Modular Arithmetic and Applications Section 2.4

Doug Rall
Mathematics 110
Spring 2017

Modular Arithmetic

Recall: We say two natural numbers **a** and **b** are

equivalent modulo n

if the remainder when **a** is divided by **n** is the same as the remainder when **b** is divided by **n**.
We write this as $\mathbf{a} \equiv \mathbf{b} \mod \mathbf{n}$

Modular Arithmetic

Recall: We say two natural numbers **a** and **b** are

equivalent modulo *n*

if the remainder when **a** is divided by **n** is the same as the remainder when **b** is divided by **n**.
We write this as $\mathbf{a} \equiv \mathbf{b} \mod \mathbf{n}$

Examples

- $\mathbf{97} \equiv \mathbf{17} \mod \mathbf{10}$
- $\mathbf{25} \equiv \mathbf{53} \mod \mathbf{7}$
- $\mathbf{3^3} \equiv \mathbf{102} \mod \mathbf{5}$

Modular Arithmetic

Practice Exercises

Fill in the blanks:

- $\mathbf{3} \times (\mathbf{4} + \mathbf{7} + \mathbf{13} + \mathbf{1}) + \mathbf{22} + \mathbf{4} + \mathbf{9} + \mathbf{8} \equiv$ _____ mod **9**

Modular Arithmetic

Practice Exercises

Fill in the blanks:

- $\mathbf{3 \times (4 + 7 + 13 + 1) + 22 + 4 + 9 + 8} \equiv$ _____ mod **9**
- $\mathbf{3 + 5 + 9 + 2 + 2 + 2 + 4 + 1 + 8} \equiv$ _____ mod **7**

Modular Arithmetic

Practice Exercises

Fill in the blanks:

- $3 \times (4 + 7 + 13 + 1) + 22 + 4 + 9 + 8 \equiv$ _____ mod 9
- $3 + 5 + 9 + 2 + 2 + 2 + 4 + 1 + 8 \equiv$ _____ mod 7
- $3 + 5 + 9 + 2 + 10 + 2 +$ ____ $+4 + 1 + 8 \equiv 5$ mod 12

Modular Arithmetic

Practice Exercises

Fill in the blanks:

- $3 \times (4 + 7 + 13 + 1) + 22 + 4 + 9 + 8 \equiv$ _____ mod 9
- $3 + 5 + 9 + 2 + 2 + 2 + 4 + 1 + 8 \equiv$ _____ mod 7
- $3 + 5 + 9 + 2 + 10 + 2 +$ ____ $+4 + 1 + 8 \equiv 5$ mod 12
- $(7 \times 14^3) + 2^9 \equiv$ _____ mod 10

Modular Arithmetic

Practice Exercises

Fill in the blanks:

- $3 \times (4 + 7 + 13 + 1) + 22 + 4 + 9 + 8 \equiv$ _____ mod 9
- $3 + 5 + 9 + 2 + 2 + 2 + 4 + 1 + 8 \equiv$ _____ mod 7
- $3 + 5 + 9 + 2 + 10 + 2 +$ ____ $+4 + 1 + 8 \equiv 5$ mod 12
- $(7 \times 14^3) + 2^9 \equiv$ _____ mod 10
- $7^8 + (32 \times 18 \times 43) \equiv$ _____ mod 5

Modular Arithmetic

Practice Exercises

Fill in the blanks:

- $3 \times (4 + 7 + 13 + 1) + 22 + 4 + 9 + 8 \equiv \_\_\_\_\_ \mod 9$
- $3 + 5 + 9 + 2 + 2 + 2 + 4 + 1 + 8 \equiv \_\_\_\_\_ \mod 7$
- $3 + 5 + 9 + 2 + 10 + 2 + \_\_\_\_ + 4 + 1 + 8 \equiv 5 \mod 12$
- $(7 \times 14^3) + 2^9 \equiv \_\_\_\_\_ \mod 10$
- $7^8 + (32 \times 18 \times 43) \equiv \_\_\_\_\_ \mod 5$
- $7^8 + (32 \times 18 \times 43) \equiv \_\_\_\_\_ \mod 6$

Modular Arithmetic

Practice Exercises

Fill in the blanks:

- $3 \times (4 + 7 + 13 + 1) + 22 + 4 + 9 + 8 \equiv$ _____ mod 9
- $3 + 5 + 9 + 2 + 2 + 2 + 4 + 1 + 8 \equiv$ _____ mod 7
- $3 + 5 + 9 + 2 + 10 + 2 +$ ____ $+4 + 1 + 8 \equiv 5$ mod 12
- $(7 \times 14^3) + 2^9 \equiv$ _____ mod 10
- $7^8 + (32 \times 18 \times 43) \equiv$ _____ mod 5
- $7^8 + (32 \times 18 \times 43) \equiv$ _____ mod 6
- $3^{123} \equiv$ _____ mod 10

ID Numbers or Codes

Functions of an ID number or ID Code:

1. To uniquely identify objects or persons so as to easily reference them or track them. Examples?

ID Numbers or Codes

Functions of an ID number or ID Code:

1. To uniquely identify objects or persons so as to easily reference them or track them. Examples?
2. To detect (and even correct) errors in transmission of data about these objects or persons. Examples?

ID Numbers or Codes

Functions of an ID number or ID Code:

1. To uniquely identify objects or persons so as to easily reference them or track them. Examples?
2. To detect (and even correct) errors in transmission of data about these objects or persons. Examples?

In each of the following examples let us try to determine what type of transmission errors would be detected and which would not be detected.

Check Digits

USPS code for money orders: An 11-digit number

$$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11}$$

having the property that a_{11} is the remainder when

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10}$$

is divided by 7.

Check Digits

USPS code for money orders: An 11-digit number

$$a_1\,a_2\,a_3\,a_4\,a_5\,a_6\,a_7\,a_8\,a_9\,a_{10}\,a_{11}$$

having the property that a_{11} is the remainder when

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10}$$

is divided by 7.

That is, a_{11} must satisfy

$$\mathbf{a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \mod 7}\,.$$

Check Digits - USPS

Examples

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \pmod 7 .$$

1. $3734551211x$ x is the check digit. $x =$

Check Digits - USPS

Examples

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \pmod 7 .$$

1. $3734551211x$ x is the check digit. $x =$
2. $1818181818y$ y is the check digit. $y =$

Check Digits - USPS

Examples

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \pmod 7 .$$

1. $3734551211x$ x is the check digit. $x =$
2. $1818181818y$ y is the check digit. $y =$
3. $2130561211z$ z is the check digit. $z =$

Check Digits - USPS

Examples

$$\mathbf{a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \mod 7}.$$

1. $3734551211x$ x is the check digit. $x =$
2. $1818181818y$ y is the check digit. $y =$
3. $2130561211z$ z is the check digit. $z =$

1. $3734551211x$ $\mathbf{x = 4}$

Check Digits - USPS

Examples

$$\mathbf{a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \mod 7}.$$

1. $3734551211x$ x is the check digit. $x =$
2. $1818181818y$ y is the check digit. $y =$
3. $2130561211z$ z is the check digit. $z =$

1. $3734551211x$ $\mathbf{x = 4}$
2. $1818181818y$ $\mathbf{y = 3}$

Check Digits - USPS

Examples

$$\mathbf{a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \pmod 7}.$$

1. $3734551211x$ x is the check digit. $x =$
2. $1818181818y$ y is the check digit. $y =$
3. $2130561211z$ z is the check digit. $z =$

1. $3734551211x$ $\mathbf{x = 4}$
2. $1818181818y$ $\mathbf{y = 3}$
3. $2130561211z$ $\mathbf{z = 1}$

Check Digits - USPS

Error Detection

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \mod 7 .$$

Check Digits - USPS

Error Detection

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \mod 7 .$$

The check digit will detect anytime a single digit is incorrect. **Why?**

Check Digits - USPS

Error Detection

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} \equiv a_{11} \pmod 7 .$$

The check digit will detect anytime a single digit is incorrect. **Why?**

Or will it?

Check Digits - UPC

The Universal Product Code (UPC) is a 12-digit number

$$d_1 d_2 d_3 d_4 d_5 d_6 d_7 d_8 d_9 d_{10} d_{11} d_{12}$$

having the property that the check digit d_{12} is chosen so that

$$3d_1 + d_2 + 3d_3 + d_4 + 3d_5 + d_6 + 3d_7 + d_8 + 3d_9 + d_{10} + 3d_{11} + d_{12}$$

is evenly divided by 10.

Check Digits - UPC

The Universal Product Code (UPC) is a 12-digit number

$$d_1\,d_2\,d_3\,d_4\,d_5\,d_6\,d_7\,d_8\,d_9\,d_{10}\,d_{11}\,d_{12}$$

having the property that the check digit d_{12} is chosen so that

$$3d_1 + d_2 + 3d_3 + d_4 + 3d_5 + d_6 + 3d_7 + d_8 + 3d_9 + d_{10} + 3d_{11} + d_{12}$$

is evenly divided by 10.

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

Check Digits - UPC

Examples

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $04141508575x$ (Publix Instant Handsanitizer) $x =$
2. $31254662936y$ (Halls Mentho-Lyptus Cough Drops) $y =$
3. $04300005000z$ (Gevalia Kaffe K-cups 12 Pack) $z =$

Check Digits - UPC

Examples

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $0414150857 5x$ (Publix Instant Handsanitizer) $x =$
2. $3125466293 6y$ (Halls Mentho-Lyptus Cough Drops) $y =$
3. $0430000500 0z$ (Gevalia Kaffe K-cups 12 Pack) $z =$

1. $0414150857 5x$ (Publix Instant Handsanitizer) $\mathbf{x = 6}$

Check Digits - UPC

Examples

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $0414150857 5x$ (Publix Instant Handsanitizer) $x =$
2. $3125466293 6y$ (Halls Mentho-Lyptus Cough Drops) $y =$
3. $0430000500 0z$ (Gevalia Kaffe K-cups 12 Pack) $z =$

1. $0414150857 5x$ (Publix Instant Handsanitizer) $\mathbf{x = 6}$
2. $3125466293 6y$ (Halls Mentho-Lyptus Cough Drops) $\mathbf{y = 3}$

Check Digits - UPC

Examples

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $0414150857 5x$ (Publix Instant Handsanitizer) $x =$
2. $3125466293 6y$ (Halls Mentho-Lyptus Cough Drops) $y =$
3. $0430000500 0z$ (Gevalia Kaffe K-cups 12 Pack) $z =$

1. $0414150857 5x$ (Publix Instant Handsanitizer) $\mathbf{x = 6}$
2. $3125466293 6y$ (Halls Mentho-Lyptus Cough Drops) $\mathbf{y = 3}$
3. $0430000500 0z$ (Gevalia Kaffe K-cups 12 Pack) $\mathbf{z = 2}$

Check Digits - UPC

Error Detection

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

Check Digits - UPC

Error Detection

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

The check digit will detect anytime a single digit is incorrect. **Why?**

Check Digits - UPC

Error Detection

$$\begin{aligned} 3 \times (d_1 + d_3 + d_5 + d_7 + d_9 + d_{11}) \quad &+ \\ (d_2 + d_4 + d_6 + d_8 + d_{10} + d_{12}) \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

The check digit will detect anytime a single digit is incorrect. **Why?**

The check digit will sometimes detect when two digits are interchanged, but sometimes this kind of error is not detected.

Check Digits - ISBN-13

The 13-digit International Standard Book Number (ISBN-13) has 13 digits

$$a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}.$$

Check Digits - ISBN-13

The 13-digit International Standard Book Number (ISBN-13) has 13 digits

$$\mathbf{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}}\,.$$

They are usually arranged into one of the following formats:

- $a_1 a_2 a_3 - a_4 - a_5 a_6 a_7 - a_8 a_9 a_{10} a_{11} a_{12} - a_{13}$
- $a_1 a_2 a_3 - a_4 - a_5 a_6 - a_7 a_8 a_9 a_{10} a_{11} a_{12} - a_{13}$
- $a_1 a_2 a_3 - a_4 - a_5 a_6 a_7 a_8 - a_9 a_{10} a_{11} a_{12} - a_{13}$

Check Digits - ISBN-13

The 13-digit International Standard Book Number (ISBN-13) has 13 digits

$$\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4}, \mathbf{a_5}, \mathbf{a_6}, \mathbf{a_7}, \mathbf{a_8}, \mathbf{a_9}, \mathbf{a_{10}}, \mathbf{a_{11}}, \mathbf{a_{12}}, \mathbf{a_{13}}\,.$$

They are usually arranged into one of the following formats:

- $a_1a_2a_3 - a_4 - a_5a_6a_7 - a_8a_9a_{10}a_{11}a_{12} - a_{13}$
- $a_1a_2a_3 - a_4 - a_5a_6 - a_7a_8a_9a_{10}a_{11}a_{12} - a_{13}$
- $a_1a_2a_3 - a_4 - a_5a_6a_7a_8 - a_9a_{10}a_{11}a_{12} - a_{13}$

For example,

- $978 - 0 - 691 - 15423 - 7$
- $978 - 0 - 43 - 125560 - 6$
- $978 - 1 - 4292 - 0900 - 7$

are valid ISBN-13 codes.

ISBN-13

In

$$\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4}, \mathbf{a_5}, \mathbf{a_6}, \mathbf{a_7}, \mathbf{a_8}, \mathbf{a_9}, \mathbf{a_{10}}, \mathbf{a_{11}}, \mathbf{a_{12}}, \mathbf{a_{13}}\,.$$

The check digit a_{13} is chosen so that

$$\begin{aligned} 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 \quad &+ \\ 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + 1a_{13} \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

ISBN-13

In

$$\mathbf{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}}\,.$$

The check digit a_{13} is chosen so that

$$\begin{aligned} 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 \quad &+ \\ 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + 1a_{13} \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $978 - 1 - 305 - 65422 - x$ (calculus book) $x =$

ISBN-13

In

$$\mathbf{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}}\,.$$

The check digit a_{13} is chosen so that

$$\begin{aligned} 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 \quad &+ \\ 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + 1a_{13} \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $978 - 1 - 305 - 65422 - x$ (calculus book) $x =$
2. $978 - 1 - 305 - 65422 - \mathbf{8}$

ISBN-13

In

$$\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4}, \mathbf{a_5}, \mathbf{a_6}, \mathbf{a_7}, \mathbf{a_8}, \mathbf{a_9}, \mathbf{a_{10}}, \mathbf{a_{11}}, \mathbf{a_{12}}, \mathbf{a_{13}}\,.$$

The check digit a_{13} is chosen so that

$$\begin{aligned} 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 \quad &+ \\ 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + 1a_{13} \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $978 - 1 - 305 - 65422 - x$ (calculus book) $x =$
2. $978 - 1 - 305 - 65422 - \mathbf{8}$
3. $978 - 0 - 19 - 974044 - y$ (puzzle book) $y =$

ISBN-13

In

$$\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4}, \mathbf{a_5}, \mathbf{a_6}, \mathbf{a_7}, \mathbf{a_8}, \mathbf{a_9}, \mathbf{a_{10}}, \mathbf{a_{11}}, \mathbf{a_{12}}, \mathbf{a_{13}}\,.$$

The check digit a_{13} is chosen so that

$$\begin{aligned} 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 \quad &+ \\ 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + 1a_{13} \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $978 - 1 - 305 - 65422 - x$ (calculus book) $x =$
2. $978 - 1 - 305 - 65422 - \mathbf{8}$
3. $978 - 0 - 19 - 974044 - y$ (puzzle book) $y =$
4. $978 - 0 - 19 - 974044 - \mathbf{4}$

ISBN-13

In

$$\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4}, \mathbf{a_5}, \mathbf{a_6}, \mathbf{a_7}, \mathbf{a_8}, \mathbf{a_9}, \mathbf{a_{10}}, \mathbf{a_{11}}, \mathbf{a_{12}}, \mathbf{a_{13}}\,.$$

The check digit a_{13} is chosen so that

$$\begin{aligned} 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 \quad &+ \\ 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + 1a_{13} \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $978 - 1 - 305 - 65422 - x$ (calculus book) $x =$
2. $978 - 1 - 305 - 65422 - \mathbf{8}$
3. $978 - 0 - 19 - 974044 - y$ (puzzle book) $y =$
4. $978 - 0 - 19 - 974044 - \mathbf{4}$
5. $978 - z - 5011 - 2560 - 7$ (Stephen King book) $z =$

ISBN-13

In

$$\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3}, \mathbf{a_4}, \mathbf{a_5}, \mathbf{a_6}, \mathbf{a_7}, \mathbf{a_8}, \mathbf{a_9}, \mathbf{a_{10}}, \mathbf{a_{11}}, \mathbf{a_{12}}, \mathbf{a_{13}}\,.$$

The check digit a_{13} is chosen so that

$$\begin{aligned} 1a_1 + 3a_2 + 1a_3 + 3a_4 + 1a_5 + 3a_6 + 1a_7 \quad &+ \\ 3a_8 + 1a_9 + 3a_{10} + 1a_{11} + 3a_{12} + 1a_{13} \quad &\equiv \quad 0 \bmod 10 \end{aligned}$$

1. $978 - 1 - 305 - 65422 - x$ (calculus book) $x =$
2. $978 - 1 - 305 - 65422 - \mathbf{8}$
3. $978 - 0 - 19 - 974044 - y$ (puzzle book) $y =$
4. $978 - 0 - 19 - 974044 - \mathbf{4}$
5. $978 - z - 5011 - 2560 - 7$ (Stephen King book) $z =$
6. $978 - \mathbf{1} - 5011 - 2560 - 7$

ISBN-13

The ISBN-13 detects all single digit errors and the transposition of most pairs of adjacent digits.

ISBN-13

The ISBN-13 detects all single digit errors and the transposition of most pairs of adjacent digits.

Do you see why all single digit errors are detected?

ISBN-13

The ISBN-13 detects all single digit errors and the transposition of most pairs of adjacent digits.

Do you see why all single digit errors are detected?

Do you see why some transpositions of pairs of adjacent digits would not be detected?

ISBN-13

The ISBN-13 detects all single digit errors and the transposition of most pairs of adjacent digits.

Do you see why all single digit errors are detected?

Do you see why some transpositions of pairs of adjacent digits would not be detected?

Can you find some pairs of digits whose transposition would not be detected?