 \implies 5 \mid n$.

Proof. Suppose not. That is suppose that there exists an integer n such that $5 \mid n^2$ but $5 \nmid n$. It follows from the definition of divides that $n^2 = 5q$ for some integer q. It follows from the quotient-remainder theorem and that fact that $5 \nmid n$ that

$$n = 5k + 1 \text{ or } n = 5k + 2 \text{ or } n = 5k + 3 \text{ or } n = 5k + 4$$

Case 1$(n = 5k + 1)$:

$$n^2 = 25k^2 + 10k + 1 = 5(5k^2 + 2k) + 1$$

Let $s = 5k^2 + 2k$. Then s is an integer as integers are closed under multiplication and addition. It follows that there exists an integer $t = n^2$ such that $t = 5q = 5s + 1$ which contradicts the uniqueness of r for a given d under the quotient remainder theorem.

Case 2$(n = 5k + 2)$:

$$n^2 = 25k^2 + 20k + 4 = 5(5k^2 + 4k) + 4$$

Let $s = 5k^2 + 4k$. Then s is an integer as integers are closed under multiplication and addition. It follows that there exists an integer $t = n^2$ such that $t = 5q = 5s + 4$ which contradicts the uniqueness of r for a given d under the quotient remainder theorem.

Case 3$(n = 5k + 3)$:

$$n^2 = 25k^2 + 30k + 9 = 5(5k^2 + 6k + 1) + 4$$

Let $s = 5k^2 + 6k + 1$. Then s is an integer as integers are closed under multiplication and addition. It follows that there exists an integer $t = n^2$ such that $t = 5q = 5s + 4$ which contradicts the uniqueness of r for a given d under the quotient remainder theorem.

Case 4$(n = 5k + 4)$:

$$n^2 = 25k^2 + 40k + 16 = 5(5k^2 + 8k + 3) + 1$$

Let $s = 5k^2 + 8k + 3$. Then s is an integer as integers are closed under multiplication and addition. It follows that there exists an integer $t = n^2$ such that $t = 5q = 5s + 1$ which contradicts the uniqueness of r for a given d under the

quotient remainder theorem.

Since a contradiction is reached in all possible cases we can conclude that the supposition is false and the theorem is true. □

Theorem: $\sqrt{5}$ is irrational.

Proof. Suppose not. That is suppose that $\sqrt{5}$ is rational. Then $\sqrt{5} = \frac{a}{b}$ for some integers a and b, such that a and b have no common factors and $b \neq 0$.

$$\begin{aligned} \left(\sqrt{5}\right)^2 &= \left(\frac{a}{b}\right)^2 \\ 5 &= \frac{a^2}{b^2} \\ a^2 &= 5 \cdot b^2 \end{aligned}$$

It follows from the definition of divisibility that $5 \mid a^2$. Thus by lemma 1, $5 \mid a$.

$$\begin{aligned} a^2 &= (5k)^2 \\ a^2 &= 25k^2 = 5 \cdot b^2 \\ b^2 &= 5k^2 \end{aligned}$$

It now follows that $5 \mid b^2$ and so by lemma 1, $5 \mid b$. But now a and b are both divisible by 5 and so they share a common factor of 5 which is a contradiction. Thus the supposition is false and the theorem is true. □

Problem 20

Prove that for any integer a, $9 \nmid (a^2 - 3)$.

Theorem: For all integers a, $9 \nmid (a^2 - 3)$

Proof. Suppose not. That is suppose that there exists an integer a such that $9 \mid (a^2 - 3)$. It follows from the definition of divisibility that $a^2 - 3 = 9k$ for some integer k. Solving for a^2 gives $a^2 = 9k + 3 = 3(3k + 1)$. It follows that $3 \mid a^2$ and so by exercise 16 (b), $3 \mid a$. If $3 \mid a$ then $a = 3c$ for some integer c. Then $a^2 = 9c^2 + 0 = 9k + 3$ which contradicts the uniqueness of r for a given d under the quotient remainder theorem. Hence the supposition is false and the theorem is true. □

Problem 21

An alternative proof of the irrationality of $\sqrt{2}$ counts the number of 2's on the two sides of the equation $2n^2 = m^2$ and uses the unique factorization of integers theorem to deduce a contradiction. Write a proof that uses this approach.

Solution

Theorem: $\sqrt{2}$ is irrational.

Proof. Suppose not. That is suppose that $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some integers a and b with $b \neq 0$. Then

$$\left(\sqrt{2}\right)^2 = \left(\frac{a}{b}\right)^2$$
$$2 = \frac{a^2}{b^2}$$
$$a^2 = 2 \cdot b^2$$

The question now is whether $a^2 = 2b^2$ is a contradiction. Let n be the number of 2's in the prime factorization of a. It follows that the number of 2's in the prime factorization of a^2 will be $2n$. Thus a^2 will have an even number of 2's in its prime factorization. Let the number of 2's in the prime factorization of b be m. The same reasoning applies to b^2 so that the number of 2's in the prime factorization of b^2 is $2m$ which is even. Now $2 \cdot b^2$ will have $2m + 1$ 2's in its prime factorization which is an odd number of 2's. If two integers are equal to each other then they have the same prime factorization but theorem 4.6.2 states that no integer can be both even and odd and so $2n \neq 2m+1$. Since a^2 and $2b^2$ cannot have the same number of 2's in their prime factorization they cannot be equal. Hence $a^2 = 2b^2$ is a contradiction and so the supposition is false and the theorem is true. □

Problem 22

Use the proof technique demonstrated in exercise 21 to prove that if n is any positive integer that is not a perfect square, then $\sqrt{n}$ is irrational.

Theorem: If n is any positive integer that is not a perfect square, then $\sqrt{n}$ is irrational.

Proof. Suppose not. That is suppose that there exists an integer n such that n is not a perfect square and $\sqrt{n}$ is rational. By the definition of rational there exist integers a and b with $b \neq 0$ such that $\sqrt{n} = \frac{a}{b}$

$$\sqrt{n} = \frac{a}{b}$$
$$\left(\sqrt{n}\right) = \left(\frac{a}{b}\right)^2$$
$$n = \frac{a^2}{b^2}$$
$$a^2 = n \cdot b^2$$

It follows from similar reasoning to problem 21 that all the prime factors in a^2 and b^2 occur an even number of times. However, since n is not a perfect square

there must exist at least one prime factor of n that occurs an odd number of times. Thus $n \cdot b^2$ will contain an odd number of occurrences of at least one prime factor. It follows from theorem 4.6.2 which states that no integer can be both even and odd the a^2 and $n \cdot b^2$ do not have the same prime factorization and thus $a^2 = n \cdot b^2$ is a contradiction. It follows that the supposition is false and the theorem is true. □

Problem 23

Prove that $\sqrt{2} + \sqrt{3}$ is irrational.

Theorem: $\sqrt{2} + \sqrt{3}$ is irrational.

Proof. Suppose not. That is suppose that $\sqrt{2}+\sqrt{3}$ is rational. Then $\sqrt{2}+\sqrt{3} = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

$$\begin{aligned} \sqrt{2} + \sqrt{3} &= \frac{a}{b} \\ (\sqrt{2} + \sqrt{3})^2 &= \left(\frac{a}{b}\right)^2 \\ 2 + 2\sqrt{2}\sqrt{3} + 3 &= \frac{a^2}{b^2} \\ \sqrt{6} &= \frac{a^2 - 5b}{2b^2} \end{aligned}$$

It follows that $\sqrt{6}$ is a ratio of integers with a nonzero denominator and so $\sqrt{6}$ is rational. However, by the results of problem 22, since 6 is not a perfect square $\sqrt{6}$ is irrational. Now $\sqrt{6}$ is rational and irrational which is a contradiction. Hence the supposition is false and the theorem true. □

Problem 24

Prove that $\log_5 2$ is irrational.

Theorem: $\log_5 2$ is irrational.

Proof. Suppose not. That is suppose that $\log_5 2$ is rational. Then $\log_5 2 = \frac{a}{b}$ for some integers a and b with $b \neq 0$.

$$\begin{aligned} \log_5 2 &= \frac{a}{b} \\ 5^{ab^{-1}} &= 2 \\ (5^a)^{b^{-1}} &= 2 \\ 5^a &= 2^b \end{aligned}$$

This is a contradiction under the unique prime factorization of the integers theorem. Thus the supposition is false and the theorem is true. □

Problem 25

Let $N = 2 \cdot 3 \cdot 5 \cdot 7 + 1$. What remainder is obtained when N is divided by 2? 3? 5? 7? Is N prime? Justify your answer.

Solution

$N \ mod \ 2 = 3 \cdot 5 \cdot 7 + \frac{1}{2}$

$N \ mod \ 3 = 2 \cdot 5 \cdot 7 + \frac{1}{3}$

$N \ mod \ 5 = 2 \cdot 3 \cdot 7 + \frac{1}{5}$

$N \ mod \ 7 = 2 \cdot 3 \cdot 5 + \frac{1}{7}$

It follows from problem 4.6.31 part (c) that in order to check the primality of an integer n, it suffices to show that n is not divisible by any prime number $p \leq \sqrt{n}$. Since $\sqrt{N} \approx 14.53$ and since N is an integer, we only need to check if N is divisible by any primes less than or equal to 14. The primes less than or equal to 14 are 2, 3, 5, 7, 11, and 13. We already know that 2, 3, 5, and 7 do not divide N. We need to check 11 and 13. Now $11 \nmid N$ and $13 \nmid N$ as $N \ mod \ 11 = 2$ and $N \ mod \ 13 = 3$. Hence N is prime.

Problem 26

Suppose that a is an integer and p is a prime number such that $p \mid a$ and $p \mid (a + 3)$. What can you deduce about p? Why?

Solution

If $p \mid a$ then $a = pk$ for some integer k. If $p \mid (a + 3)$ then $a + 3 = pj$ for some integer j. It follows that $a = pj - 3$ By the transitive property of equality

$$\begin{aligned} a = pk &= pj - 3 \\ 3 &= pj - pk \\ 3 &= p(j - k) \end{aligned}$$

It follows from the definition of divisibility that $p \mid 3$. However by theorem 4.3.1, $p \leq 3$. The only two prime numbers that qualify are 2 and 3 but $2 \nmid 3$. Hence $p = 3$.

Problem 27

Let $p_1, p_2, p_3, ...$ be a list of all prime numbers in ascending order. Here is a table of the first six:

p_1	p_2	p_3	p_4	p_5	p_6
2	3	5	7	11	13

(a) For each $i = 1, 2, 3, 4, 5, 6$, let $N_i = p_1 p_2 ... p_i + 1$. Calculate N_1, N_2, N_3, N_4, N_5, and N_6.

(b) For each $i = 1, 2, 3, 4, 5, 6$, find the smallest prime numbers q_i such that q_i divides N_i.

Solution

(a) $N_1 = 2 + 1 = 3$
$N_2 = 2 \cdot 3 + 1 = 7$
$N_3 = 2 \cdot 3 \cdot 5 + 1 = 31$
$N_4 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$
$N_5 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2,311$
$N_6 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30,031$

(b) To solve this problem simply apply the primality test from 4.6.31

N_1: 3 is the smallest prime q_1 such that $q_1 \mid N_1$
N_2: 7 is the smallest prime q_2 such that $q_2 \mid N_2$
N_3: 31 is the smallest prime q_3 such that $q_3 \mid N_3$
N_4: 211 is the smallest prime q_4 such that $q_4 \mid N_4$
N_5: 2311 is the smallest prime q_5 such that $q_5 \mid N_5$
N_6: 59 is the smallest prime q_6 such that $q_6 \mid N_6$

Problem 28

An alternative proof of the infinitude of the prime numbers begins as follows:

Proof. Suppose there are only finitely many prime numbers. Then one is the largest. Call it p. Let $M = p! + 1$. We will show that there is a prime number q such that $q > p$. Complete this proof.

Solution

Theorem: The set of prime numbers is infinite.

Proof. Suppose there are only finitely many prime numbers. Then one is the largest. Call it p. Let $M = p! + 1$. We will show that there is a prime number q such that $q > p$. It follows from theorem 4.3.4 that M must be divisible by some prime number q. Since $p!$ is the product of every positive integer $\leq p$ and since p is the largest prime number and since q is prime $q \mid p!$. It follows from proposition 4.7.3 that q does not divide $p! + 1$ which equals M. Hence M is divisible by q and M is not divisible by q which is a contradiction. Therefore, the supposition is false and the theorem is true. □

Problem 29

Prove that for all integers n, if $n > 2$ then there is a prime number p such that $n < p < n!$.

Theorem: For all integers n, if $n > 2$ then there is a prime number p such that $n < p < n!$.

Proof. Suppose not. That is suppose that there exists an integer n such that $n > 2$ and for any prime number p, $p \leq n$ or $p \geq n!$. It follows from theorem 4.3.4 that there exists a prime number p such that $p \mid (n! - 1)$. It follows from theorem 4.3.1 that $p \leq n! - 1 < n!$ and so $p \not\geq n!$. Thus $p \leq n$. It follows from theorem 4.7.3 that $p \mid (n! - 1) \implies p \nmid (n!)$. Since $n!$ is the product of all positive integers $\leq n$ if $p \leq n$ then p would divide one of the factors of $n!$ Thus $p > n$. We therefore have that $p \leq n$ and $p > n$ which is a contradiction. Hence the supposition is false and the theorem is true. □

Problem 30

Prove that if $p_1, p_2, ...,$ and p_n are distinct prime numbers with $p_1 = 2$ and $n > 1$, then $p_1 p_2 ... p_n + 1$ can be written in the form $4k + 3$ for some integer k.

Theorem: If $p_1, p_2, ...,$ and p_n are distinct prime numbers with $p_1 = 2$ and $n > 1$, then $p_1 p_2 ... p_n + 1$ can be written in the form $4k + 3$ for some integer k.

Proof. Let $N = p_1 p_2 ... p_n + 1$ such that $p_1, p_2, ...,$ and p_n are distinct prime numbers with $p_1 = 2$ and $n > 1$. Since $p_1 = 2$ and the product of primes has 1 added to it we can conclude that N is odd. It follows from the quotient-remainder theorem that every integer can be expressed as

$$4k \text{ or } 4k + 1 \text{ or } 4k + 2 \text{ or } 4k + 3$$

for some integer k. However since N is odd and $4k$ and $4k + 2$ are even we can conclude that N can be expressed as

$$4k + 1 \text{ or } 4k + 3$$

If $N = 4k + 1$ then

$$4k + 1 = p_1 p_2 ... p_n + 1$$
$$4k = p_1 p_2 ... p_n$$

It follows from the definition of divisibility that $4 \mid (p_1 p_2 ... p_n)$. However this is not possible as all of the primes are distinct and there is only one even prime number, namely 2. And since $4 = 2 \cdot 2$, once the first two is divided out the remaining 2 in the prime factorization of 4 will not divide any of the other primes.

$$\frac{\cancel{p_1} p_2 ... p_n}{\cancel{2} \cdot 2} = \frac{p_2 ... p_n}{2}$$

Therefore N can only be written as $4k + 3$. □

Problem 31

(a) Fermat's last theorem says that for all integers $n > 2$, the equation $x^2 + y^2 = z^2$ has no positive integer solutions. Prove the following: If for all prime number $p > 2$, $x^p + y^p = z^p$ has no positive integer solution, then for any integer $n > 2$ that is not a power of 2, $x^n + y^n = z^n$ has no positive integer solution.

(b) Fermat proved that there are no positive integers x, y, and z such that $x^4 + y^4 = z^4$. Use this result to remove the restriction in part (a) that n not be a power of 2. That is, prove that if n is a power of 2 and $n > 4$, then $x^n + y^n = z^n$ has no positive integer solution.

Solution

(a) *Contrapositive*: If for some integer $n > 2$ that is not a power of 2, $x^n + y^n = z^n$ has a positive integer solution, then for some prime number $p > 2$, $x^p + y^p = z^p$ has a positive integer solution.

Theorem: If for all prime number $p > 2$, $x^p + y^p = z^p$ has no positive integer solution, then for any integer $n > 2$ that is not a power of 2, $x^n + y^n = z^n$ has no positive integer solution.

Proof. Suppose that for some integer $n > 2$ that is not a power of 2, $x^n + y^n = z^n$ has a positive integer solution. Then there exist positive integers a, b, and c such that

$$a^n + b^n = c^n$$

It follows from theorem 4.3.4 that there exists a prime number p such that $p \mid n$. It follows the definition of divisibility and the fact that $n > 0$ and $p > 0$ that

$$n = pk \quad \text{for some integer } k > 0$$

Furthermore, since n is not a power of 2, n must have primes other than 2 in its prime factorization. Therefore we can select p so that $p > 2$. By substitution

$$a^n + b^n = c^n$$
$$a^{pk} + b^{pk} = c^{pk}$$
$$(a^k)^p + (b^k)^p = (c^k)^p$$

It follows from the fact that a, b, c, and k are positive integers and then from closure under multiplication that a^k, b^k, and c^k are positive integers. Now we have a prime number $p > 2$ and positive integers $x = a^k$, $y = b^k$, and $z = c^k$ such that

$$x^p + y^p = z^p$$

□

(b) *Theorem*: If n is a power of 2 and $n > 4$, then $x^n + y^n = z^n$ has no positive integer solution.

Proof. Suppose not. That is suppose that there exists an integer $n > 4$ which is a power of 2 such that $x^n + y^n = z^n$ has a positive integer solution. Then there exist positive integers a, b, and c such that

$$a^n + b^n = c^n$$

Since n is a power of 2, $n = 2^k$ for some integer k. Furthermore, since $n > 4$, $k > 2$ as $2^2 = 4 < n$. By substitution,

$$\begin{aligned} a^n + b^n &= c^n \\ a^{2^k} + b^{2^k} &= c^{2^k} \\ a^{2^2 \cdot 2^{k-2}} + b^{2^2 \cdot 2^{k-2}} &= c^{2^2 \cdot 2^{k-2}} \\ a^{4 \cdot 2^{k-2}} + b^{4 \cdot 2^{k-2}} &= c^{4 \cdot 2^{k-2}} \\ \left(a^{2^{k-2}}\right)^4 + \left(b^{2^{k-2}}\right)^4 &= \left(c^{2^{k-2}}\right)^4 \end{aligned}$$

It follows that since $k > 2$, $k - 2 > 0$ and so 2^{k-2} is a positive integer. It follows from this and the fact that a, b, and c are positive integers that $a^{2^{k-2}}$, $b^{2^{k-2}}$, and $c^{2^{k-2}}$ are also positive integers. Now we have positive integers $x = a^{2^{k-2}}$, $y = b^{2^{k-2}}$, and $z = c^{2^{k-2}}$ such that

$$x^4 + y^4 = z^4$$

But this is a contradiction as Fermat proved that there are no positive integers x, y, and z such that $x^4 + y^4 = z^4$. Hence the supposition is false and the theorem is true which states that for all integers $n > 4$ which are a power of 2, $x^n + y^n = z^n$ has no positive integer solution. □

Problem 32

Prove that there exists a unique prime number of the form $n^2 - 1$, where n is an integer that is greater than or equal to 2.

Theorem: There exists a unique prime number of the form $n^2 - 1$, where n is an integer such that $n \geq 2$.

Proof. Let $n = 2$. Then $n^2 - 1 = 2^2 - 1 = 3$ which is prime and so there exists a prime of the form $n^2 - 1$ where $n \geq 2$. We must now show that every prime that takes the form $n^2 - 1 = 3$. Let m be any integer such that $m^2 - 1$ is prime and $m \geq 2$.

$$m^2 - 1 = (m + 1)(m - 1)$$

Since $m^2 - 1$ is prime either $m + 1 = 1$ or $m - 1 = 1$. But if $m + 1 = 1$ then $m = 0 < 2$ which is a contradiction. Thus $m - 1 = 1$ and so $m = 2$ and $m^2 - 1 = 3$. □

Problem 33

Prove that there exists a unique prime number of the form $n^2 + 2n - 3$, where n is a positive integer.

Theorem: There exists a unique prime number of the form $n^2 + 2n - 3$, where n is an integer such that $n > 0$

Proof. Let $n = 2$. Then $n^2 + 2n - 3 = 2^2 + 2 \cdot 2 - 3 = 5$ which is prime and so there exists a prime of the form $n^2 + 2n - 3$ where $n > 0$. We must now show that every prime that takes the form $n^2 + 2n - 3 = 5$. Let m be any integer such that $m^2 + 2m - 3$ is prime and $m > 0$.

$$m^2 + 2m - 3 = (m + 3)(m - 1)$$

Since $m^2 + 2m - 3$ is prime either $m + 3 = 1$ or $m - 1 = 1$. But if $m + 3 = 1$ then $m = -2 < 0$ which is a contradiction. Thus $m - 1 = 1$ and so $m = 2$ and $m^2 + 2m - 3 = 5$. □

Problem 34

Prove that there is at most one real number a with the property that $a + r = r$ for all real numbers r.

Theorem: There is is at most one real number a with the property that $a+r = r$ for all $r \in \mathbb{R}$

Proof. Suppose that a_1 and a_2 are real numbers such that for all $r \in \mathbb{R}$,

$$a_1 + r = r \ (1) \quad \text{and} \quad a_2 + r = r \ (2)$$

Since a_1 and a_2 are real numbers substitute a_2 for r in equation (1) and substitute a_1 for r in equation (2).

$$a_1 + a_2 = a_2 \quad \text{and} \quad a_2 + a_1 = a_1$$

It follows that

$$a_2 = a_1 + a_1 = a_2 + a_1 = a_1$$

Hence $a_2 = a_1$ and so there is at most one real number a such that $a + r = r$ for all $r \in \mathbb{R}$. □

Problem 35

Prove that there is at most one real number b with the property that $b \cdot r = r$ for all real numbers r.

Theorem: There is at most one real number b with the property that $b \cdot r = r$ for all real numbers r.

Proof. Suppose that b_1 and b_2 are real numbers such that for all $r \in \mathbb{R}$,

$$b_1 \cdot r = r \ (1) \quad \text{and} \quad b_2 \cdot r = r \ (2)$$

Since b_1 and b_2 are real numbers substitute b_2 for r in equation (1) and substitute b_1 for r is equation (2).

$$b_1 \cdot b_2 = b_2 \quad \text{and} \quad b_2 \cdot b_1 = b_1$$

It follows that

$$b_2 = b_1 \cdot b_2 = b_2 \cdot b_1 = b_1$$

Hence $b_2 = b_1$ and so there is at most one real number b such that $b \cdot r = r$ for all $r \in \mathbb{R}$. $\square$