Chapter 6. Integer properties

6.1 The Division Algorithm

6.2 Modular arithmetic

6.1 The Division Algorithm

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory.

6.1 The Division Algorithm

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory.

[Def. 1]
If a and b are integers, with $a \neq 0$, we say that a divides b if there is an integer c such that $b = c \cdot a$ (i.e. no remainder in division $b \div a$)

6.1 The Division Algorithm

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory.

[Def. 1]
If a and b are integers, with $a \neq 0$, we say that a divides b if there is an integer c such that $b = c \cdot a$ (i.e. no remainder in division $b \div a$)

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

a is called a factor of b,
b is called a multiple of a

denotation: $a \mid b$ "a divides b"
$a \nmid b$ "a doesn't divide b"

6.1 The Division Algorithm

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory.

[Def. 1]
If a and b are integers, with $a \neq 0$, we say that a divides b if there is an integer c such that $b = c \cdot a$ (i.e. no remainder in division $b \div a$)

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

a is called a factor of b,
b is called a multiple of a

denotation: $a \mid b$ "a divides b"
$a \nmid b$ "a doesn't divide b"

if we use Predicate Logic: $\exists c\,(a \cdot c = b)$, with domain: all integers

6.1 The Division Algorithm

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory.

[Def. 1]
If a and b are integers, with $a \neq 0$, we say that a divides b if there is an integer c such that $b = c \cdot a$ (i.e. no remainder in division $b \div a$)

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

a is called a factor of b,
b is called a multiple of a

denotation: $a \mid b$ "a divides b"
$a \nmid b$ "a doesn't divide b"

Example 1:
Determine whether $7 \mid 24$, and $7 \mid 168$

6.1 The Division Algorithm

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory.

[Def. 1]
If a and b are integers, with $a \neq 0$, we say that a divides b if there is an integer c such that $b = c \cdot a$ (i.e. no remainder in division $b \div a$)

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

a is called a factor of b,
b is called a multiple of a

denotation: $a \mid b$ "a divides b"
$a \nmid b$ "a doesn't divide b"

Example 1:
Determine whether $7 \mid 24$, and $7 \mid 168$

Solution:
$7 \nmid 24$ *because* $24 \div 7 \approx 3.43$ – *not an integer*

6.1 The Division Algorithm

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called number theory.

[Def. 1]
If a and b are integers, with $a \neq 0$, we say that a divides b if there is an integer c such that $b = c \cdot a$ (i.e. no remainder in division $b \div a$)

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

a is called a factor of b,
b is called a multiple of a

denotation: $a \mid b$ "a divides b"
$a \nmid b$ "a doesn't divide b"

Example 1:
Determine whether $7 \mid 24$, and $7 \mid 168$

Solution:
$7 \nmid 24$ *because* $24 \div 7 \approx 3.43$ – *not an integer*

$7 \mid 168$ *because* $168 \div 7 = 24$, $c = 24$
– there is an integer such that $7 \cdot 24 = 168$

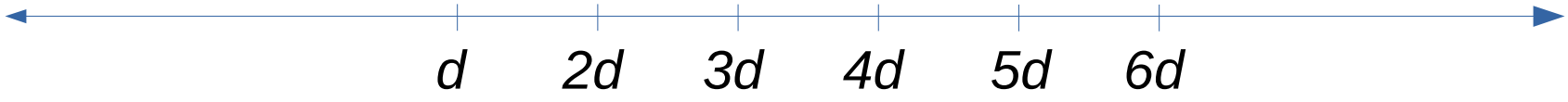
Example 2:
Let *n* and *d* be positive integers. How many positive integers not exceeding *n* are divisible by *d*?

Example 2:
Let *n* and *d* be positive integers. How many positive integers not exceeding *n* are divisible by *d*?

Solution:
The positive integers divisible by *d* are multiples of *d*, i.e. have form *dk*, where *k* is a positive integer.

Example 2:
Let *n* and *d* be positive integers. How many positive integers not exceeding *n* are divisible by *d*?

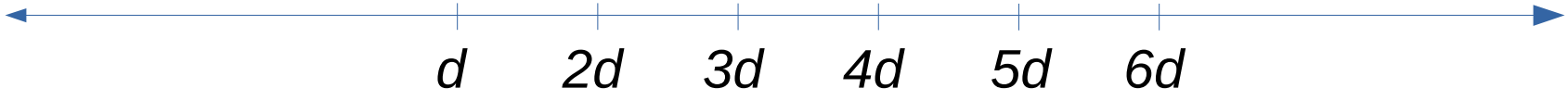
Solution:
The positive integers divisible by *d* are multiples of *d*, i.e. have form *dk*, where *k* is a positive integer.



$dk \leq n$

Example 2:
Let *n* and *d* be positive integers. How many positive integers not exceeding *n* are divisible by *d*?

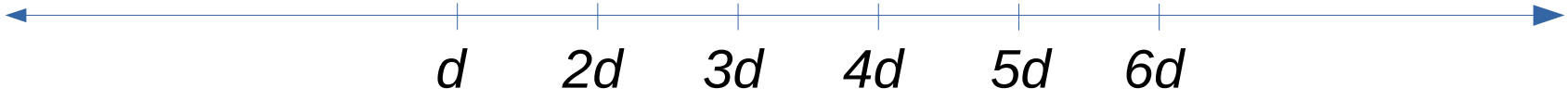
Solution:
The positive integers divisible by *d* are multiples of *d*, i.e. have form *dk*, where *k* is a positive integer.



$dk \leq n$ or $k \leq \frac{n}{d}$

Example 2:
Let *n* and *d* be positive integers. How many positive integers not exceeding *n* are divisible by *d*?

Solution:
The positive integers divisible by *d* are multiples of *d*, i.e. have form *dk*, where *k* is a positive integer.



$dk \le n$ or $k \le \frac{n}{d}$ and finally $k = \left\lfloor \frac{n}{d} \right\rfloor$ ← that many

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

Examples:
(1) $2 \mid 4$, $2 \mid 8$, then $2 \mid (4+8)$ i.e. $2 \mid 12$
(2) $2 \mid 4$, then $2 \mid 4*2$, $2 \mid 4*3$, $2 \mid 4*4$, …
(3) $2 \mid 4$, $4 \mid 8$, then $2 \mid 8$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

$2 \mid 4$, $2 \mid 8$, then $2 \mid (4+8)$ i.e. $2 \mid 12$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

$2 \mid 4$, $2 \mid 8$, then $2 \mid (4+8)$ i.e. $2 \mid 12$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

$2 \mid 4$, $2 \mid 8$, then $2 \mid (4+8)$ i.e. $2 \mid 12$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

$2 \mid 4$, $2 \mid 8$, then $2 \mid (4+8)$ i.e. $2 \mid 12$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k$ ($c = a \cdot k$)
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

$2 \mid 4$, $4 \mid 8$, then $2 \mid 8$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

$2 \mid 4$, $4 \mid 8$, then $2 \mid 8$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$,

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

$2 \mid 4$, $4 \mid 8$, then $2 \mid 8$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$, Therefore $a \mid c$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$, Therefore $a \mid c$

(2) left as homework suggested practice

qed

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$, Therefore $a \mid c$

(2) left as homework assignment

qed

[Corollary]
If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m and n.

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$, Therefore $a \mid c$

(2) left as homework assignment

qed

[Corollary]
If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m and n.

Example: $3 \mid 6$ and $3 \mid 9$, then $3 \mid (2 \cdot 6 + 4 \cdot 9)$ or $3 \mid 48$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$, Therefore $a \mid c$

(2) left as homework assignment

qed

[Corollary]
If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m and n.

Proof: if $a \mid b$, then by (2) from Theorem 1, $a \mid mb$

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$, Therefore $a \mid c$

(2) left as homework assignment

qed

[Corollary]
If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m and n.

Proof: if $a \mid b$, then by (2) from Theorem 1, $a \mid mb$
if $a \mid c$, then by (2) from Theorem 1, $a \mid nc$

6.1 The Division Algorithm

[Theorem 1] *Basic properties of divisibility*
Let a, b, and c be integers. Then
(1) if $a \mid b$ and $a \mid c$, then $a \mid (b+c)$
(2) if $a \mid b$, then $a \mid bc$, for all integers c
(3) if $a \mid b$ and $b \mid c$, then $a \mid c$

Proof:
(1) If $a \mid b$ then there exists an integer s such that $b = a \cdot s$,
if $a \mid c$ then $\exists k\ (c = a \cdot k)$
Then $b + c = as + ak = a(s+k)$, therefore $a \mid (b+c)$

(3) If $a \mid b$ and $b \mid c$, then $\exists s\ (b = a \cdot s)$, and $\exists k\ (c = b \cdot k)$
So, $c = b \cdot k = a \cdot s \cdot k$, Therefore $a \mid c$

(2) left as homework assignment

qed

[Corollary]
If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m and n.

Proof: if $a \mid b$, then by (2) from Theorem 1, $a \mid mb$
if $a \mid c$, then by (2) from Theorem 1, $a \mid nc$
Therefore, $a \mid (mb + nc)$, by (1) from Theorem 1

6.1 The Division Algorithm

[Theorem 2] *The Division Algorithm*
Let a be an integer, and d be a positive integers. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

6.1 The Division Algorithm

[Theorem 2] *The Division Algorithm*
Let a be an integer, and d be a positive integers. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$

notation:
$q = a$ **div** d
$r = a$ **mod** d

6.1 The Division Algorithm

[Theorem 2] *The Division Algorithm*
Let a be an integer, and d be a positive integers. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$

dividend *divisor* *quotient* *remainder*

```
  q R r
d ) a
  .....
```

or

```
a | d
..| q R r
```

notation:
$q = a$ **div** d
$r = a$ **mod** d

```
   19
7 ) 134
  - 7
    64
  - 63
     1
```

6.1 The Division Algorithm

[Theorem 2] *The Division Algorithm*
Let a be an integer, and d be a positive integers. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$

dividend *divisor* *quotient* *remainder*

```
  q R r
d ) a          or    a | d
   .....             ...|q R r
```

notation:
$q = a$ **div** d
$r = a$ **mod** d

Example 3:
$134 \div 7 = 19$ **R** 1

a (dividend) *d (divisor)* *q (quotient)* *r (remainder)*

```
   19
7 ) 134
  - 7
    64
  - 63
     1
```

6.1 The Division Algorithm

[Theorem 2] *The Division Algorithm*
Let a be an integer, and d be a positive integers. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$

dividend *divisor* *quotient* *remainder*

```
  q R r
d ) a          or    a | d
  .....              ...|q R r
```

notation:
$q = a$ **div** d
$r = a$ **mod** d

Example 3: $a = d \cdot q + r$

$134 \div 7 = 19$ **R** 1 or $134 = 7 \cdot 19 + 1$

a (dividend) *d (divisor)* *q (quotient)* *r (remainder)*

```
   19
7 ) 134
  - 7
    64
  - 63
     1
```

As you probably noticed, Theorem 2 is not actually an algorithm, but it is its traditional name, so we'll use it.

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution: 113 ÷ 11
$q = 113 \textbf{ div } 11 = 10$ – quotient

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution: 113 ÷ 11
q = *113* **div** *11 = 10* – quotient
r = *113* **mod** *11 = 3* – remainder

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution: 113 ÷ 11
$q = 113 \textbf{ div } 11 = 10$ – quotient
$r = 113 \textbf{ mod } 11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution: 113 ÷ 11
$q = 113 \textbf{ div } 11 = 10$ – quotient
$r = 113 \textbf{ mod } 11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution: 113 ÷ 11
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: -17 ÷ 4
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution:
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: -17 ÷ 4
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

$q = -17$ **div** $4 = -4$ – quotient
r = -17 **mod** $4 = 1$ or -1 ?

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution:
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: $-17 \div 4$
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

$q = -17$ **div** $4 = -4$ – quotient
$r = -17$ **mod** $4 = 1$ or -1 ?

Let's check: $-17 = 4 \cdot (-4) + 1 = -16 + 1 = -15$

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution:
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: $-17 \div 4$
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

$q = -17$ **div** $4 = -4$ – quotient - take one less: $q = -5$, therefore $4 \cdot -5 = -20$
$r = -17$ **mod** $4 = 1$ or -1 ?

Let's check: $-17 = 4 \cdot (-4) + 1 = -16 + 1 = -15$

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution:
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: $-17 \div 4$
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

$q = -17$ **div** $4 = -4$ – quotient - take one less: $q = -5$, therefore $4 \cdot -5 = -20$
$r = -17$ **mod** $4 = 1$ or -1 ? – remainder $r = -17 - (-20) = 3$

Let's check: $-17 = 4 \cdot (-4) + 1 = -16 + 1 = -15$

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution:
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: $-17 \div 4$
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

$q = -17$ **div** $4 = -4$ – quotient - take one less: $q = -5$, therefore $4 \cdot -5 = -20$
$r = -17$ **mod** $4 = 1$ or -1 ? – remainder $r = -17 - (-20) = 3$

Let's check: $-17 = 4 \cdot (-4) + 1 = -16 + 1 = -15$
re-do the check: $-17 = 4 \cdot (-5) + 3$

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution:
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: $-17 \div 4$
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

$q = -17$ **div** $4 = -4$ – quotient - take one less: $q = -5$, therefore $4 \cdot -5 = -20$
$r = -17$ **mod** $4 = 1$ or -1 ? – remainder $r = -17 - (-20) = 3$

Let's check: $-17 = 4 \cdot (-4) + 1 = -16 + 1 = -15$
re-do the check: $-17 = 4 \cdot (-5) + 3 = -20 + 3 = -17$

Example 4:
What are the quotient and remainder when *113* is divided by *11*?

Solution:
$q = 113$ **div** $11 = 10$ – quotient
$r = 113$ **mod** $11 = 3$ – remainder

Let's check: $113 = 11 \cdot 10 + 3 = 110 + 3 = 113$

Example 5:
What are the quotient and remainder when *-17* is divided by *4*?

Solution: $-17 \div 4$
divisor *d* is a positive integer, therefore quotient *q* will carry the sign, also remainder *r* is a positive integer, $0 \leq r < d$

$q = -17$ **div** $4 = -4$ – quotient - take one less: $q = -5$, therefore $4 \cdot -5 = -20$
$r = -17$ **mod** $4 = 1$ or -1 ? – remainder $r = -17 - (-20) = 3$

Let's check: $-17 = 4 \cdot (-4) + 1 = -16 + 1 = -15$
re-do the check: $-17 = 4 \cdot (-5) + 3 = -20 + 3 = -17$

Answer: q = -5, r = 3

Recall $q = a$ ***div*** d, q is a quotient
$r = a$ ***mod*** d, r is a remainder

6.2 Modular arithmetic

Recall $q = a \textbf{ div } d$, q is a quotient
$r = a \textbf{ mod } d$, r is a remainder

Karl Friedrich Gauss developed the concept of congruence (in 18th century). The notion of congruence played an important role in development of number theory

[Def. 1]
Let a,b be integers, and m be a positive integer. a is congruent to b modulo m, if $m \mid (a-b)$

6.2 Modular arithmetic

Recall $q = a$ ***div*** d, q is a quotient
$r = a$ ***mod*** d, r is a remainder

Karl Friedrich Gauss developed the concept of congruence (in 18th century). The notion of congruence played an important role in development of number theory

[Def. 1]
Let a,b be integers, and m be a positive integer. a is congruent to b modulo m, if $m \mid (a-b)$

Notation: $a \equiv b \pmod{m}$ " a is congruent to b modulo m "
$a \not\equiv b \pmod{m}$ " a is not congruent to b modulo m "

6.2 Modular arithmetic

Recall $q = a$ ***div*** d, q is a quotient
$r = a$ ***mod*** d, r is a remainder

Karl Friedrich Gauss developed the concept of congruence (in 18th century). The notion of congruence played an important role in development of number theory

[Def. 1]
Let a,b be integers, and m be a positive integer. a is congruent to b modulo m, if $m \mid (a-b)$

Notation: $a \equiv b \pmod{m}$ " a is congruent to b modulo m "
$a \not\equiv b \pmod{m}$ " a is not congruent to b modulo m "

- we use the notation of congruency to indicate that two numbers have the same remainders when divided by m.

6.2 Modular arithmetic

Recall $q = a$ ***div*** d, q is a quotient
$r = a$ ***mod*** d, r is a remainder

Karl Friedrich Gauss developed the concept of congruence (in 18th century). The notion of congruence played an important role in development of number theory

[Def. 1]
Let a,b be integers, and m be a positive integer. a is congruent to b modulo m, if $m \mid (a-b)$

Notation: $a \equiv b \pmod{m}$ " a is congruent to b modulo m "
$a \not\equiv b \pmod{m}$ " a is not congruent to b modulo m "

- we use the notation of congruency to indicate that two numbers have the same remainders when divided by m.

Example 1:
Let $a = 25$, $b = 19$, and $m = 3$.

6.2 Modular arithmetic

Recall $q = a$ ***div*** d, q is a quotient
$r = a$ ***mod*** d, r is a remainder

Karl Friedrich Gauss developed the concept of congruence (in 18th century). The notion of congruence played an important role in development of number theory

[Def. 1]
Let *a,b* be integers, and *m* be a positive integer. *a* is congruent to *b* modulo *m*, if *m* | *(a-b)*

Notation: $a \equiv b$ (**mod** *m*) " *a* is congruent to *b* modulo *m* "
$a \not\equiv b$ (**mod** *m*) " *a* is not congruent to *b* modulo *m* "

- we use the notation of congruency to indicate that two numbers have the same remainders when divided by *m*.

Example 1:
Let $a = 25$, $b = 19$, and $m = 3$.

25 is congruent to *19* modulo *3*, because *3* | *(25-19)*, i.e. *3* | *6*
Note that *25* ***mod*** *3* = *1*, and *19* ***mod*** *3* = *1*

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Recall the example 1's note: $25 \bmod 3 = 1$, and $19 \bmod 3 = 1$

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Proof:
1) Let's prove $\Rightarrow$: proof will be here

[Theorem 3]
Let a,b be integers, and m be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Proof:
1) Let's prove $\Rightarrow$: proof will be here

2) Let's prove $\Leftarrow$: assume that $a \bmod m = b \bmod m = r$, $r > 0$,
then $\exists$q,s – intgers ($a = mq + r$ and $b = ms + r$).

From there, $a-b = mq + r - (ms + r) = mq + r - ms - r = mq - ms = m(q-s)$
Therefore m | (a-b).

qed

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 2:
Determine whether *17* is congruent to *24* modulo *7* and whether *24* and *14* are congruent modulo *6*.

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 2:
Determine whether *17* is congruent to *24* modulo *7* and whether *24* and *14* are congruent modulo *6*.

Solution:
The questions posed: $17 \equiv 24 \pmod{7}$?
$7 \equiv 24 \pmod{6}$?

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 2:
Determine whether *17* is congruent to *24* modulo *7* and whether *24* and *14* are congruent modulo *6*.

Solution:
The questions posed: $17 \equiv 24 \pmod{7}$? Yes
$7 \equiv 24 \pmod{6}$?

1) $17 \bmod 7 = 3$, and $24 \bmod 7 = 3$, therefore $17 \equiv 24 \pmod{7}$.

[Theorem 3]
Let a,b be integers, and m be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 2:
Determine whether 17 is congruent to 24 modulo 7 and whether 24 and 14 are congruent modulo 6.

Solution:
The questions posed: $17 \equiv 24 \pmod{7}$? Yes
$7 \equiv 24 \pmod{6}$?

1) $17 \bmod 7 = 3$, and $24 \bmod 7 = 3$, therefore $17 \equiv 24 \pmod{7}$.

2) $24 \bmod 6 = 0$, and $14 \bmod 6 = 2$,

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 2:
Determine whether *17* is congruent to *24* modulo *7* and whether *24* and *14* are congruent modulo *6*.

Solution:
The questions posed: $17 \equiv 24 \pmod{7}$? Yes
$7 \equiv 24 \pmod{6}$? No

1) $17 \bmod 7 = 3$, and $24 \bmod 7 = 3$, therefore $17 \equiv 24 \pmod{7}$.

2) $24 \bmod 6 = 0$, and $14 \bmod 6 = 2$, therefore $7 \not\equiv 24 \pmod{6}$.

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$
therefore we are looking for something which is a multiple of 5, +3

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$
therefore we are looking for something which is a multiple of 5, +3

$x: 2 \cdot 5 + 3 = 13$,

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$
therefore we are looking for something which is a multiple of 5, +3

x: 2·5+3 = 13, 4·5+3 = 23,

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$
therefore we are looking for something which is a multiple of 5, +3

x: 2·5+3 = 13, 4·5+3 = 23, 1·5 + 3 = 8

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$
therefore we are looking for something which is a multiple of 5, +3

$x: 2 \cdot 5+3 = 13$, $4 \cdot 5+3 = 23$, $1 \cdot 5 + 3 = 8$
how about negative ones? - don't forget that we need to be carefull

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$
therefore we are looking for something which is a multiple of 5, +3

x: 2·5+3 = 13, 4·5+3 = 23, 1·5 + 3 = 8
how about negative ones? - don't forget that we need to be carefull
(-2) · 5 + 3 = -7 *check: -7 = (-2) · 5 + 3 True*

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

Example 3:
List three integers that are congruent to *3* modulo *5*.

Solution:
$x \equiv 3 \pmod{5}$ or $x \bmod 5 = 3 \bmod 5$;
$3 \bmod 5 = 3$, therefore $x \bmod 5 = 3$
therefore we are looking for something which is a multiple of 5, +3

$x: 2 \cdot 5+3 = 13$, $4 \cdot 5+3 = 23$, $1 \cdot 5 + 3 = 8$
how about negative ones? - don't forget that we need to be carefull
$(-2) \cdot 5 + 3 = -7$ check: $-7 = (-2) \cdot 5 + 3$ True
Answer: {13, 23, 8, -7}

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

[Theorem 4]
Let *m* be a positive integer ($m \in \mathbf{Z}^+$), $a \equiv b \pmod{m}$ iff $\exists k \in \mathbf{Z}\ (a = b+km)$

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

[Theorem 4]
Let *m* be a positive integer ($m \in \mathbf{Z}^+$), $a \equiv b \pmod{m}$ iff $\exists k \in \mathbf{Z}\ (a = b+km)$

Example: assume that $13 = 1 + 3 \cdot 4$, then $13 \equiv 1 \pmod{4}$

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

[Theorem 4]
Let *m* be a positive integer ($m \in \mathbf{Z}^+$), $a \equiv b \pmod{m}$ iff $\exists k \in \mathbf{Z}\ (a = b+km)$

Proof: let $a \equiv b \pmod{m}$,

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

[Theorem 4]
Let *m* be a positive integer ($m \in \mathbf{Z}^+$), $a \equiv b \pmod{m}$ iff $\exists k \in \mathbf{Z}\ (a = b+km)$

Proof: let $a \equiv b \pmod{m}$, then by **def. 1** $m \mid (a-b)$.

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

[Theorem 4]
Let *m* be a positive integer ($m \in \mathbf{Z}^+$), $a \equiv b \pmod{m}$ iff $\exists k \in \mathbf{Z}\ (a = b+km)$

Proof: let $a \equiv b \pmod{m}$, then by **def. 1** $m \mid (a-b)$.
If $m \mid (a-b)$ then by **def.** of divisibility $\exists k \in \mathbf{Z}\ (a-b = k \cdot m)$

[Theorem 3]
Let *a,b* be integers, and *m* be a positive integer. Then $a \equiv b \pmod{m}$ iff (if and only if) $a \bmod m = b \bmod m$.

[Theorem 4]
Let *m* be a positive integer ($m \in \mathbf{Z}^+$), $a \equiv b \pmod{m}$ iff $\exists k \in \mathbf{Z}\ (a = b+km)$

Proof: let $a \equiv b \pmod{m}$, then by **def. 1** $m \mid (a-b)$.
If $m \mid (a-b)$ then by **def.** of divisibility $\exists k \in \mathbf{Z}\ (a-b = k \cdot m)$, or
$\exists k \in \mathbf{Z}\ (a = km + b)$

qed

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Examples:
$5 \equiv 1 \pmod 4$ and $3 = 11 \pmod 4$, then

$5+3 \equiv 1+11 \pmod 4$, i.e. $8 \equiv 12 \pmod 4$

and

$5 \cdot 3 \equiv 1 \cdot 11 \pmod 4$, i.e. $15 \equiv 11 \pmod 4$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$ or $(a + c) = (b+d)+m(k+s)$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$ or $(a + c) = (b+d)+m(k+s)$
therefore by **Theorem 4**, $a + c \equiv b + d \pmod{m}$, with integer $k' = (k+s)$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$ or $(a + c) = (b+d)+m(k+s)$
therefore by **Theorem 4**, $a + c \equiv b + d \pmod{m}$, with integer $k' = (k+s)$

$ac = (b+km)\ (d+sm) =$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$ or $(a + c) = (b+d)+m(k+s)$
therefore by **Theorem 4**, $a + c \equiv b + d \pmod{m}$, with integer $k' = (k+s)$

$ac = (b+km)\,(d+sm) = bd + bsm + kdm + ksm^2 = bd + m(bs + kd + ksm)$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$ or $(a + c) = (b+d)+m(k+s)$
therefore by **Theorem 4**, $a + c \equiv b + d \pmod{m}$, with integer $k' = (k+s)$

$ac = (b+km)\,(d+sm) = bd + bsm + kdm + ksm^2 = bd + m(bs + kd + ksm)$
therefore by **Theorem 4**, $ac \equiv bd \pmod{m}$

qed

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$ or $(a + c) = (b+d)+m(k+s)$
therefore by **Theorem 4**, $a + c \equiv b + d \pmod{m}$, with integer $k' = (k+s)$

$ac = (b+km)\,(d+sm) = bd + bsm + kdm + ksm^2 = bd + m(bs + kd + ksm)$
therefore by **Theorem 4**, $ac \equiv bd \pmod{m}$

qed

[Corollary]
Let $m \in \mathbf{Z}^+$, and $a,b \in \mathbf{Z}$. Then
$(a+b) \bmod m = ((a \bmod m)+(b \bmod m)) \bmod m$
$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

[Theorem 5]
Let $m \in \mathbf{Z}^+$. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then
$a + c \equiv b + d \pmod{m}$, and
$ac \equiv bd \pmod{m}$

Proof: let $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$
then $\exists k \in \mathbf{Z}\ (a = b+km)$ and $\exists s \in \mathbf{Z}\ (c = d+sm)$

$a + c = b+d+km+sm$ or $(a + c) = (b+d)+m(k+s)$
therefore by **Theorem 4**, $a + c \equiv b + d \pmod{m}$, with integer $k' = (k+s)$

$ac = (b+km)\ (d+sm) = bd + bsm + kdm + ksm^2 = bd + m(bs + kd + ksm)$
therefore by **Theorem 4**, $ac \equiv bd \pmod{m}$
qed

[Corollary]
Let $m \in \mathbf{Z}^+$, and $a,b \in \mathbf{Z}$. Then
$(a+b) \bmod m = ((a \bmod m)+(b \bmod m)) \bmod m$
$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

Proof: not presented here

6.2 Modular arithmetic

Theorem 5 and its **corollary** are very useful in computing arithmetic expressions **mod** *n*

Example: to compute 15^{120} **mod** *68*

we would do 15^{120} first, and then take the result **mod** *68*.

-use the calculator to calculate it

15^{120} is a very large number,
multiplying large numbers is less efficient than multiplying small numbers

6.2 Modular arithmetic

Theorem 5 and its **corollary** are very useful in computing arithmetic expressions **mod** *n*

Example: to compute 15^{120} **mod** *68*

we would do 15^{120} first, and then take the result **mod** *68*.

-use the calculator to calculate it

<u>another approach</u>:

$15^{120} = \underbrace{15 \cdot 15 \cdot \ldots \cdot 15}_{120 \quad 15s}$

It is meaningless to do
((15 **mod** 68)(15 **mod** 68) … (15 **mod** 68))**mod** 68

[Theorem 5]
Let $m \in \mathbf{Z}^+$, and $a,b \in \mathbf{Z}$.
If $a \equiv b$ (***mod*** m) and
$c \equiv d$ (***mod*** m) then
$a + c \equiv b + d$ (***mod*** m), and
$ac \equiv bd$ (***mod*** m)
[Corollary]
$(a+b)$ ***mod*** $m = ((a$ ***mod*** $m)+(b$ ***mod*** $m))$ ***mod*** m
ab ***mod*** $m = ((a$ ***mod*** $m)(b$ ***mod*** $m))$ ***mod*** m

6.2 Modular arithmetic

Theorem 5 and its **corollary** are very useful in computing arithmetic expressions **mod** *n*

Example: to compute 15^{120} **mod** *68*

we would do 15^{120} first, and then take the result **mod** *68*.

-use the calculator to calculate it

<u>another approach</u>:

$15^{120} = \underbrace{15 \cdot 15 \cdot \ldots \cdot 15}_{120 \quad 15s}$

[Theorem 5]
Let $m \in \mathbf{Z}^+$, and $a,b \in \mathbf{Z}$.
If $a \equiv b$ (***mod*** m) and
$c \equiv d$ (***mod*** m) then
$a + c \equiv b + d$ (***mod*** m), and
$ac \equiv bd$ (***mod*** m)
[Corollary]
$(a+b)$ ***mod*** $m = ((a$ ***mod*** $m)+(b$ ***mod*** $m))$ ***mod*** m
ab ***mod*** $m = ((a$ ***mod*** $m)(b$ ***mod*** $m))$ ***mod*** m

It is meaningless to do
((15 **mod** 68)(15 **mod** 68) … (15 **mod** 68))**mod** 68

Instead do
p = (15 · 15) mod 68
p = (p · 15) mod 68 and so forth … 119 times

6.2 Modular arithmetic

Theorem 5 and its **corollary** are very useful in computing arithmetic expressions **mod** *n*

Example: to compute 15^{120} **mod** *68*

we would do 15^{120} first, and then
take the result **mod** *68*.

-use the calculator to calculate it

<u>another approach</u>:

$15^{120} = \underbrace{15 \cdot 15 \cdot \ldots \cdot 15}_{120 \quad 15s}$

Instead do

p = (15 · 15) mod 68

p = (p · 15) mod 68 and so forth … 119 times

```
p := 15

For i:= 1 to 119
 p := (15*p) mod 68
End-for

Return(p)
```

i = 1 , p = 21
i = 2 , p = 43
i = 3 , p = 33
i = 4 , p = 19
i = 5 , p = 13
i = 6 , p = 59
i = 7 , p = 1
i = 8 , p = 15
i = 9 , p = 21
i = 10 , p = 43
i = 11 , p = 33
i = 12 , p = 19
i = 13 , p = 13
i = 14 , p = 59
i = 15 , p = 1
i = 16 , p = 15
i = 17 , p = 21
i = 18 , p = 43
i = 19 , p = 33
i = 20 , p = 19
i = 21 , p = 13
i = 22 , p = 59
i = 23 , p = 1
i = 24 , p = 15
i = 25 , p = 21
i = 26 , p = 43
i = 27 , p = 33

i = 28 , p = 19
i = 29 , p = 13
i = 30 , p = 59
i = 31 , p = 1
i = 32 , p = 15
i = 33 , p = 21
i = 34 , p = 43
i = 35 , p = 33
i = 36 , p = 19
i = 37 , p = 13
i = 38 , p = 59
i = 39 , p = 1
i = 40 , p = 15
i = 41 , p = 21
i = 42 , p = 43
i = 43 , p = 33
i = 44 , p = 19
i = 45 , p = 13
i = 46 , p = 59
i = 47 , p = 1
i = 48 , p = 15
i = 49 , p = 21
i = 50 , p = 43
i = 51 , p = 33
i = 52 , p = 19
i = 53 , p = 13
i = 54 , p = 59

i = 55 , p = 1
i = 56 , p = 15
i = 57 , p = 21
i = 58 , p = 43
i = 59 , p = 33
i = 60 , p = 19
i = 61 , p = 13
i = 62 , p = 59
i = 63 , p = 1
i = 64 , p = 15
i = 65 , p = 21
i = 66 , p = 43
i = 67 , p = 33
i = 68 , p = 19
i = 69 , p = 13
i = 70 , p = 59
i = 71 , p = 1
i = 72 , p = 15
i = 73 , p = 21
i = 74 , p = 43
i = 75 , p = 33
i = 76 , p = 19
i = 77 , p = 13
i = 78 , p = 59
i = 79 , p = 1
i = 80 , p = 15
i = 81 , p = 21

```
p := 15

For i:= 1 to 119
 p := (15*p) mod 68
End-for

Return(p)
```

i = 82 , p = 43
i = 83 , p = 33
i = 84 , p = 19
i = 85 , p = 13
i = 86 , p = 59
i = 87 , p = 1
i = 88 , p = 15
i = 89 , p = 21
i = 90 , p = 43
i = 91 , p = 33
i = 92 , p = 19
i = 93 , p = 13
i = 94 , p = 59
i = 95 , p = 1
i = 96 , p = 15
i = 97 , p = 21
i = 98 , p = 43
i = 99 , p = 33
i = 100 , p = 19

i = 101 , p = 13
i = 102 , p = 59
i = 103 , p = 1
i = 104 , p = 15
i = 105 , p = 21
i = 106 , p = 43
i = 107 , p = 33
i = 108 , p = 19
i = 109 , p = 13
i = 110 , p = 59
i = 111 , p = 1
i = 112 , p = 15
i = 113 , p = 21
i = 114 , p = 43
i = 115 , p = 33
i = 116 , p = 19
i = 117 , p = 13
i = 118 , p = 59
i = 119 , p = 1

$15^{120} \bmod 68 = 1$

6.2 Modular arithmetic

Example: compute $(15^{12} + 17 \cdot 23)$ **mod** 7

$$(15^{12} + 17 \cdot 23) \textbf{ mod } 7 =$$
$$= [(15 \textbf{ mod } 7)^{12} + (17 \textbf{ mod } 7) \cdot (23 \bmod 7)] \textbf{ mod } 7 =$$
$$= [\quad 1^{12} \quad + \quad 3 \quad \cdot \quad 2 \quad] \textbf{ mod } 7 =$$
$$= [\quad 1 \quad + \quad 6 \quad] \textbf{ mod } 7 = 7 \textbf{ mod } 7 = 0$$

6.2 Modular arithmetic - rings

The operation defined by adding two numbers and applying **mod** *n* to the result is called addition **mod** *n*.

The operation defined by multiplying two numbers and applying **mod** *n* to the result is called multiplication **mod** *n*.

The set {0, 1, 2,..., n-1} along with addition and multiplication **mod** *n* defines a closed mathematical system with *n* elements called a ring.

Denotation: Z_n

Many different kinds of rings are studied in abstract mathematics.

We will only be concerned with rings of the form Z_n for some integer *n>1*

6.2 Modular arithmetic - rings

Example: let's consider Z_8

elements of the Z_8: 0,1,2,3,4,5,6,7 operations: + (**mod** 8), $\times$ (**mod** 8)

$3 + 5$ in Z_8 is (3+5) **mod** 8 = 8 **mod** 8 = 0

3×5 in Z_8 is (3×5) **mod** 8 = 15 **mod** 8 = 7

6.2 Applications of Congruences : Hashing Functions

The central computer at an insurance company maintains records for each of its customers.
How can memory locations be assigned so that customer records can be retrieved quickly?
- use a suitably chosen hashing function

6.2 Applications of Congruences : Hashing Functions

The central computer at an insurance company maintains recordds for each of its customers.
How can memory locations be assigned so that customer records can be retrieved quickly?
- use a suitably chosen hashing function

- records are identified using a unique **key** (for example, SSN)

6.2 Applications of Congruences : Hashing Functions

The central computer at an insurance company maintains recordds for each of its customers.
How can memory locations be assigned so that customer records can be retrieved quickly?
- use a suitably chosen hashing function

- records are identified using a unique **key** (for example, SSN)
- a hashing function ***h*** assigns memory location ***h(k)*** to the record that has ***k*** as its key.

6.2 Applications of Congruences : Hashing Functions

The central computer at an insurance company maintains recordds for each of its customers.
How can memory locations be assigned so that customer records can be retrieved quickly?
- use a suitably chosen hashing function

- records are identified using a unique **key** (for example, SSN)
- a hashing function ***h*** assigns memory location ***h(k)*** to the record that has ***k*** as its key.

In practice many different hashing functions are used. One of them is $h(k) = k \bmod m$, m is the number of available memory locations

6.2 Applications of Congruences : Hashing Functions

The central computer at an insurance company maintains recordds for each of its customers.
How can memory locations be assigned so that customer records can be retrieved quickly?
- use a suitably chosen hashing function

- records are identified using a unique **key** (for example, SSN)
- a hashing function ***h*** assigns memory location ***h(k)*** to the record that has ***k*** as its key.

In practice many different hashing functions are used. One of them is $h(k) = k \bmod m$, m is the number of available memory locations

Requirements to hashing functions:
- Hashing functions should be easily evaluated, so that files can be quickly located. $h(k) = k \bmod m$ meets the requirement.

6.2 Applications of Congruences : Hashing Functions

The central computer at an insurance company maintains recordds for each of its customers.
How can memory locations be assigned so that customer records can be retrieved quickly?
- use a suitably chosen hashing function

- records are identified using a unique **key** (for example, SSN)
- a hashing function ***h*** assigns memory location ***h(k)*** to the record that has ***k*** as its key.

In practice many different hashing functions are used. One of them is $h(k) = k \bmod m$, m is the number of available memory locations

Requirements to hashing functions:
- Hashing functions should be easily evaluated, so that files can be quickly located. $h(k) = k \bmod m$ meets the requirement.
- Hashing functions should be onto, so that all memory locations are possible. $h(k) = k \bmod m$ is onto.

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 =$
$111678907 \div 102 = 1094891.186...$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$

$111678907 \div 102 = 1094891.186...$

therefore $111678907 - 102 \cdot 1094891 = 25$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$

$111678907 \div 102 = 1094891.186...$

therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 =$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$

$111678907 \div 102 = 1094891.186...$

therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 =$

$192876903 \div 102 = 1890950.029...$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$

$111678907 \div 102 = 1094891.186...$

therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 = 3$

$192876903 \div 102 = 1890950.029...$

therefore $192876903 - 102 \cdot 1890950 = 3$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$

$111678907 \div 102 = 1094891.186...$

therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 = 3$

$192876903 \div 102 = 1890950.029...$

therefore $192876903 - 102 \cdot 1890950 = 3$

$h(111679615) = 111679621 \bmod 102 =$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$
$111678907 \div 102 = 1094891.186...$
therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 = 3$
$192876903 \div 102 = 1890950.029...$
therefore $192876903 - 102 \cdot 1890950 = 3$

$h(111679615) = 111679621 \bmod 102 =$
$111679621 \div 102 = 1094898.186$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$
$111678907 \div 102 = 1094891.186...$
therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 = 3$
$192876903 \div 102 = 1890950.029...$
therefore $192876903 - 102 \cdot 1890950 = 3$

$h(111679615) = 111679621 \bmod 102 = 25$
$111679621 \div 102 = 1094898.186$
therefore $111679621 - 102 \cdot 1094898 = 25$

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$
$111678907 \div 102 = 1094891.186...$
therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 = 3$
$192876903 \div 102 = 1890950.029...$
therefore $192876903 - 102 \cdot 1890950 = 3$

$h(111679615) = 111679621 \bmod 102 = 25$
$111679621 \div 102 = 1094898.186$
therefore $111679621 - 102 \cdot 1094898 = 25$

Answer: $h(s_1) = 25$, $h(s_2) = 3$, $h(s_3) = 25$.

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679615$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$
$111678907 \div 102 = 1094891.186...$
therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 = 3$
$192876903 \div 102 = 1890950.029...$
therefore $192876903 - 102 \cdot 1890950 = 3$

$h(111679615) = 111679621 \bmod 102 = 25$
$111679621 \div 102 = 1094898.186$
therefore $111679621 - 102 \cdot 1094898 = 25$

Answer: $h(s_1) = 25$, $h(s_2) = 3$, $h(s_3) = 25$.

Did you notice that this hashing function is not one-to-one?

6.2 Applications of Congruences : Hashing Functions

Example 5:
Let $m = 102$, $s_1 = 111678907$, $s_2 = 192876903$, and $s3 = 111679621$
Assume that $h(k) = k$ **mod** m. Find $h(s_1)$, $h(s_2)$, $h(s_3)$.

$h(111678907) = 111678907 \bmod 102 = 25$
$111678907 \div 102 = 1094891.245...$
therefore $111678907 - 102 \cdot 1094891 = 25$

$h(192876903) = 192876903 \bmod 102 = 3$
$192876903 \div 102 = 1890950.029...$
therefore $192876903 - 102 \cdot 1890950 = 3$

$h(111679621) = 111679621 \bmod 102 = 25$
$111679621 \div 102 = 1094898.245...$
therefore $111679621 - 102 \cdot 1094898 = 25$

Answer: $h(s_1) = 25$, $h(s_2) = 3$, $h(s_3) = 25$.

Did you notice that this hashing function is not one-to-one?
- collision occurs when more than one file is assigned to the same memory location.

6.2 Applications of Congruences : Pseudo-random Numbers

randomly chosen numbers are often needed for computer simulations and other applications.

6.2 Applications of Congruences : Pseudo-random Numbers

randomly chosen numbers are often needed for computer simulations and other applications.

Different methods have been devised for generating numbers that have properties close to randomly chosen numbers, but they are still not random numbers, because they were generated by *systematic methods*.

Such numbers are called pseudorandom numbers.

6.2 Applications of Congruences : Pseudo-random Numbers

randomly chosen numbers are often needed for computer simulations and other applications.

Different methods have been devised for generating numbers that have properties close to randomly chosen numbers, but they are still not random numbers, because they were generated by *systematic methods*.

Such numbers are called pseudorandom numbers.

One of the methods: linear congruential method
- we choose 4 integers:

the **modulus** m,	with
the **multiplier** a,	$2 \le a < m$,
the **increment** c, and	$0 \le c < m$, and
the **seed** x_0,	$0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m

$$0 \le x_n < m, \text{ for all } n$$

6.2 Applications of Congruences : Pseudo-random Numbers

randomly chosen numbers are often needed for computer simulations and other applications.

Different methods have been devised for generating numbers that have properties close to randomly chosen numbers, but they are still not random numbers, because they were generated by *systematic methods*.

Such numbers are called pseudorandom numbers.

One of the methods: linear congruential method
- we choose 4 integers:

the **modulus** m,	with
the **multiplier** a,	$2 \le a < m$,
the **increment** c, and	$0 \le c < m$, and
the **seed** x_0,	$0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m

$$0 \le x_n < m, \text{ for all } n$$

If $c = 0$, then the generator is called a pure multiplicative generator

6.2 Pseudo-random Numbers

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

6.2 Pseudo-random Numbers

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:
$x_0 = 2$

6.2 Pseudo-random Numbers

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 =$

6.2 Pseudo-random Numbers

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:
$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11$

6.2 Pseudo-random Numbers

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 =$

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 = 1 \bmod 11 = 1$

6.2 Pseudo-random Numbers

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 = 1 \bmod 11 = 1$

$x_4 = (3 \cdot 1 + 1) \bmod 11 = 4 \bmod 11 = 4$

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6:
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 = 1 \bmod 11 = 1$

$x_4 = (3 \cdot 1 + 1) \bmod 11 = 4 \bmod 11 = 4$

$x_5 = (3 \cdot 4 + 1) \bmod 11 = 13 \bmod 11 = 2$

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6:
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 = 1 \bmod 11 = 1$

$x_4 = (3 \cdot 1 + 1) \bmod 11 = 4 \bmod 11 = 4$

$x_5 = (3 \cdot 4 + 1) \bmod 11 = 13 \bmod 11 = 2$ – note that we got 2 again (as x_0)

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6:
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 = 1 \bmod 11 = 1$

$x_4 = (3 \cdot 1 + 1) \bmod 11 = 4 \bmod 11 = 4$

$x_5 = (3 \cdot 4 + 1) \bmod 11 = 13 \bmod 11 = 2$ – note that we got 2 again (as x_0)

$x_6 = (3 \cdot 2 + 1) \bmod 11 =$

modulus m, **multiplier** a, **increment** c, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 = 1 \bmod 11 = 1$

$x_4 = (3 \cdot 1 + 1) \bmod 11 = 4 \bmod 11 = 4$

$x_5 = (3 \cdot 4 + 1) \bmod 11 = 13 \bmod 11 = 2$ – note that we got 2 again (as x_0)

$x_6 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

6.2 Pseudo-random Numbers

modulus *m*, **multiplier** *a*, **increment** *c*, and the **seed** x_0,

$2 \le a < m$, $0 \le c < m$, and $0 \le x_0 < m$

Sequence $\{x_n\}$ of pseudorandom numbers is generated by

$x_{n+1} = (ax_n + c)$ **mod** m, where $0 \le x_n < m$, for all n

Example 6*:*
What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 1)$ ***mod*** 11, with the seed $x_0 = 2$?

Solution:

$x_0 = 2$

$x_1 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$

$x_2 = (3 \cdot 7 + 1) \bmod 11 = 22 \bmod 11 = 0$

$x_3 = (3 \cdot 0 + 1) \bmod 11 = 1 \bmod 11 = 1$

$x_4 = (3 \cdot 1 + 1) \bmod 11 = 4 \bmod 11 = 4$

$x_5 = (3 \cdot 4 + 1) \bmod 11 = 13 \bmod 11 = 2$ – note that we got 2 again (as x_0)

$x_6 = (3 \cdot 2 + 1) \bmod 11 = 7 \bmod 11 = 7$ – not good, because from now on we have a pattern in number-generation:

2 7 0 1 4 2 7 0 1 4 2 7 0 1 4 2 7 0 1 4 ....