Math 3110 Lecture 4

Greg Oman

University of Colorado
Colorado Springs

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element. So all we have to do is show that there is some integer x such that $m - nx \geq 0$, that is, $nx \leq m$.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element. So all we have to do is show that there is some integer x such that $m - nx \geq 0$, that is, $nx \leq m$. But this is equivalent to the existence of an integer x such that $x \leq \frac{m}{n}$.

Division Algorithm

Let's begin by recalling the final result from the previous lecture:

Lemma

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. Then S has a least element.

Proof.

Let m, n, and S be as defined above. Note by definition that $S \subseteq \mathbb{N}$. So by (a slightly more general version of) the Well-Ordering Principle, as long as S is nonempty, then S has a least element. So all we have to do is show that there is some integer x such that $m - nx \geq 0$, that is, $nx \leq m$. But this is equivalent to the existence of an integer x such that $x \leq \frac{m}{n}$. For every real number r, there is an integer $x \leq r$, so this proves it. $\square$

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Theorem (Division Algorithm)

Let m be an integer and let n be a positive integer.

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Theorem (Division Algorithm)

Let m be an integer and let n be a positive integer. Then there are **unique** *integers q and r such that*

1. $m = nq + r$, *and*
2. $0 \leq r < n$.

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Theorem (Division Algorithm)

Let m be an integer and let n be a positive integer. Then there are **unique** *integers q and r such that*

1. $m = nq + r$, *and*
2. $0 \leq r < n$.

Proof.

Let m be an integer and let n be a positive integer.

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Theorem (Division Algorithm)

Let m be an integer and let n be a positive integer. Then there are **unique** *integers q and r such that*

1. $m = nq + r$, *and*
2. $0 \leq r < n$.

Proof.

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$.

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Theorem (Division Algorithm)

Let m be an integer and let n be a positive integer. Then there are **unique** *integers q and r such that*

1. $m = nq + r$, *and*
2. $0 \leq r < n$.

Proof.

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. By the previous lemma, S has a least element; call it r.

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Theorem (Division Algorithm)

Let m be an integer and let n be a positive integer. Then there are **unique** *integers q and r such that*

1. $m = nq + r$, *and*
2. $0 \leq r < n$.

Proof.

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. By the previous lemma, S has a least element; call it r. Since $r \in S$, by definition of S, we see that □

Division Algorithm

We are now ready to present the main result of this section (see section 2.2 of the text).

Theorem (Division Algorithm)

Let m be an integer and let n be a positive integer. Then there are **unique** *integers q and r such that*

1. $m = nq + r$, *and*
2. $0 \leq r < n$.

Proof.

Let m be an integer and let n be a positive integer. Now let $S = \{m - nx \colon x \in \mathbb{Z} \text{ and } m - nx \geq 0\}$. By the previous lemma, S has a least element; call it r. Since $r \in S$, by definition of S, we see that □

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

(b) $r = m - nq$ for some integer q, that is, $m = nq + r$.

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

(b) $r = m - nq$ for some integer q, that is, $m = nq + r$.

Next, we show that $r < n$.

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

(b) $r = m - nq$ for some integer q, that is, $m = nq + r$.

Next, we show that $r < n$. Suppose by way of contradiction that $r \geq n$.

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

(b) $r = m - nq$ for some integer q, that is, $m = nq + r$.

Next, we show that $r < n$. Suppose by way of contradiction that $r \geq n$. Then $r - n \geq 0$ and $r - n < r$.

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

(b) $r = m - nq$ for some integer q, that is, $m = nq + r$.

Next, we show that $r < n$. Suppose by way of contradiction that $r \geq n$. Then $r - n \geq 0$ and $r - n < r$. By (b), we have
$r - n = m - nq - n = m - n(q + 1) \in S$.

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

(b) $r = m - nq$ for some integer q, that is, $m = nq + r$.

Next, we show that $r < n$. Suppose by way of contradiction that $r \geq n$. Then $r - n \geq 0$ and $r - n < r$. By (b), we have
$r - n = m - nq - n = m - n(q+1) \in S$. But this contradicts that r is the *least* element of S.

Division Algorithm

Proof.

(a) $r \geq 0$, that is, $0 \leq r$, and

(b) $r = m - nq$ for some integer q, that is, $m = nq + r$.

Next, we show that $r < n$. Suppose by way of contradiction that $r \geq n$. Then $r - n \geq 0$ and $r - n < r$. By (b), we have $r - n = m - nq - n = m - n(q + 1) \in S$. But this contradicts that r is the *least* element of S. We have now shown that $m = nq + r$ and $0 \leq r < n$. □

Division Algorithm

Proof.

It remains to show that q and r are unique.

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,
3. $0 \leq r_1 < n$, and

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,
3. $0 \leq r_1 < n$, and
4. $0 \leq r_2 < n$.

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,
3. $0 \leq r_1 < n$, and
4. $0 \leq r_2 < n$.

for some integers q_1, q_2, r_1, and r_2.

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,
3. $0 \leq r_1 < n$, and
4. $0 \leq r_2 < n$.

for some integers q_1, q_2, r_1, and r_2. We will show that $q_1 = q_2$ and $r_1 = r_2$.

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,
3. $0 \leq r_1 < n$, and
4. $0 \leq r_2 < n$.

for some integers q_1, q_2, r_1, and r_2. We will show that $q_1 = q_2$ and $r_1 = r_2$.
Subtracting r_2 throughout 3., we get $-r_2 \leq r_1 - r_2 < n - r_2$.

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,
3. $0 \leq r_1 < n$, and
4. $0 \leq r_2 < n$.

for some integers q_1, q_2, r_1, and r_2. We will show that $q_1 = q_2$ and $r_1 = r_2$. Subtracting r_2 throughout 3., we get $-r_2 \leq r_1 - r_2 < n - r_2$. From 4., $-n < -r_2$, so we get

Division Algorithm

Proof.

It remains to show that q and r are unique. So suppose that we have

1. $m = nq_1 + r_1$,
2. $m = nq_2 + r_2$,
3. $0 \leq r_1 < n$, and
4. $0 \leq r_2 < n$.

for some integers q_1, q_2, r_1, and r_2. We will show that $q_1 = q_2$ and $r_1 = r_2$. Subtracting r_2 throughout 3., we get $-r_2 \leq r_1 - r_2 < n - r_2$. From 4., $-n < -r_2$, so we get □

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

From 1. and 2. on the previous slide, it follows that $nq_1 + r_1 = nq_2 + r_2$.

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

From 1. and 2. on the previous slide, it follows that $nq_1 + r_1 = nq_2 + r_2$. Hence $r_1 - r_2 = n(q_2 - q_1)$.

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

From 1. and 2. on the previous slide, it follows that $nq_1 + r_1 = nq_2 + r_2$. Hence $r_1 - r_2 = n(q_2 - q_1)$. Using the above inequality, we see that $-n < n(q_2 - q_1) < n$.

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

From 1. and 2. on the previous slide, it follows that $nq_1 + r_1 = nq_2 + r_2$. Hence $r_1 - r_2 = n(q_2 - q_1)$. Using the above inequality, we see that $-n < n(q_2 - q_1) < n$. Multiplying through by $\frac{1}{n}$, we get $-1 < q_2 - q_1 < 1$, and thus $q_2 - q_1 = 0$.

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

From 1. and 2. on the previous slide, it follows that $nq_1 + r_1 = nq_2 + r_2$. Hence $r_1 - r_2 = n(q_2 - q_1)$. Using the above inequality, we see that $-n < n(q_2 - q_1) < n$. Multiplying through by $\frac{1}{n}$, we get $-1 < q_2 - q_1 < 1$, and thus $q_2 - q_1 = 0$. This implies that $q_1 = q_2$, as desired.

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

From 1. and 2. on the previous slide, it follows that $nq_1 + r_1 = nq_2 + r_2$. Hence $r_1 - r_2 = n(q_2 - q_1)$. Using the above inequality, we see that $-n < n(q_2 - q_1) < n$. Multiplying through by $\frac{1}{n}$, we get $-1 < q_2 - q_1 < 1$, and thus $q_2 - q_1 = 0$. This implies that $q_1 = q_2$, as desired. Recall above that we have $r_1 - r_2 = n(q_2 - q_1) = n \cdot 0 = 0$, and so $r_1 = r_2$.

Division Algorithm

Proof.

$-n < -r_2 \leq r_1 - r_2 < n - r_2 \leq n$, and hence

$$-n < r_1 - r_2 < n.$$

From 1. and 2. on the previous slide, it follows that $nq_1 + r_1 = nq_2 + r_2$. Hence $r_1 - r_2 = n(q_2 - q_1)$. Using the above inequality, we see that $-n < n(q_2 - q_1) < n$. Multiplying through by $\frac{1}{n}$, we get $-1 < q_2 - q_1 < 1$, and thus $q_2 - q_1 = 0$. This implies that $q_1 = q_2$, as desired. Recall above that we have $r_1 - r_2 = n(q_2 - q_1) = n \cdot 0 = 0$, and so $r_1 = r_2$. The proof is now complete. □

Division Algorithm

Definition

Let m be an integer and let n be a positive integer.

Division Algorithm

Definition

Let m be an integer and let n be a positive integer. From the previous theorem (Division Algorithm), there are unique integers q and r such that $m = nq + r$ and $0 \leq r < n$.

Division Algorithm

Definition

Let m be an integer and let n be a positive integer. From the previous theorem (Division Algorithm), there are unique integers q and r such that $m = nq + r$ and $0 \leq r < n$. We call q the **quotient** and r the **remainder** upon dividing m by n.

Division Algorithm

Definition

Let m be an integer and let n be a positive integer. From the previous theorem (Division Algorithm), there are unique integers q and r such that $m = nq + r$ and $0 \leq r < n$. We call q the **quotient** and r the **remainder** upon dividing m by n.

We close this section with a couple of examples applying the Division Algorithm.

Division Algorithm

Definition

Let m be an integer and let n be a positive integer. From the previous theorem (Division Algorithm), there are unique integers q and r such that $m = nq + r$ and $0 \leq r < n$. We call q the **quotient** and r the **remainder** upon dividing m by n.

We close this section with a couple of examples applying the Division Algorithm.

Example

Every integer is either even or odd.

Division Algorithm

Definition

Let m be an integer and let n be a positive integer. From the previous theorem (Division Algorithm), there are unique integers q and r such that $m = nq + r$ and $0 \leq r < n$. We call q the **quotient** and r the **remainder** upon dividing m by n.

We close this section with a couple of examples applying the Division Algorithm.

Example

Every integer is either even or odd.

Division Algorithm

Proof.

Let m be an arbitrary integer.

Division Algorithm

Proof.

Let m be an arbitrary integer. Now divide m by 2; the Division Algorithm tells us that there are (unique) integers q and r such that $m = 2q + r$ and $0 \leq r < 2$.

Division Algorithm

Proof.

Let m be an arbitrary integer. Now divide m by 2; the Division Algorithm tells us that there are (unique) integers q and r such that $m = 2q + r$ and $0 \leq r < 2$. We now have two cases.

Division Algorithm

Proof.

Let m be an arbitrary integer. Now divide m by 2; the Division Algorithm tells us that there are (unique) integers q and r such that $m = 2q + r$ and $0 \leq r < 2$. We now have two cases.

Case 1: $r = 0$.

Division Algorithm

Proof.

Let m be an arbitrary integer. Now divide m by 2; the Division Algorithm tells us that there are (unique) integers q and r such that $m = 2q + r$ and $0 \leq r < 2$. We now have two cases.

Case 1: $r = 0$. Then $m = 2q$, and so m is even.

Division Algorithm

Proof.

Let m be an arbitrary integer. Now divide m by 2; the Division Algorithm tells us that there are (unique) integers q and r such that $m = 2q + r$ and $0 \leq r < 2$. We now have two cases.

Case 1: $r = 0$. Then $m = 2q$, and so m is even.

Case 2: $r = 1$.

Division Algorithm

Proof.

Let m be an arbitrary integer. Now divide m by 2; the Division Algorithm tells us that there are (unique) integers q and r such that $m = 2q + r$ and $0 \leq r < 2$. We now have two cases.

Case 1: $r = 0$. Then $m = 2q$, and so m is even.

Case 2: $r = 1$. Then $m = 2q + 1$, and m is odd. □

Division Algorithm

Proof.

Let m be an arbitrary integer. Now divide m by 2; the Division Algorithm tells us that there are (unique) integers q and r such that $m = 2q + r$ and $0 \leq r < 2$. We now have two cases.

Case 1: $r = 0$. Then $m = 2q$, and so m is even.

Case 2: $r = 1$. Then $m = 2q + 1$, and m is odd. □

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Case 1: $r = 0$.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Case 1: $r = 0$. Then $\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = \frac{27q^3+6q}{3} = 9q^3 + 2q$, which is an integer (since q is an integer).

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Case 1: $r = 0$. Then $\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = \frac{27q^3+6q}{3} = 9q^3 + 2q$, which is an integer (since q is an integer).

Case 2: $r = 1$.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Case 1: $r = 0$. Then $\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = \frac{27q^3+6q}{3} = 9q^3 + 2q$, which is an integer (since q is an integer).

Case 2: $r = 1$. Then
$\frac{a(a^2+2)}{3} = \frac{(3q+1)((3q+1)^2+2)}{3} = \frac{(3q+1)(9q^2+6q+3)}{3} = (3q+1)(3q^2+2q+1)$,
which is also an integer as above.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Case 1: $r = 0$. Then $\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = \frac{27q^3+6q}{3} = 9q^3 + 2q$, which is an integer (since q is an integer).

Case 2: $r = 1$. Then
$\frac{a(a^2+2)}{3} = \frac{(3q+1)((3q+1)^2+2)}{3} = \frac{(3q+1)(9q^2+6q+3)}{3} = (3q+1)(3q^2+2q+1)$,
which is also an integer as above.

Case 3: $r = 2$.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Case 1: $r = 0$. Then $\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = \frac{27q^3+6q}{3} = 9q^3 + 2q$, which is an integer (since q is an integer).

Case 2: $r = 1$. Then $\frac{a(a^2+2)}{3} = \frac{(3q+1)((3q+1)^2+2)}{3} = \frac{(3q+1)(9q^2+6q+3)}{3} = (3q+1)(3q^2+2q+1)$, which is also an integer as above.

Case 3: $r = 2$. Then $\frac{a(a^2+2)}{3} = \frac{(3q+2)((3q+2)^2+2)}{3} = \frac{(3q+2)(9q^2+12q+6)}{3} = (3q+2)(3q^2+4q+2)$, which is also an integer.

Division Algorithm

Example

Prove that for every integer a, $\frac{a(a^2+2)}{3}$ is an integer.

Proof.

Let a be an integer. Now divide a by 3 using the Division Algorithm to get $a = 3q + r$ for some integers q and r with $0 \leq r < 3$. Then $r = 0$, $r = 1$, or $r = 2$. We consider these cases separately.

Case 1: $r = 0$. Then $\frac{a(a^2+2)}{3} = \frac{3q((3q)^2+2)}{3} = \frac{27q^3+6q}{3} = 9q^3 + 2q$, which is an integer (since q is an integer).

Case 2: $r = 1$. Then
$\frac{a(a^2+2)}{3} = \frac{(3q+1)((3q+1)^2+2)}{3} = \frac{(3q+1)(9q^2+6q+3)}{3} = (3q+1)(3q^2+2q+1)$,
which is also an integer as above.

Case 3: $r = 2$. Then
$\frac{a(a^2+2)}{3} = \frac{(3q+2)((3q+2)^2+2)}{3} = \frac{(3q+2)(9q^2+12q+6)}{3} = (3q+2)(3q^2+4q+2)$,
which is also an integer. □