Section 2.2

Prove that the statements are true for every positive integer n.

Problem # 6

For every positive integer n, let P_n be the statement

$$1^3 + 2^3 + 3^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4} \tag{1}$$

Solution

Part 1

For $n = 1$

$$\begin{aligned} 1^3 &= \frac{1^2(1+1)^2}{4} \\ 1 &= \frac{4}{4} \\ 1 &= 1 \end{aligned} \tag{2}$$

Thus P_1 is true.

Part 2

Assume that P_k is true.

Part 3

For $n = k + 1$

$$\begin{aligned} 1^3 + 2^3 + 3^3 + \cdots + k^3 + (k+1)^3 &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= \frac{k^4 + 2k^3 + k^3}{4} + k^3 + 3k^2 + 3k + 1 \\ &= \frac{k^4 + 2k^3 + k^2}{4} + \frac{4k^3 + 12k^3 + 12k + 4}{4} \\ &= \frac{k^4 + 6k^3 + 13k^2 + 12k + 4}{4} \\ &= (k+1)^2\left(\frac{k^2 + 4k + 4}{4}\right) \\ &= (k+1)^2\left(\frac{(k+2)^2}{2^2}\right) \\ &= \left(\frac{(k+1)^2(k+2)}{2}\right)^2 \end{aligned} \tag{3}$$

This fraction matches exactly the fraction

$$\frac{n^2 (n+1)^2}{4}$$

when n is replaced by $k+1$. Thus P_{k+1} is true whenever P_k is true. It follows from the induction postulate that P_n is true for all positive integers n.

Problem # 7

For every positive integer n, let P_n be the statement

$$4 + 4^2 + 4^3 + \cdots + 4^n = \frac{4(4^n - 1)}{3} \tag{4}$$

Solution

Part 1

For $n = 1$

$$\begin{aligned} 4^1 &= \frac{4(4^1 - 1)}{3} \\ 4 &= \frac{12}{3} \\ &= 4 \end{aligned} \tag{5}$$

Thus P_1 is true.

Part 2

Assume that P_k is true.

Part 3

For $n = k+1$

$$\begin{aligned} 4 + 4^2 + 4^3 + \cdots + 4^k + 4^{k+1} &= \frac{4(4^n - 1)}{3} + 4^{k+1} \\ &= \left(\frac{4}{3}\right)(4^n - 1 + 3(4^n)) \\ &= \left(\frac{4}{3}\right)(4(4^n) - 1) \\ &= \left(\frac{4}{3}\right)\left(4^{n+1} - 1\right) \end{aligned} \tag{6}$$

This fraction matches exactly the fraction

$$\frac{4(4^n - 1)}{4} \tag{7}$$

when n is replaced by $k+1$. Thus P_{k+1} is true whenever P_k is true. It follows from the induction postulate that P_n is true for all positive integers n.

Problem # 8

For every positive integer n, let P_n be the statement

$$1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2\left(2n^2 - 1\right) \tag{8}$$

Solution

Part 1

For $n = 1$

$$\begin{aligned} 1^3 &= 1^2\left(2\left(1^2\right) - 1\right) \\ 1 &= 1\,(2-1) \\ &= 1 \end{aligned} \tag{9}$$

Thus P_1 is true.

Part 2

Assume that P_k is true.

Part 3

For $n = k + 1$

$$\begin{aligned} 1^3 + 3^3 + 5^3 + \cdots + (2k-1)^3 + (2\,(k+1)-1)^3 &= n^2\left(2n^2-1\right) + (2\,(k+1)-1)^3 \\ &= n^2\left(2n^2-1\right) + (2n+1)^3 \\ &= \left(2n^4 - n^2\right) + (2n+1)^3 \\ &= \left(2n^4 - n^2\right) + \left(8n^3 + 10n^2 + 6n + 1\right) \\ &= 2n^4 + 4n^3 - n^2 + 4n^3 + 8n^2 - 2n + 3n^2 + 4n + 1 \\ &= \left(n^2 + 2n + 1\right)\left(2n^2 + 4n - 1\right) \\ &= \left(n^2 + 2n + 1\right)\left(2\,(n+1)^2 - 1\right) \\ &= (n+1)^2\left(2\,(n+1)^2 - 1\right) \end{aligned} \tag{10}$$

This expression matches exactly the expression

$$n^2\left(2n^2 - 1\right) \tag{11}$$

when n is replaced by $k + 1$. Thus P_{k+1} is true whenever P_k is true. It follows from the induction postulate that P_n is true for all positive integers n.

Section 2.3

Problem # 2b

List all common divisors of 42 and 45.

Solution

1, 3

With a and b as given in problems 4 and 6, find the q and r that satisfy the conditions in the Division Algorithm.

Problem # 6

$a = 1205, b = 37$

Solution

$q = 32, r = 21$

Problem # 12

$a = 15, b = 512$

Solution

$q = -1, r = 507$

Problem # 19

Let a, b, c, m, and n be integers such that $a \mid b$ and $a \mid c$. Prove that $a \mid (mb + nc)$.

Solution

Because a divides b and a divides c there must exist $x, y \in \mathbb{Z}$ such that $ax = b$ and $ay = c$. Then

$$\begin{aligned} (mb + nc) &= (max + nay) \\ &= a\,(mx + ny) \end{aligned} \tag{12}$$

The properties of addition and multiplication of integers means that $(mx + ny)$ is an integer. Therefore a divides $(mb + nc)$.

Problem # 20

Let a, b, c, and n be integers such that $a \mid b$ and $a \mid c$. Prove that $ac \mid bd$.

Solution

Because a divides b and a divides c, there must exist $x, y \in \mathbb{Z}$ such that $ax = b$ and $cy = d$. So

$$\begin{aligned} bd &= (ax)(cy) \\ &= (ac)(xy) \end{aligned} \tag{13}$$

The product xy is an integer. Thus ac divides bd.

Problem # 21

Prove that if a and b are integers such that $a \mid b$ and $b \mid a$, then either $a = b$ or $a = -b$.

Solution

$a \mid b$ and $b \mid a$ so we know that there exist $x, y \in \mathbb{Z}$ such that $ax = b$ and $by = a$. Then

$$\begin{aligned} b &= \frac{a}{y} \\ ax &= \frac{a}{y} \\ x &= \frac{a}{ay} \\ x &= \frac{1}{y} \\ xy &= 1 \end{aligned} \tag{14}$$

x and y are either both 1 or both -1. Therefore for $ax = b$ either

$$x = 1, a(1) = b \implies a = b \tag{15}$$

or

$$x = -1, a(-1) = b \implies a = -b \tag{16}$$

Problem # 23

Let a and b be integers such that $a \mid b$ and $|b| < |a|$. Prove that $b = 0$.

Solution

It is clear that if $a \mid b$, then $|a| \mid |b|$. Changing the sign of the two divisors will only change the sign of the quotient. This means that there exists a $z \in \mathbb{Z}$ such that $z|a| = |b|$. Both $|a|$ and $|b|$ are positive and thus z must also be positive or zero.
As demonstrated by problem 18 from section 2.1, for integers $a > b$ and $z > 0$ then $za > zb$. So, in the case that z is positive

$$z|a| > z|b| > |b| \tag{17}$$

this contradicts the fact that we know $z|a| = |b|$. Thus z must equal 0 and $z|a| = |b| = 0$ so $b = 0$.

Problem # 25

Let a, b, and c be integers. Prove or disprove that $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Solution

Let $a = 100, b = 10$ and $c = 30$. Then $a \mid bc = 100 \mid 300$ is true but it is not true that $100 \mid 10$ or that $100 \mid 30$. The statement is thus disproved.

Problem # 28

Let a be an odd integer. Prove that $8 \mid (a^2 - 1)$.

Solution

$$n^2 - 1 = (n-1)(n+1) \tag{18}$$

n is odd so both $n-1$ and $n+1$ are even and thus divisible by 2. Given that $n+1 = (n-1)+2$ then either $(n-1)$ or $(n+1)$ must be divisible by 4. Assuming that $(n-1) \mid 4$ then there exists $x, y \in \mathbb{Z}$ such that $n-1 = 4x$ and $n+1 = 2y$. Therefore the product

$$\begin{aligned} (n-1)(n+1) &= (4x)(2y) \\ &= 8(xy) \end{aligned} \tag{19}$$

and is divisible by 8. It can be seen that due to the commutative property of multiplication that it is irrelevant which of $n-1$ and $n+1$ is divisible by 4 and which by 2.

Problem # 29

Let m be an arbitrary integer. Prove that there is no integer n such that $m < n < m+1$.

Solution

Assume there is some number n such that $m < n < m+1$. By substracting m from this relation we find $0 < n - m < 1$. There are no integers between 0 and 1 so $(n-m) \notin \mathbb{Z}$. We are told that $m \in \mathbb{Z}$ and therefore $n \notin \mathbb{Z}$.

Problem # 47

For all a and b in $\mathbb{Z}$, $a - b$ is a factor of $a^n - b^n$.

Solution

Part 1

For $n = 1$

$$\left(a^1 - b^1\right) = (a-b)(1) \tag{20}$$

so the statement is true for $n = 1$.

Part 2

Assume the statement is true for $n = k$. This means that there exists a $z \in \mathbb{Z}$ such that $z\,(a-b) = a^k - a^b$.

Part 3

Part 2 indicated that we can write $a^{k+1} = a[(a+b)\,z + b^k]$ and $-b^{k+1} = b[(a+b)\,z - a^k]$, thus

$$\begin{aligned} a^{k+1} - b^{k+1} &= a[(a+b)\,z + b^k] + b[(a+b)\,z - a^k] \\ &= (a+b)\left[(a+b)\,z + b^k + (a+b)\,z - a^k\right] \end{aligned} \tag{21}$$

The result of $[(a+b)\,z + b^k + (a+b)\,z - a^k]$ must be an integer which means that $(a+b)$ divides ${}^{k+1} - b^{k+1}$. It follows from the induction postulate that the same is true for all integers.

Problem # 48

For all a and b in $\mathbb{Z}$, $a+b$ is a factor of $a^{2n} - b^{2n}$.

Solution

Part1

For $n = 1$

$$a^{2n} + b^{2n} = a^2 + b^2 \tag{22}$$
$$= (a+b)\,(a-b) \tag{23}$$

so $(a+b)$ divides $a^{2n} + b^{2n}$ for $n = 1$.

Part 2

Assume the statement is true for $n = k$ so $(a+b)$ divides $a^{2k} + b^{2k}$.

Part 3

For $n = k+1$

$$\begin{aligned} a^{2n} + b^{2n} &= a^{2(k+1)} + b^{2(k+1)} \\ &= a^{2k+2} + b^{2k+2} \\ &= a^{2k}a^2 + b^{2k}b^2 \\ &= \left(a^2 + b^2\right)\left(a^{2k} + b^{2k}\right) \\ &= (a+b)\,(a-b)\left(a^{2k} + b^{2k}\right) \end{aligned} \tag{24}$$

Thus $(a+b)$ divides $a^{2(k+1)} + b^{2(k+1)}$. It follows from the induction hypothesis that $a+b$ is a factor of $a^{2n} + b^{2n}$ for all $a, b \in \mathbb{Z}$.

Problem # 49

(a) The binomial coefficients $\binom{n}{r}$ are defined in Exercise 25 of Section 2.2. Use induction on r to prove that if p is a prime integer, then p is a factor of $\binom{p}{r}$ for $r = 1, 2, \ldots, p-1$. (From Exercise 26 of Section 2.2, it is known that $\binom{p}{r}$ is an integer).

(b) Use induction on n to prove that if p is a prime integer, then p is a factor of $n^p - n$.

Solution

Part (a)

1. For $r = 1$, $\binom{p}{r} = \frac{p!}{(p-1)!(1)!} = p$. p divides p.
2. Assume that the statement is true for $n = k$. Therefore $p \mid \binom{p}{k}$.
3.

$$\begin{aligned}\binom{p}{k+1} &= \frac{p!}{(p-k-1)!\,(k+1)!} \\ &= \frac{p!}{(p-k-1)!\,(k+1)\,(k)!} \\ &= \frac{(p!)\,(p-k)}{(p-k)!\,(k+1)\,(k)!} \\ &= \left(\frac{p!}{(p-k)!}\right)\left(\frac{(p-k)}{(k+1)}\right) \\ &= \frac{p-k}{k+1}\binom{p}{k}\end{aligned} \tag{25}$$

So $(p-k)\binom{p}{k} = (k+1)\binom{p}{k+1}$. The left side of the equation is divisible by p because $p \mid \binom{p}{k}$ so there exists some $z \in \mathbb{Z}$ such that $zp = \binom{p}{k}$. Then

$$\begin{aligned}(p-k)\binom{p}{k} &= (p-k)\,(pz) \\ &= pzp - pzk \\ &= p\,(zp - zk)\end{aligned} \tag{26}$$

We know that either $p \mid \binom{p}{k+1}$ or $p \mid (k+1)$ by Euclid's Lemma. p cannot divide $(k+1)$ because it is given that $(k+1) < p$. Therefore $p \mid \binom{p}{k+1}$. It follows from the induction postulate that $p \mid \binom{p}{r}$ for $r = 1, 2, \ldots, p-1$.

Part (b)

1. For $n = 1, 1^p - 1 = 0$. p is a factor of 0 because $0 = (0)\,p$.
2. Assume p is a factor of $k^p - k$ for some number k.
3. $n = k + 1$

By the binomial theorem

$$(k+1)^p = k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1 \tag{27}$$

From part a we know that all binomials of the form $\binom{p}{r}$ for $r < p$ are divisible by p. Each of the middle terms are then divisible by p. Therefore

$$\begin{aligned}(k+1)^p - (k+1) &= \binom{p}{1}k^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + k^p + 1 - (k+1) \\ &= \binom{p}{1}k^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + (k^p - k)\end{aligned} \tag{28}$$

it is known that each of the terms of the addition on the right side of the equation is divisible by p, therefore the left side of the equation is also divisible by p. It follows from the induction postulate that p is a factor of $n^p - n$ for any prime integer p.

Section 2.4

Problem # 6

Show that $n^2 - n + 5$ is a prime integer when $n = 1, 2, 3, 4$ but that it is not true that $n^2 - n + 5$ is always a prime integer. Write out a similar set of statements for the polynomial $n^2 - n + 11$.

Solution

For $n^2 - n + 5$
$n = 1$

$$1^2 - 1 + 5 = 5 \text{ is prime} \tag{29}$$

$n = 2$

$$2^2 - 2 + 5 = 7 \text{ is prime} \tag{30}$$

$n = 3$

$$3^2 - 3 + 5 = 11 \text{ is prime} \tag{31}$$

$n = 4$

$$4^2 - 4 + 5 = 17 \text{ is prime} \tag{32}$$

But $n = 5$

$$5^2 - 5 + 5 = 25 \text{ is not prime} \tag{33}$$

A similar result can be shown for $n^2 - n + 11$
$n = 1$

$$1^2 - 1 + 11 = 11 \text{ is prime} \tag{34}$$

$n = 2$

$$2^2 - 2 + 11 = 13 \text{ is prime} \tag{35}$$

$n = 3$

$$3^2 - 3 + 11 = 17 \text{ is prime} \tag{36}$$

$n = 4$

$$4^2 - 4 + 11 = 23 \text{ is prime} \tag{37}$$

But $n = 11$

$$11^2 - 11 + 11 = 121 \text{ is not prime} \tag{38}$$

Problem # 20

Prove that $(ab, c) = 1$ if and only if $(a, c) = 1$ and $(b, c) = 1$.

Solution

Let $d = (ab, c) = 1$ and $x = (b, c)$. Assume that $x \neq 1$. From the definition of the gcd we know that x must then be some positive integer larger than 1.
If $x \mid b$ then there exists $z \in \mathbb{Z}$ such that $xz = b$. Multiplying each side by a gives $x(za) = (ab)$. Therefore x divides ab. By its definition $x \mid c$. Because d is the gcd of ab and c then x must also divide d. However, $d = 1$ and we have already shown that $x > 1$. It is impossible for x to divide d. We have reached a contradiction and x must equal 1. The same argument can be used to show that $y + (a, c)$ must also equal 1.

The above shows that

$$(ab, c) \implies (a, c) = 1 \text{ and } (b, c) = 1 \tag{39}$$

Assume that $(a, c) = 1$ and Each of $a, b,$ and c has a unique prime factorization. So let $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, $b = q_1^{f_1} q_2^{f_2} \cdots q_\ell^{f_\ell}$. The greatest common divisor between each of these numbers and c is 1. The product ab can then be written as $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} q_1^{f_1} q_2^{f_2} \cdots q_\ell^{f_\ell}$. Assume that this product has a common divisor x with c that is greater than 1. Then each of the prime factors of x is either a factor of a or a factor of b and must be contained somewhere in one of their prime factorizations. Because x is a divisor of c it must also be a product of some of the prime factors of c . Therefore there are factors of $x > 1$ that are also factors of c and either a or b. This contradicts the fact that c is relatively prime in regards to both a and b.

The above shows that

$$(a, c) = 1 \text{ and } (b, c) = 1 \implies (ab, c) \tag{40}$$

By combining the two relations established above we conclude that

$$(ab, c) \iff (a, c) = 1 \text{ and } (b, c) = 1 \tag{41}$$

Problem # 21

Let $(a, b) = 1$ and $(a, c) = 1$. Prove or disprove that $(ac, b) = 1$.

Solution

Let $a = 1$, $b = 3$, and $c = 3$. Then $(a, b) = (1, 3) = 1$, $(a, c) = (1, 3) = 1$, but $(ac, b) = (3, 3) = 3$. So $(ac, b) \neq 1$.

Problem # 25

Prove that if $m > 0$ and (a, b) exists, then $(ma, mb) = m \cdot (a, b)$.

Solution

Let $d = (a, b)$ and $x = (ma, mb)$. Then

$$\begin{aligned} x &= i_1\,(ma) + j_1\,(mb) \\ d &= i_2\,(a) + j_2\,(b) \end{aligned} \tag{42}$$

We want to show that $m\,(i_1 a + j_1 b) = m\,(i_2 a + j_2 b)$. Dividing by m this is equivalent to saying that $(i_1 a + j_1 b) = (i_2 a + j_2 b)$. The right side of the equation can't be larger because it is equal to d which is the least possible integer of that form. The left side can't be larger because that would imply that $x = m\,(i_1 a + j_1 b) > m\,(i_2 a + j_2 b)$. We know this is not the case because x is the smallest integer that can be written in that form. Therefore the two sides are equal and $(ma, mb) = m \cdot (a, b)$.