Section 4.4

Sterling Jeppson

October 9, 2020

For each of the values of n and d in problems 1-6, find integers q and r such that $n = dq + r$ and $0 \leq r < d$.

Problem 1

$n = 70$, $d = 9$

Solution

$70 = 9 \cdot 7 + 7$; hence $q = 7$ and $r = 7$.

Problem 2

$n = 62$, $d = 7$

Solution

$62 = 7 \cdot 8 + 4$; hence $q = 8$ and $r = 4$.

Problem 3

$n = 36$, $d = 40$

Solution

$36 = 40 \cdot 0 + 36$; hence $q = 0$ and $r = 36$.

Problem 4

$n = 3$, $d = 11$

Solution

$3 = 11 \cdot 0 + 3$; hence $q = 0$ and $r = 3$.

Problem 5

$n = -45$, $d = 11$

Solution

$-45 = 11 \cdot (-5) + 10$; hence $q = -5$ and $r = 10$.

Problem 6

$n = -27$, $d = 8$

Solution

$-27 = 8 \cdot (-4) + 5$; hence $q = -4$ and $r = 5$.

Problem 7 and Solution

(a) $43\ div\ 9 = 4$

(b) $43\ mod\ 9 = 7$

Problem 8 and Solution

(a) $50\ div\ 7 = 7$

(b) $50\ mod\ 7 = 1$

Problem 9 and Solution

(a) $28\ div\ 5 = 5$

(b) $28\ mod\ 5 = 3$

Problem 10 and Solution

(a) $30\ div\ 2 = 15$

(b) $30\ mod\ 2 = 0$

Problem 11

Verify the correctness of formula 4.4.1($DayN = (DayT + N)\ mod\ 7$, for Sunday = 0, Monday = 1,..., Saturday = 6 and $DayT$ is the day of the week today and $DayN$ is the day of the week in N days.) for the following values of $DayT$ and N.

(a) $DayT = 6$(Saturday) and $N = 15$

(b) $DayT$ = 0(Sunday) and $N = 7$

(c) $DayT$ = 4(Thursday) and $N = 12$

Solution

(a) *Day* 15 = (6 + 15) *mod* 7 = 0 = Sunday

(b) *Day* 7 = (0 + 7) *mod* 7 = 0 = Sunday

(c) *Day* 4 = (4 + 12) *mod* 7 = 2 = Tuesday

Problem 12

Justify the formula used in problem 11 for general values of $DayT$ and N.

Solution

By the quotient remainder theorem there exists some integers q and r such that $DayT$ + N = $7q + r$ with $0 \leq r < 7$. Starting from Sunday(day 0), $DayT$ + N is the number of days until *DayN*. Because the days are counted as 0-6 $DayT$ + N may be greater than 6 and thus would not be a valid day. To make it a valid day we must subtract $7q$, with q being an integer equal to the number of times we leave Sunday starting from $DayT$ and proceeding forward N days. Thus *DayN* = $DayT$ + N - $7q$. But $DayT$ + N - $7q$ = r and so *DayN* = r. Thus

$$DayT + N = 7q + DayN$$

It follows from the definition of *mod* that *DayN* = ($DayT$ + N) *mod* 7.

Problem 13

On a Monday a friend says he will meet you again in 30 days. What day of the week will that be?

Solution

According to the formula given in problem 11, *DayN* = (1 + 30) *mod* 7 = 3. Thus the friend will see you again on Wednesday.

Problem 14

If today is Tuesday, what day of the week will it be 1,000 days from today?

Solution

According to the formula given in problem 11, *DayN* = (2 + 1000) *mod* 7 = 1. Thus the day will be a Monday.

Problem 15

January 1, 2000, was a Saturday, and 2000 was a leap year. What day of the week will January 1, 2050, be?

Solution

There is a leap year every 4 years and so from 2000 to 2050 there will be 13 leap years. There are 50 years from 2000 to 2050 and so there will be 50 - 13 = 37 non leap years. In a regular year there are 365 days but in a leap year there are 366 days. Thus the total number of days is $(366 \cdot 13) + (365 \cdot 37) = 18,263$ days. Since the days in a week never change(always 7 days with Sunday through Saturday) we can still use the formula $DayN = (DayT + N)$ *mod* 7. Thus $DayN$ = (6 + 18,263) *mod* 7 = 6. And so the day of the week will be Saturday.

Problem 16

Suppose that d is a positive integer and n is any integer. If $d \mid n$, what is the remainder obtained when the quotient remainder theorem is applied to n with divisor d?

Solution

By the definition of divides $n = dq = dq + 0$ for some integer q. Thus the remainder obtained is 0.

Problem 17

Prove that the product of any two consecutive integers is even.

Theorem: The product of any two consecutive integers is even.

Proof. Let m be any integer. Then m and $m + 1$ are two consecutive integers.

Case 1(m is even): If m is even then by the Parity of Consecutive Integers theorem $m + 1$ is odd. It follows from the fact that the product of any even integer and any odd integer is even that $m(m + 1)$ is even.

Case 2(m is odd): If m is odd then by the Parity of Consecutive Integers theorem $m + 1$ is even. It follows from the fact that the product of any even integer and any odd integer is even that $m(m + 1)$ is even.

Since $m(m + 1)$ is even in the case that m is odd and in the case that m is odd the product of any two consecutive integers is even. □

Problem 18

The result of exercise 17 suggests that the second apparent blind alley in the discussion of Example 4.4.7 might not be a blind alley after all. Write a new proof of Theorem 4.4.3 based on this observation.

Theorem: The square of any odd integer has the form $8m + 1$ for some integer m.

Proof. Let n be any odd integer. Then $n = 2q + 1$ for some integer q.

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

$q(q + 1)$ is a product of 2 consecutive integers and so by problem 17 it is even. Thus $q(q + 1) = 2m$ for some integer m.

$$4(q(q + 1)) + 1 = 4(2m) + 1 = 8m + 1.$$

Thus for any odd integer n, $n^2 = 8m + 1$ for some integer m. □

Problem 19

Prove that for all integers n, $n^2 - n + 3$ is odd.

Theorem: For all integers n, $n^2 - n + 3$ is odd.

Proof. Suppose that n is any integer.

Case 1(n is even): By definition of odd $n = 2p$ for some integer q.

$$\begin{aligned} n^2 - n + 3 &= (2p)^2 - 2p + 3 \\ &= 4p^2 - 2p + 3 \\ &= 2(2p^2) + 2(-p) + 2 + 1 \\ &= 2(2p^2 - p + 1) + 1 \end{aligned}$$

It follows from closure under multiplication, addition, and subtraction that $2p^2 - p + 1$ is an integer. Let that integer be t. Then $n^2 - n + 3 = 2t + 1$. It follows from the definition of odd that $n^2 - n + 3$ is odd.

Case 2(n is odd): Be definition of odd $n = 2q + 1$ for some integer q.

$$\begin{aligned} n^2 - n + 3 &= (2q+1)^2 - (2q+1) + 3 \\ &= 4q^2 + 4q + 1 - 2q - 1 + 3 \\ &= 4q^2 + 2q + 3 \\ &= 2(2q^2) + 2(q) + 2 + 1 \\ &= 2(2q^2 + q + 1) + 1 \end{aligned}$$

It follows from closure under addition and multiplication that $2q^2 + q + 1$ is an integer. Let that integer be t. Then $n^2 - n + 3 = 2t + 1$. It follows from the definition of odd that $n^2 - n + 3$ is odd.

Since $n^2 - n + 3$ is odd in the case the n is even and in the case that n is odd $n^2 - n + 3$ is odd for any integer n. □

Problem 20

Suppose that a is an integer. If $a \ mod \ 7 = 4$. What is $5a \ mod \ 7$? In other words, if division of a by 7 gives a remainder of 4, what is the remainder when $5a$ is divided by 7?

Solution

If $a \ mod \ 7 = 4$ then $a = 7q + 4$ for some integer q.

$$\begin{aligned} 5a &= 5(7q) + 5(4) \\ 5a &= 7 \cdot 5 \cdot q + 7 \cdot 2 + 6 \\ 5a &= 7(5 \cdot p + 2) + 6 \end{aligned}$$

Thus $5a \ mod \ 7 = 6$.

Problem 21

Suppose that b is an integer. If $b \ mod \ 12 = 5$. What is $8b \ mod \ 12$? In other words, if division of b by 12 gives a remainder of 5, what is the remainder when $8b$ is divided by 12?

Solution

If $b \ mod \ 12 = 5$ then $b = 12q + 5$ for some integer q.

$$\begin{aligned} 8b &= 96q + 40 \\ 8b &= 12 \cdot 8 \cdot q + 12 \cdot 3 + 4 \\ 8b &= 12(8 \cdot q + 3) + 4 \end{aligned}$$

Thus $8b \ mod \ 12 = 4$.

Problem 22

Suppose that c is an integer. If $c\ mod\ 15 = 3$. What is $10c\ mod\ 15$? In other words, if division of c by 15 gives a remainder of 3, what is the remainder when $10c$ is divided by 15?

Solution

If $c\ mod\ 15 = 3$ then $c = 15q + 3$ for some integer q.

$$\begin{aligned}10c &= 150q + 30\\ 10c &= 15 \cdot 10 \cdot q + 15 \cdot 2 + 0\\ 10c &= 15(10 \cdot q + 2) + 0\end{aligned}$$

Thus $10c\ mod\ 15 = 0$.

Problem 23

Prove that for all integers n, if $n\ mod\ 5 = 3$ then $n^2\ mod\ 5 = 4$.

Theorem: For all integers n, if $n\ mod\ 5 = 3$ then $n^2\ mod\ 5 = 4$.

Proof. Let n be any integer such that $n\ mod\ 5 = 3$. Then $n = 5q + 3$ for some integer q.

$$\begin{aligned}n^2 &= 25q^2 + 30q + 9\\ n^2 &= 5 \cdot 5q^2 + 5 \cdot 6q + 5 + 4\\ n^2 &= 5(5q^2 + 6q + 1) + 4\end{aligned}$$

It follows from closure under multiplication and addition that $5q^2 + 6q + 1$ is an integer. Let that integer be t. Then $n^2 = 5t + 4$. Thus $n^2\ mod\ 5 = 4$. □

Problem 24

Prove that for all integers m and n, if $m\ mod\ 5 = 2$ and $n\ mod\ 5 = 1$ then $mn\ mod\ 5 = 2$.

Theorem: For all integers m and n, if $m\ mod\ 5 = 2$ and $n\ mod\ 5 = 1$ then $mn\ mod\ 5 = 2$.

Proof. Let m and n be any integers such that $m\ mod\ 5 = 2$ and $n\ mod\ 5 = 1$. Then $m = 5q + 2$ and $n = 5p + 1$ for some integers p and q.

$$\begin{aligned}mn &= 25qp + 5q + 10p + 2\\ mn &= 5 \cdot 5qp + 5 \cdot q + 5 \cdot 2p + 2\\ mn &= 5(5qp + q + 2p) + 2\end{aligned}$$

It follows from closure under addition and multiplication that $5qp + q + 2p$ is an integer. Let that integer be t. Then $mn = 5t + 2$. Thus $mn\ mod\ 5 = 2$. □

Problem 25

Prove that for all integers a and b, if $a\ mod\ 7 = 5$ and $b\ mod\ 7 = 6$ then $ab\ mod\ 7 = 2$.

Theorem: For all integers a and b, if $a\ mod\ 7 = 5$ and $b\ mod\ 7 = 6$ then $ab\ mod\ 7 = 2$.

Proof. Let a and b be any integers such that $a\ mod\ 7 = 5$ and $b\ mod\ 7 = 6$. Then $a = 7q + 5$ and $b = 7p + 6$ for some integers q and p.

$$\begin{aligned} ab &= 49qp + 42q + 35p + 30 \\ ab &= 7 \cdot 7qp + 7 \cdot 6q + 7 \cdot 5p + 7 \cdot 4 + 2 \\ ab &= 7(7qp + 6q + 5p + 4) + 2 \end{aligned}$$

If follows from closure under multiplication and addition that $7qp + 6q + 5p + 4$ is an integer. Let that integer be t. Then $ab = 7t + 2$. Thus $ab\ mod\ 7 = 2$. □

Problem 26

Prove that a necessary and sufficient condition for a nonnegative integer n to be divisible by a positive integer d is that $n\ mod\ d = 0$.

Theorem: For all nonnegative integers n and positive integers d,
$d \mid n \iff n\ mod\ d = 0$.

Proof. Let a and b be any nonnegative integers such that $d \mid n$.

$$\begin{aligned} n &= dk \quad \text{for some integer k} \\ n &= dk + 0 \end{aligned}$$

Thus $n\ mod$ d = 0.

Now Let a and b be any nonnegative integers such that $n\ mod\ d = 0$.

$$\begin{aligned} n &= dk + 0 \quad \text{for some integer k} \\ n &= dk \end{aligned}$$

Thus $d \mid n$.

Since $d \mid n \implies n\ mod\ d = 0$ and $n\ mod\ d = 0 \implies d \mid n$ we conclude that $d \mid n \iff n\ mod\ d = 0$. □

Problem 27

Show that any integer n can be written in one of the three forms

$$n = 3q \quad \text{or} \quad n = 3q + 1 \quad \text{or} \quad n = 3q + 2$$

for some integer q.

Proof. Let n be an integer. Then by the quotient-remainder theorem with $d = 3$, there exists integers q and r such that $n = 3q + r$ with $0 \leq r < 3$. But the only integers that are in the range from $[0, 3)$ are 0, 1, and 2. Thus

$$n = 3q \quad \text{or} \quad n = 3q + 1 \quad \text{or} \quad n = 3q + 2$$

for some integer q. □

Problem 28

(a) Use the quotient-remainder theorem with $d = 3$ to prove that the product of any three consecutive integers is divisible by 3.

(b) Use the *mod* notation to rewrite the results of part (a).

Solution

(a) *Theorem*: The product of any three consecutive integers is divisible by 3.

Proof. Let n be any integer. Then $n(n + 1)(n + 2)$ is a product of any three consecutive integers. By the quotient-remainder theorem

$$n = 3q \quad \text{or} \quad n = 3q + 1 \quad \text{or} \quad n = 3q + 2$$

for some integer q.

Case 1 $(n = 3q)$:

$$\begin{aligned} n(n+1)(n+2) &= 3q(3q+1)(3q+2) \\ &= 27q^3 + 27q^2 + 6q \\ &= 3(9q^3 + 9q^2 + 2q) \end{aligned}$$

It follows from closure under multiplication and addition that $9q^3+9q^2+2q$ is an integer. Let that integer be t then $n(n + 1)(n + 2) = 3t$. Thus $3 \mid (n(n + 1)(n + 2))$.

Case 2 $(n = 3q + 1)$:

$$\begin{aligned} n(n+1)(n+2) &= (3q+1)(3q+2)(3q+3) \\ &= 27q^3 + 54q^2 + 33q + 6 \\ &= 3(9q^3 + 18q^2 + 11q + 2) \end{aligned}$$

It follows from closure under multiplication and addition that $9q^3+18q^2+11q + 2$ is an integer. Let that integer be t. Then $n(n + 1)(n + 2) = 3t$. Thus $3 \mid (n(n + 1)(n + 2))$.

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

$$\begin{aligned} n(n+1)(n+2) &= (3q+2)(3q+3)(3q+4) \\ &= 27q^3 + 81q^2 + 78q + 24 \\ &= 3(9q^3 + 9q^2 + 26q + 8) \end{aligned}$$

It follows from closure under multiplication and addition that $9q^3 + 9q^2 + 26q + 8$ is an integer. Let that integer be t. Then $n(n+1)(n+2) = 3t$. Thus $3 \mid (n(n+1)(n+2))$.

Since $3 \mid n(n+1)(n+2)$ in the case that $n = 3q$, $n = 3q+1$, and $n = 3q+2$ and since the quotient remainder theorem guarantees that every integer can be expressed in one of these forms, we can conclude that for any integer n, $3 \mid (n(n+1)(n+2))$. Thus the product of any three consecutive integers is divisible by 3. □

(b) For all integers n, $n(n+1)(n+2)$ *mod* $3 = 0$.

Problem 29

(a) Use the quotient remainder theorem with $d = 3$ to prove that the square of any integer has the form $3k$ or $3k+1$ for some integer k.

(b) Use the mod notation the rewrite the results of part (a).

Solution

(a) *Theorem*: The square of any integer has the form $3k$ or $3k+1$ for some integer k.

Proof. Let n be any integer. By the quotient-remainder theorem
$$n = 3q \quad \text{or} \quad n = 3q+1 \quad \text{or} \quad n = 3q+2$$
for some integer q.

Case 1$(n = 3q)$:

$$\begin{aligned} n^2 &= (3q)^2 \\ &= 9q^2 \\ &= 3(3q^2) \end{aligned}$$

It follows from closure under multiplication that $3q^2$ is an integer. Let that integer be k. Then $n^2 = 3k$.

*Case 2*$n = 3q+1$:

$$\begin{aligned} n^2 &= (3q+1)^2 \\ &= 9q^2 + 6q + 1 \\ &= 3(3q^2 + 2q) + 1 \end{aligned}$$

It follows from closure under multiplication and addition that $3q^2 + 2q$ is an integer. Let that integer be k. Then $n^2 = 3k + 1$.

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

$$\begin{aligned} n^2 &= (3q+2)^2 \\ &= (9q^2 + 6q + 4 \\ &= (9q^2 + 6q + 3 + 1 \\ &= 3(3q^2 + 2q + 1) + 1 \end{aligned}$$

It follows from closure under multiplication and addition that $3q^2+2q+1$ is an integer. Let that integer be k then $n^2 = 3k + 1$.

Since n^2 can be written in the form $3k$ or $3k + 1$ in the case that $n = 3q$, $n = 3q + 1$, and $n = 3q + 2$ and since the quotient-remainder theorem guarantees that every integer can be expressed in one of these forms, we can conclude that for any integer n, $n^2 = 3k$ or $n^2 = 3k + 1$ for some integer k. □

(b) For all integers n, $n^2 \ mod \ 3 = 0$ or $n^2 \ mod \ 3 = 1$.

Problem 30

(a) Use the quotient-remainder theorem with $d = 3$ to prove that the product of any two consecutive integers has the form $3k$ or $3k+2$ for some integer k.

(b) Use the *mod* notation the rewrite the result of part (a).

Solution

(a) *Theorem*: The product of any two consecutive integers has the form $3k$ or $3k + 2$ for some integer k.

Proof. Let n be any integer. Then $n(n+1)$ defines the product of any two consecutive integers. By the quotient-remainder theorem

$$n = 3q \quad \text{or} \quad n = 3q + 1 \quad \text{or} \quad n = 3q + 2$$

for some integer q.

Case 1 $(n = 3q)$:

$$\begin{aligned} n(n+1) &= 3q(3q+1) \\ &= 9q^2 + 3q \\ &= 3(3q^2 + 1) \end{aligned}$$

It follows from closure under multiplication and addition that $3q^2 + 1$ is an integer. Let that integer be k then $n(n + 1) = 3k$.

Case 2 $(n = 3q + 1)$:

$$\begin{aligned} n(n+1) &= (3q+1)(3q+2) \\ &= (9q^2 + 9q + 2) \\ &= 3(3q^2 + 3q) + 2 \end{aligned}$$

It follows from closure under multiplication and addition that $3q^2 + 3q$ is an integer. Let that integer be k then $n(n+1) = 3k + 2$.

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

$$\begin{aligned} n(n+1) &= (3q+2)(3q+3) \\ &= (9q^2 + 15q + 6) \\ &= 3(3q^2 + 5q + 2) \end{aligned}$$

It follows from closure under multiplication and addition that $3q^2 + 5q + 2$ is an integer. Let that integer be k then $n(n+1) = 3k$.

Since $n(n+1)$ can be written in the form $3k$ or $3k + 2$ in the case that $n = 3q$, $n = 3q+1$, and $n = 3q+2$ and since the quotient-remainder theorem guarantees that every integer can be expressed in one of these forms, we can conclude that for any integer n, $n(n+1) = 3k$ or $n(n+1) = 3k+2$ for some integer k. □

(b) For all integers n, $n(n+1)$ *mod* $3 = 0$ or $n(n+1)$ *mod* $3 = 2$.

0.1 Problem 31

(a) Prove that for all integers m and n, $m+n$ and $m-n$ are either both odd or both even.

(b) Find all solutions to the equation $m^2 - n^2 = 56$ for which both m and n are positive integers.

(c) Find all solutions to the equation $m^2 - n^2 = 88$ for which both m and n are positive integers.

Solution

(a) *Theorem*: For all integers m and n, $m+n$ and $m-n$ are either both odd or both even.

Proof. Let m and n be any integers. By the parity property m must be either even or odd and n must be either even or odd.

Case 1(m even n even): Since the sum and difference of any two even integers is even $m + n$ is even and $m - n$ is even.

Case 2(opposite parity): Since the sum and difference of any even integer and any odd integer is odd. $m + n$ is odd and $m - n$ is odd.

Case 3(m odd n odd): Since the sum and difference of any two odd integers is even $m + n$ is even and $m - n$ is even.

Since $m + n$ and $m - n$ have the same parity for any combination of even and odd parity of m and n and since the parity property guarantees that all integers have either even or odd parity we can conclude that for all integers m and n, $m + n$ and $m - n$ are either both odd or both even. □

(b) $m^2 - n^2 = (m + n)(m - n)$. By part (a) above $m + n$ and $m - n$ must be either both even or both odd for any integers m and n. However $(m + n)(m - n) = 56$ and 56 is even. Thus $m + n$ and $m - n$ cannot both be odd as the product of any two odd integers is odd and so they must both be even. The only two pairs of even integers that multiply to 56 are $2 \cdot 28$ and $4 \cdot 14$. Since m and n must both be positive $(m + n) > (m - n)$. Thus two systems of equations arise.

$$\begin{aligned} m + n &= 28 \qquad & m + n &= 14 \\ m - n &= 2 \qquad & m - n &= 4 \end{aligned}$$

Solving each system of equations gives $m = 15$, and $n = 13$ or $m = 9$ and $n = 5$.

(c) Similar to part (b) above two systems of equations arise

$$\begin{aligned} m + n &= 44 \qquad & m + n &= 22 \\ m - n &= 2 \qquad & m - n &= 4 \end{aligned}$$

Solving each system of equations gives $m = 23$, and $n = 21$ or $m = 13$ and $n = 9$.

Problem 32

Given any integers a, b, and c, if $a - b$ is even and $b - c$ is even, what can you say about the parity of $2a - (b + c)$? Prove your answer.

Theorem: Given any integers a, b, and c, if $a - b$ is even and $b - c$ is even then $2a - (b + c)$ has even parity.

Proof. Let a, b, and c be any integers such that $a - b$ is even and $b - c$ is even. It follows from the fact that the product of any two even integers is even that

$2(a-b)$ is even. It follows from the fact that the sum or any two even integers is even that $2(a-b)+(b-c)$ is even.

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

Since $2(a-b)+(b-c) = 2a-(b+c)$ and $2(a-b)+(b-c)$ is even, $2a-(b+c)$ must be even. □

Problem 33

Given any integers a, b, and c, if $a-b$ is odd and $b-c$ is even, what can you say about the parity of $a-c$? Prove your answer.

Theorem: Given any integers a, b, and c, if $a-b$ is odd and $b-c$ is even, then $a-c$ is odd.

Proof. Let a, b, and c be any integers such that $a-b$ is odd and $b-c$ is even. It follows from the fact that the sum of any odd integer and any even integer is odd that $(a-b)+(b-c)$ is odd. Since $(a-b)+(b-c) = a-c$ we can conclude that $a-c$ is odd. □

Problem 34

Given any integer n, if $n > 3$, could n, $n+2$, and $n+4$ all be prime? Prove or give a counterexample.

Theorem: Given any integer n, if $n > 3$ then it is not possible for n, $n+2$, and $n+4$ to all be prime.

Proof. Let n be any integer such that $n > 3$. By the quotient-remainder theorem

$$n = 3q \quad \text{or} \quad n = 3q+1 \quad \text{or} \quad n = 3q+2$$

for some integer q.

Case 1 $(n = 3q)$: If $n = 3q$ then n cannot be prime as $1 < 3 < n$ and $3 \mid n$ which contradicts the definition of prime.

Case 2 $(n = 3q+1)$: If $n = 3q+1$ then $n+2 = 3q+3 = 3(q+1)$. It follows then that $n+2$ cannot be prime as $1 < 3 < n+2$ and $3 \mid (n+2)$ which contradicts the definition of prime.

Case 3 $(n = 3q+2)$: If $n = 3q+2$ then $n+4 = 3q+6 = 3(q+2)$. It follows then that $n+4$ cannot be prime as $1 < 3 < n+4$ and $3 \mid (n+4)$ which contradicts the definition of prime.

The quotient-remainder theorem guarantees that any integer n can be expressed in one of the above forms. In all of these forms for n being any integer greater than 3, at least one case of n, $n+2$, or $n+4$ is not prime. Thus we can conclude that it is not possible for n, $n+2$, and $n+4$ to all be prime if n is any integer greater than 3. □

Problem 35

Prove that the fourth power of any integer has the form $8m$ or $8m+1$ for some integer m.

Theorem: The fourth power of any integer has the form $8m$ or $8m+1$ for some integer m.

Proof. Let n be any integer. By the parity property n is either even or odd.

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

$$n^4 = (2k)^4 = 8(2k^4)$$

It follows from closure under multiplication that $2k^4$ is an integer. Let that integer be m. Then $n^4 = 8m$.

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

$$n^4 = 16k^4 + 32k^3 + 24k^2 + 8k + 1 = 8(2k^2 + 4k^3 + 3k^2 + k) + 1$$

It follows from closure under multiplication and addition that $2k^2+4k^3+3k^2+k$ is an integer. Let that integer be m. Then $n^4 = 8m+1$.

Since all integers are either even or odd and since for some integer m, $n^4 = 8m$ in the case that n is even and $n^4 = 8m+1$ in the case that n is odd, we can conclude that the fourth power of all integers can be written in the form $8m$ or $8m+1$. □

Problem 36

Prove that the product of any four consecutive integers is divisible by 8.

Theorem: The product of any four consecutive integers is divisible by 8.

Proof. Let n be any integer. Then $n(n+1)(n+2)(n+3)$ defines the product of any four consecutive integers. By the quotient-remainder theorem

$$n = 4q \quad \text{or} \quad n = 4q+1 \quad \text{or} \quad n = 4q+2 \quad \text{or} \quad n = 4q+3$$

for some integer q.

Case 1 $(n = 4q)$:

$$\begin{aligned} n(n+1)(n+2)(n+3) &= 4q(4q+1)(4q+2)(4q+3) \\ &= 256q^4 + 384q^3 + 176q^2 + 24q \\ &= 8(32q^4 + 48q^3 + 22q^2 + 3q) \end{aligned}$$

It follows from closure under multiplication and addition that $32q^4 + 48q^3 + 22q^2 + 3q$ is an integer. Let that integer be m. Then $n(n+1)(n+2)(n+3) = 8m$. It follows that $8 \mid (n(n+1)(n+2)(n+3))$.

Case 2 $(n = 4q + 1)$:

$$\begin{aligned} n(n+1)(n+2)(n+3) &= (4q+1)(4q+2)(4q+3)(4q+4) \\ &= 256q^4 + 640q^3 + 560q^2 + 200q + 24 \\ &= 8(32q^4 + 80q^3 + 70q^2 + 25q + 3) \end{aligned}$$

It follows from closure under multiplication and addition that $32q^4 + 80q^3 + 70q^2 + 25q + 3$ is an integer. Let that integer be m. Then $n(n+1)(n+2)(n+3) = 8m$. It follows that $8 \mid (n(n+1)(n+2)(n+3))$.

Case 1 $(n = 4q + 2)$:

$$\begin{aligned} n(n+1)(n+2)(n+3) &= (4q+2)(4q+3)(4q+4)(4q+5) \\ &= 256q^4 + 896q^3 + 1136q^2 + 616q + 120 \\ &= 8(32q^4 + 112q^3 + 142q^2 + 77q + 15) \end{aligned}$$

It follows from closure under multiplication and addition that $32q^4 + 112q^3 + 142q^2 + 77q + 15$ is an integer. Let that integer be m. Then $n(n+1)(n+2)(n+3) = 8m$. It follows that $8 \mid (n(n+1)(n+2)(n+3))$.

Case 1 $(n = 4q + 3)$:

$$\begin{aligned} n(n+1)(n+2)(n+3) &= (4q+3)(4q+4)(4q+5)(4q+6) \\ &= 256q^4 + 1152q^3 + 1904q^2 + 1368q + 360 \\ &= 8(32q^4 + 144q^3 + 238q^2 + 171q + 45) \end{aligned}$$

It follows from closure under multiplication and addition that $32q^4 + 144q^3 + 238q^2 + 171q + 45$ is an integer. Let that integer be m. Then $n(n+1)(n+2)(n+3) = 8m$. It follows that $8 \mid (n(n+1)(n+2)(n+3))$.

Since $8 \mid (n(n+1)(n+2)(n+3))$ no matter which form n takes under the quotient-remainder theorem with $d = 4$ we can conclude that the product of any four consecutive integers is divisible by 8. □

Problem 37

Prove that the square of any integer has the form $4k$ or $4k+1$ for some integer k.

Theorem: The square of any integer has the form $4k$ or $4k + 1$ for some integer k.

Proof. Let n be any integer. By the parity property n is either even or odd.

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

$$\begin{aligned} n^2 &= (2r)^2 \\ &= 4r^2 \end{aligned}$$

It follows from closure under multiplication that r^2 is an integer. Let that integer be k. Then $n^2 = 4k$.

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

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

It follows from closure under multiplication and addition that $r^2 + r$ is an integer. Let that integer be k. Then $n^2 = 4k + 1$.

Since n^2 can be written in the form $4k$ if n is even and $4k + 1$ if n is odd and since all integers are either even or odd we can conclude that the square of any integer has the form $4k$ or $4k + 1$ for some integer k. □

Problem 38

Prove that for any integer n, $n^2 + 5$ is not divisible by 4.

Theorem: For any integer n, $n^2 + 5$ is not divisible by 4.

Proof. Let n be any integer. By the parity property n is either even or odd.

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

$$\begin{aligned} n^2 + 5 &= (2r)^2 + 5 \\ &= 4r^2 + 5 \\ &= 4(r^2 + 1) + 1 \end{aligned}$$

It follows from the definition of *mod* that $(n^2 + 5)$ *mod* $4 = 1$. Thus $4 \nmid (n^2 + 5)$.

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

$$\begin{aligned} n^2 + 5 &= (2r+1)^2 + 5 \\ &= 4r^2 + 4r + 1 + 5 \\ &= 4r^2 + 4r + 4 + 2 \\ &= 4(r^2 + r + 1) + 2 \end{aligned}$$

It follows from the definition of *mod* that $(n^2 + 5)$ *mod* $4 = 2$. Thus $4 \nmid (n^2 + 5)$. Since $4 \nmid (n^2 + 5)$ in the case that n is even, and in the case that n is odd and since all integer are either even or odd we can conclude that there is no integer n such that $4 \mid (n^2 + 5)$. □

Problem 39

Prove that the sum of any four consecutive integers has the form $4k+2$ for some integer k.

Theorem: The sum of any four consecutive integers has the form $4k + 2$ for some integer k.

Proof. Let n be any integer. Then $n + (n+1) + (n+2) + (n+3)$ defines a sum of any 4 consecutive integers. By the parity property all integers are either even or odd.

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

$$\begin{aligned} n + (n+1) + (n+2) + (n+3) &= 2s + (2s+1) + (2s+2) + (2s+3) \\ &= 8s + 4 + 2 \\ &= 4(2s+1) + 2 \end{aligned}$$

It follows from closure under addition that $2s+1$ is an integer. Let that integer be k. Then $n + (n+1) + (n+2) + (n+3) = 4k + 2$.

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

$$\begin{aligned} n + (n+1) + (n+2) + (n+3) &= (2s+1) + (2s+2) + (2s+3) + (2s+4) \\ &= 8s + 8 + 2 \\ &= 4(2s+2) + 2 \end{aligned}$$

It follows from closure under addition that $2s+2$ is an integer. Let that integer be k. Then $n + (n+1) + (n+2) + (n+3) = 4k + 2$.

Since $n + (n+1) + (n+2) + (n+3)$ can be written as $4k + 2$ in the case that n is even or n is odd and since all integers are either even or odd, we can conclude that The sum of any four consecutive integers has the form $4k + 2$ for some integer k. □

Problem 40

Prove that for any integer n, $n(n^2-1)(n+2)$ is divisible by 4.

Theorem: For any integer n, $n(n^2-1)(n+2)$ is divisible by 4.

Proof. Let n be any integer. By the parity property n is either even or odd.

Case 1(n is even): If n is even then the product takes the form

$$\begin{aligned} n(n^2-1)(n+2) &= n(n+1)(n-1)(n+2) \\ &= (n-1)(n)(n+1)(n+2) \\ &= (\text{odd} \cdot \text{even}) \cdot (\text{odd} \cdot \text{even}) \\ &= \text{even} \cdot \text{even} \end{aligned}$$

Since $n(n^2-1)(n+2)$ takes this form it can be written as $(2s)(2r)$ for some integers s and r. Thus is can be written as $4(sr)$. It follows from closure under multiplication that sr is an integer. Let that integer be k. Then $n(n^2-1)(n+2) = 4k$. It follows from the definition of divisibility that $4 \mid (n(n^2-1)(n+2))$.

Case 2(n is odd): If n is odd then the product takes the form

$$\begin{aligned} n(n^2-1)(n+2) &= n(n+1)(n-1)(n+2) \\ &= (n-1)(n)(n+1)(n+2) \\ &= (\text{even} \cdot \text{odd}) \cdot (\text{even} \cdot \text{odd}) \\ &= \text{even} \cdot \text{even} \end{aligned}$$

Since $n(n^2-1)(n+2)$ takes this form it can be written as $(2s)(2r)$ for some integers s and r. Thus is can be written as $4(sr)$. It follows from closure under multiplication that sr is an integer. Let that integer be k. Then $n(n^2-1)(n+2) = 4k$. It follows from the definition of divisibility that $4 \mid (n(n^2-1)(n+2))$.

Since $n(n^2-1)(n+2)$ is divisible by 4 in the case that n is even or odd and all integers are either even or odd we can conclude that For any integer n, $n(n^2-1)(n+2)$ is divisible by 4. □

Problem 41

Prove that for all integers m, $m^2 = 5k$, or $m^2 = 5k+1$, or $m^2 = 5k+4$ for some integer k.

Theorem: For all integers m, $m^2 = 5k$, or $m^2 = 5k+1$, or $m^2 = 5k+4$ for some integer k.

Proof. Let m be any integer. By the quotient-remainder theorem

$m = 5q$ or $m = 5q+1$ or $m = 5q+2$ or $m = 5q+3$ or $m = 5q+4$

for some integer q.

Case 1$(m = 5q)$: $m^2 = 25q^2 = 5(5q^2) = 5k$, for some integer $k = 5q^2$.

Case 2$(m = 5q + 1)$: $m^2 = 25q^2 + 10q + 1 = 5(5q^2 + 2q) + 1 = 5k + 1$, for some integer $k = 5q^2 + 2q$.

Case 3$(m = 5q + 2)$: $m^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 = 5k + 4$, for some integer $k = 5q^2 + 4q$.

Case 4$(m = 5q + 3)$: $m^2 = 25q^2 + 30q + 9 = 5(5q^2 + 6q + 1) + 4 = 5k + 4$, for some integer $k = 5q^2 + 6q + 1$.

Case 5$(m = 5q + 4)$: $m^2 = 25q^2 + 40q + 16 = 5(5q^2 + 8q + 3) + 1 = 5k + 1$, for some integer $k = 5q^2 + 8q + 3$.

Since m^2 takes the form $5k$ or $5k+1$ or $5k+4$ in all of the above cases and since every integer is guaranteed to take one of the above forms, we can conclude that for all integers m, $m^2 = 5k$, or $m^2 = 5k + 1$, or $m^2 = 5k + 4$ for some integer k. □

Problem 42

Prove that every prime number except 2 and 3 has the form $6q + 1$ or $6q + 5$ for some integer q.

Theorem: Every prime number except 2 and 3 has the form $6q + 1$ or $6q + 5$ for some integer q.

Proof. Let n be any prime number except 2 or 3. Then n is an integer and by the quotient-remainder theorem

$$n = 6q \text{ or } n = 6q + 1 \text{ or } n = 6q + 2 \text{ or } n = 6q + 3 \text{ or } n = 6q + 4 \text{ or } n = 6q + 5$$

for some integer q.

Case 1$(n = 6q)$: But this cannot be as n is prime but $6 \mid n$ which is a contradiction.

Case 2$(n = 6q + 1)$: No contradiction as by definition the only numbers that divides n are n and 1

Case 3$(n = 6q + 2)$: But this cannot be as n is prime but $2 \mid n$ which is a contradiction.

Case 4$(n = 6q + 3)$: But this cannot be as n is prime but $3 \mid n$ which is a contradiction.

Case 5$(n = 6q + 4)$: But this cannot be as n is prime but $2 \mid n$ which is a contradiction.

Case 6$(n = 6q + 5)$: No contradiction as by definition the only numbers that divides n are n and 1

Since no prime numbers except 2 and 3 take any of the forms in Case 1, Case 3, Case 4, and Case 6 and since all integers can be represented in one of the forms from Case 1 through Case 6 and since all primes are integers we can conclude that every prime except 2 or 3 has the form $6q + 1$ or $6q + 5$ for some integer q. □

Problem 43

Prove that if n is an odd integer, then n^4 *mod* $16 = 1$.

Theorem: If n is an odd integer, then n^4 *mod* $16 = 1$.

Proof. Let n be any odd integer. By the quotient-remainder theorem

$$n = 4q + 1 \text{ or } n = 4q + 3$$

for some integer q.

Case 1$(n = 4q + 1)$:

$$\begin{aligned} n^4 &= (4q+1)^4 \\ &= 256q^4 + 256q^3 + 96q^2 + 16q + 1 \\ &= 4(64q^4 + 64q^3 + 24q^2 + 4q) + 1 \\ &= 4k + 1, \quad \text{for some integer } k \end{aligned}$$

Case 2$(n = 4q + 3)$:

$$\begin{aligned} n^4 &= (4q+3)^4 \\ &= 256q^4 + 768q^3 + 864q^2 + 432q + 81 \\ &= 4(64q^4 + 192q^3 + 216q^2 + 108q + 20) + 1 \\ &= 4k + 1, \quad \text{for some integer } k \end{aligned}$$

Since $n^4 = 4k + 1$, for some integer k in both of the cases above and since every odd integer can be represented as one of the two forms above we can conclude that if n is an odd integer, then n^4 *mod* $16 = 1$. □

Problem 44

Prove that for all real numbers x and y, $|x| \cdot |y| = |xy|$.

Theorem: For all real numbers x and y, $|x| \cdot |y| = |xy|$.

Proof. Let x and y be any real numbers.
Case 1($x \geq 0$ and $y \geq 0$):

$$\begin{aligned} |x| \cdot |y| &= x \cdot y \\ &= |xy| \end{aligned}$$

Case 2($x \geq 0$ and $y < 0$):

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

Case 3($x < 0$ and $y \geq 0$):

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

Case 1($x < 0$ and $y < 0$):

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

Since all every possible combination of two real numbers belongs to one of cases 1-4, and since in each case of 1-4 $|x| \cdot |y| = |xy|$, we can conclude that for all real numbers x and y, $|x| \cdot |y| = |xy|$. □

Problem 45

Prove that for all real numbers r and c with $c \geq 0$, if $-c \leq r \leq c$, then $|r| \leq c$.

Theorem: For all real numbers r and c with $c \geq 0$, if $-c \leq r \leq c$, then $|r| \leq c$.

Proof. Let r and c be real numbers such that $c \geq 0$ and $-c \leq r \leq c$.

Case 1($r \geq 0$): Since $r \geq 0$ by definition $r = |r|$. Thus $r \leq c \implies |r| \leq c$.

Case 2($r < 0$): Since $r < 0$ by definition $|r| = -r$. Thus $r = -|r|$.

$$\begin{aligned} -c &\leq r \\ -c &\leq -|r| \\ c &\geq |r| \\ |r| &\leq c \end{aligned}$$

Since $|r| \leq c$ in the case that $r < 0$ and in the case that $r \geq 0$ and since all real numbers meet one of those two criteria we can conclude that for all real numbers r and c with $c \geq 0$, if $-c \leq r \leq c$, then $|r| \leq c$. □

Problem 46

Prove that for all real numbers r and c with $c \geq 0$, if $|r| \leq c$, then $-c \leq r \leq c$.

Theorem: For all real numbers r and c with $c \geq 0$, if $|r| \leq c$, then $-c \leq r \leq c$.

Proof. Let r and c be real numbers such that $c \geq 0$ and $|r| \leq c$.

Case 1 $(r \geq 0)$: Since $r \geq 0$ by definition $r = |r|$ and so $r \leq c$.

$$\begin{aligned} r &\geq 0 \\ c &\geq 0 \\ -c \leq 0 &\leq r \\ -c \leq r &\leq c \end{aligned}$$

Case 2 $(r < 0)$: Since $r < 0$ by definition $|r| = -r$ and so $-r \leq c$. Thus $-c \leq r$.

$$\begin{aligned} r &< 0 \\ c &\geq 0 > r \\ c &\geq r \\ r &\leq c \\ -c \leq r &\leq c \end{aligned}$$

Thus regardless of whether $r \geq 0$ or $r < 0$, $|r| \leq c \implies -c \leq r \leq c$. □

Problem 47

A Matrix $\mathbf{M}$ has 3 rows and 4 column.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$$

The 12 entries in the matrix are to be stored in row major form in locations 7,609 to 7,620 in a computers main memory. This means that the entries in the first row are stored first, then the entries in the second row, and finally the entries in the third row.

(a) Which location will a_{22} be stored in?

(b) Write a formula in i and j that gives the integer n so that a_{ij} is stored in location 7,609 + n.

(c) find formulas in n for r and s so that a_{rs}, is stored in location 7,609 + n.

Solution

(a) a_{22} will be stored in 7,614

(b) $n = 4(i - 1) + (j - 1)$

(c) $r = n\ div\ 4 + 1$, $s = n\ mod\ 4 + 1$

Problem 48

Let **M** be a matrix with m rows and n columns, and suppose that the entries of **M** are stored in a computer's memory in row major form in locations N, $N + 1$, $N + 2$,..., $N + mn - 1$. Find formulas in k for r and s so that a_{rs} is stored in location $N + k$.

Solution

$r = k\ div\ n + 1$, $s = k\ mod\ n + 1$.

Problem 49

If m, n, and d are integers, $d > 0$, and $m\ mod\ d = n\ mod\ d$, does it necessarily follows that $m = n$? That $m - n$ is divisible by d? Prove your answers.

Counterexample: Let $m = 4$, $n = 2$, $d = 2$. Then $m\ mod\ d = n\ mod\ d$ but $m \neq n$.

Theorem: If m, n, and d are integers, such that $d > 0$, and $m\ mod\ d = n\ mod\ d$, then $m - n$ is divisible by d.

Proof. Let m, n, and d be integers such that $d > 0$ and $m\ mod\ d = n\ mod\ d$. Let r be an integer such that $r = m\ mod\ d$. Then $r = n\ mod\ d$. Also by the definition of *mod* $n = dq + r$ and $m = dp + r$ for some integers q and p.

$$\begin{aligned} m - n &= dp + r - (dq + r) \\ &= dp + r - dq - r \\ &= dp - dq \\ &= d(p - q) \end{aligned}$$

It follows from closure under subtraction that $p - q$ is an integer. Let that integer be k then $m - n = dk$ It follows from the definition of divisibility that $d \mid (m - n)$. □

Problem 50

If m, n, and d are integers, with $d > 0$, and $d \mid (m - n)$, what is the relation between $m\ mod\ d$ and $n\ mod\ d$? Prove your answer.

Theorem: If m, n, and d are integers such that $d > 0$, and $d \mid (m - n)$ then n $mod\ d = m\ mod\ d$.

Proof. Let m, n, and d be integers such that $d > 0$ and $d \mid (m - n)$. Suppose that $m\ mod\ d = r$ and that $n\ mod\ d = s$ for some integers r and s. Then $m = dq + r$ and $n = dp + s$ for some integers q and p with such that $0 \le r < d$ and $0 \le s < d$.

$$\begin{aligned} m - n &= dq + r - (dp + s) \\ &= dq + r - dp - s \\ &= d(q - p) + r - s \\ &= dc + b \end{aligned}$$

It follows from closure under subtraction that c and b are both integers. We know that $d \mid (m - n)$ and so $d \mid (dc + b)$. This means that b must be able to be written as a multiple of d so that $b = dk$ for some integer k. But $b = r - s$ and $0 \le r < d$ and $0 \le s < d$. Thus the only multiple of d that $r - s$ can be is 0, and so $k = 0$ and thus $b = 0$. Since $b = 0$ it follows that $r = s$. Thus $m\ mod$ $d = n\ mod\ d$. □

Problem 51

If m, n, a, b, and d are integers, $d > 0$, and $m\ mod\ d = a$ and $n\ mod\ d = b$, is $(m+n)\ mod\ d = a+b$? Is $(m+n)\ mod\ d = (a+b)\ mod\ d$? Prove your answers.

Solution

Part 1: Let m, n, a, and b be integers such that $d > 0$ and $m\ mod\ d = a$ and $n\ mod\ d = b$. Then $m = dq + a$ and $n = dp + b$ for some integers q and p such that $0 \le a < d$ and $0 \le b < d$.

$$\begin{aligned} m + n &= dq + a + dp + b \\ &= dq + dp + a + b \\ &= d(q + p) + a + b \end{aligned}$$

Suppose that $(m + n)\ mod\ d = a + b$. Then $m + n = dr + a + b$ such that $0 \le a + b < d$. But this is not true as $a + b$ can be greater than or equal to d.

Counterexample: Let $m = 8$, $n = 10$, and $d = 3$. Then $m\ mod\ d = 2$ and n $mod\ d = 1$. Then $a = 2$, $b = 1$, and $a+b = 3$, but $(m+n)\ mod\ d = 0 \ne a+b = 3$.

Part 2: *Theorem*: If m, n, a, b, and d are integers, $d > 0$, and $m\ mod\ d = a$ and $n\ mod\ d = b$, then $(m + n)\ mod\ d = (a + b)\ mod\ d$.

Proof. Let m, n, a, b, and d be integers such that $d > 0$ and m *mod* $d = a$ and n *mod* $d = b$. Then $m = dq + a$ and $n = dp + b$ for some integers q and p such that $0 \le a < d$ and $0 \le b < d$. By the quotient remainder theorem $a + b = sd + r$ for some integers r and s such that $0 \le r < d$. Thus $(a + b)$ *mod* $d = r$.

$$\begin{aligned} m + n &= dq + a + dp + b \\ &= dq + dp + a + b \\ &= dq + dp + sd + r \\ &= d(q + p + s) + r \end{aligned}$$

It follows from closure under addition that $q + p + s$ is an integer. Let that integer be t. Then $m + n = dt + r$. It follows from the definition of r that $0 \le r < d$. It now follows from the definition of *mod* that $m + n$ *mod* $d = r$. Since $r = (a + b)$ *mod* d, we can conclude that $(m + n)$ *mod* $d = (a + b)$ *mod* d. □

Problem 52

If m, n, a, b, and d are integers and $d > 0$, and m *mod* $d = a$ and n *mod* $d = b$, is mn *mod* $d = ab$? Is mn *mod* $d = ab$ *mod* d? Prove your answer.

Solution

Part 1: Let m, n, a, b, and d be integers such that $d > 0$ and m *mod* $d = a$ and n *mod* $d = b$. Then $m = dq + a$ and $n = dp + b$ for some integers q and p such that $0 \le a < d$ and $0 \le b < d$.

$$\begin{aligned} mn &= (dq + a)(dp + b) \\ &= d^2qp + dqb + dpa + ab \\ &= d(dqp + qb + pa) + ab \end{aligned}$$

Suppose that (mn) *mod* $d = ab$. Then $mn = dr + ab$ such that $0 \le ab < d$. But this is not true as ab can be greater than or equal to d.

Counterexample: Let $m = 11$, $n = 5$, and $d = 3$. Then $a = 11$ *mod* $3 = 2$ and $b = 5$ *mod* $3 = 2$. Now mn *mod* $3 = 1 \neq 4 = ab$.

Part 2: *Theorem*: If m, n, a, b, and d are integers and $d > 0$, and m *mod* $d = a$ and n *mod* $d = b$, then mn *mod* $d = ab$ *mod* d.

Proof. Let m, n, a, b, and d be integers such that $d > 0$ and m *mod* $d = a$ and n *mod* $d = b$. Then $m = dq + a$ and $n = dp + b$ for some integers q and p such that $0 \le a < d$ and $0 \le b < d$. By the quotient remainder theorem $ab = sd + r$

for some integers r and s such that $0 \leq r < d$. Thus $ab\ mod\ d = r$.

$$\begin{aligned} mn &= (dq + a)(dp + b) \\ &= d^2qp + dqb + dpa + sd + r \\ &= d(dqp + qb + pa + s) + r \end{aligned}$$

It follows from closure under multiplication and addition that $dqp + qb + pa + s$ is an integer. Let that integer be t. Then $mn = dt + r$. It follows from the definition of r that $0 \leq r < d$. It now follows from the definition of *mod* that $mn\ mod\ d = r$. Since $r = ab\ mod\ d$, we can conclude that $mn\ mod\ d = ab\ mod\ d$. □

Problem 53

Prove that if m, d, and k are integers and $d > 0$, then $(m{+}dk)\ mod\ d = m\ mod\ d$.

Theorem: If m, d, and k are integers and $d > 0$, then $(m + dk)\ mod\ d = m\ mod\ d$.

Proof. Let m, d, and k be integers with $d > 0$. By the quotient remainder theorem $m + dk = dq + r$ for some integers q and r such that $0 \leq r < d$. It follows from the definition of *mod* that $(m + dk)\ mod\ d = r$.

$$\begin{aligned} m + dk &= dq + r \\ m &= dq - dk + r \\ &= d(q - k) + r \end{aligned}$$

It follows from closure under subtraction that $q - k$ is an integer. Let that integer be t. Then $m = dt + r$ with $0 \leq r < d$. It follows from the definition of *mod* that $m\ mod\ d = r$ but $r = (m + dk)\ mod\ d$. It follows from the transitive property of equality that $(m + dk)\ mod\ d = m\ mod\ d$. □