Mod Arithmetic

Revision: 5063

12 February 2024

Aziz Manva

azizmanva@gmail.com

Table of contents

1. Remainders

1.1 Foundation

A. Remainder Equation

1.1: Remainder Equation

$$Dividend = Divisor \times Quotient + Remainder$$

$$\frac{Dividend}{Quotient} = Divisor + \frac{Remainder}{Quotient}$$

$$\underbrace{17}_{Dividend} = \underbrace{5}_{Divisor} \times \underbrace{3}_{Quotient} + \underbrace{2}_{Remainder}$$

$$\frac{17}{5} = 3 + \frac{2}{5}$$

1.2: Shortforms

$$R = Remainder$$
$$Q = Quotient$$

Example 1.3

Find the remainder when:

A. 17 is divided by 5?
B. 24 is divided by 3?
C. 21 is divided by 8?
D. 12 is divided by 7?

$$\frac{17}{5} = 3\frac{2}{5} \Rightarrow R2Q3$$

Example 1.4

Find the maximum possible value of the remainder when a positive integer is divided by

A. 5
B. 12
C. 3
D. 7
E. 3

$$Max\ Remainder = 4$$

B. Days of the Week

Quotient	*Remainder*						
No. of Weeks	R0	R1	R2	R3	No. of Weeks	R0	R1
	Mon	Tue	Wed	Thu		Mon	Tue
0	0	1	2	3	0	0	1
1	7	8	9	10	1	7	8
2	14	15	16	17	2	14	15
3	21	22	23	24	3	21	22

4	28	29	30	31	4	28	29

Example 1.5

Today is Monday. What day is it

A. 3 days from now?
B. 10 days from now?
C. 17 days from now?

$$Mon + 3 = Thu$$
$$Mon + 10 = Mon + 7 + 3 = Mon + 3 = Thu$$
$$Mon + 17 = Thu$$

1.6: Adding a Week

Whenever you add seven days (which is a week), or any multiple of seven days (which is a whole number of weeks), then you get the same day that you started with.

Example 1.7

Today is Monday, 1st Jan. What day is it:

A. Four days from now?
B. Seven days from now?
C. Fourteen days from now?

$$Mon + 4\ days = Friday$$
$$Mon + 7\ days = Mon$$
$$Mon + 14\ days = Mon$$

Example 1.8

Today a Tuesday. I decide to go jogging every day, starting today. Which day is the 100^{th} day of my jogging routine?

Since I start jogging today, I jog for 99 days more beyond today.

$$Tuesday + 99$$
$$= Tuesday + 98 + 1$$
$$= Tuesday + 1$$
$$= Wednesday$$

Example 1.9

Today is Jan 1st, Thursday. What day is Feb 1st?

Mon	Tue	Wed	Thu	Fri	Sat	Sun
			1			
			8			
			15			
			22			
			29	30	**31**	1^{st}

$$Thu + 31 = Thu + 28 + 3 = Thu + 3 = Sun$$

Example 1.10

Today is Feb 1st, Wed of a leap year. What day is Mar 1st?

Mon	Tue	Wed	Thu	Fri	Sat	Sun
		1				
		8				
		15				
		22				
		29	1			

$$Wed + 29 = Wed + 28 + 1 = Wed + 1 = Thu$$

Example 1.11

Today is Saturday, the first day of the last month of the year. What day is the last day of the first month of the next year?

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	
					8	
					15	
					22	
					29	30
31	1					
	8					
	15					
	22					
	29	30	31			

Example 1.12

A. Today is Friday. What day is it seven days from now?
B. The first day ($Jan\ 1^{st}$) of a particular non-leap year is Friday. What day is the first day of the next year?
C. The first day ($Jan\ 1^{st}$) of a particular leap year is Sunday. What day is the first day of the next year?

Part A

$$Friday + 7 = Friday$$

Part B

$$Friday + 365 = Friday + 364 + 1 = Friday + 1 = Saturday$$

Part C

$$Sun + 366 = Sun + 364 + 2 = Sun + 2 = Tue$$

Example 1.13

Today is Wed, Jan 1st, 2025 What day is it on Jan 1st, 2028?

$$Jan\ 1st\ 2026 = Wed + 365 = Wed + 1 = Thu$$
$$Jan\ 1st\ 2027 = Thu + 365 = Thu + 1 = Fri$$
$$Jan\ 1st\ 2028 = Fri + 365 = Fri + 1 = Sat$$

$$Wed + 365(3) = Wed + 1(3) = Sat$$

Example 1.14

Today is Wed, Jan 1st of a leap year. What day is it on Jan 1st three years from now?

$$Jan\ 1\ of\ Year\ 1 = Wed$$
$$Jan\ 1\ of\ Year\ 2 = Wed + 2 = Fri$$
$$Jan\ 1\ of\ Year\ 3 = Fri + 1 = Sat$$
$$Jan\ 1\ of\ Year\ 4 = Sat + 1 = Sun$$

$$Shortcut: Wed + 2 + 1 + 1 = Sun$$

Example 1.15

Jan 1st, 2024 is a Monday. What day will it be on the last day of January 2024?

Mon	Tue	Wed	Thu	Fri	Sat	Sun
1						
8						
15						
22						
29	30	31				

$$31\ is\ a\ Wednesday$$

1.16: Days in February

February has

- 28 days if it not a leap year
- 29 days if it is a leap year

1.17: Leap Year Rules

- A year is a leap year if it is divisible by 4
- There is one exception to the above point. If a year is divisible by 100, then it is a leap year, if it is divisible by 400.

- Two leaps always have 4 years or 8 years between them.

Example 1.18

A. What are the leap years between 1940 and 1960
B. Is 1900 a leap year?

Part A

1940 is a leap year, but we want the years between 1940 and 1960, so we should not count 1940, or 1960.

$$1944, 1948, 1952, 1956 \Rightarrow 4\ years$$

Part B

Normally we would check if the year is divisible by 4. But,1900 is a century year (divisible by 100).
Hence, we need to check if it is divisible by 400.

$$1900\ is\ not\ divisible\ by\ 400 \Rightarrow Not\ a\ leap\ year$$

Example 1.19

The 1st of February is a Tuesday. On what two days can the last day of the month be? Explain.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1					
	8					
	15					
	22					
28	29					

28: $Monday$, 29: $Tuesday$

Example 1.20
The 5^{th} day of a month is Wednesday. On what four days can the last day of the month be? Explain.

If the 5^{th} is a Wednesday, then the 1^{st} day must be a Saturday.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
					1	2
3	4	5			8	
					15	
					22	
				28	29	30
31						

The last date of the month can be
28: $Friday$, 29: $Saturday$, 30: $Sunday$, 31: $Monday$

C. Months of the Year

Quotient	*Remainder*											
No. of Years	R0	R1	R2	R3	R4	R5	R6	R7	R8	R9	R10	R11
	Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec
0	0	1	2	3	4	5	6	7	8	9	10	11
1	12	13	14	15	16	17	18	19	20	21	22	23
2												
3												
4												

Example 1.21
Dorothy's brother was born in the middle of May. Her sister was born 26 months after her brother. What month was her sister born in?

$$May + 26 = May + 24 + 2 = May + 2 = May$$

Example 1.22
Isabel went to the USA in April from India. She returned to visit after 40 months. What month was it?

$$April + 40 = April + 36 + 4 = April + 4 = Aug$$

D. Time of the Day

Example 1.23

A. It is currently 4 am. What is the time after 37 hours?

$$\begin{gathered} 4\ am + 37\ hours \\ = 4\ am + 24 + 13\ hours \\ = 4\ am + 13\ hours \\ = 4\ am + 12 + 1\ hours \\ = 4\ pm + 1\ hours \\ = 5\ pm \end{gathered}$$

Example 1.24

A. It is currently $14{:}00\ hours$. What is the time after 41 hours?

$$\begin{gathered} 14{:}00 + 41\ hours \\ = 14{:}00 + 24 + 17\ hours \\ = 14{:}00 + 17\ hours \\ = 14{:}00 + 10 + 7hours \\ = 24{:}00 + 7\ hours \\ = 00{:}00 + 7hours \\ = 7{:}00\ hours \end{gathered}$$

E. Dozens

Example 1.25

A. Bananas are sold by the dozen. I have 55 bananas. If I sell only complete dozens, how many bananas will be left over?

B. I bought some boxes of bananas. Each box has a dozen bananas. Because I asked for a discount, I got 3 bananas for free. The number of bananas that I have is between 30 and 50. What is the number of bananas that I have?

Part A

$$\frac{55}{12} = \frac{48}{12} + \frac{7}{12} = 4\frac{7}{12} \Rightarrow 7\ Bananas$$

Part B

$$\begin{gathered} 4(12) + 3 = 48 + 3 = 51 > 50 \\ 3(12) + 3 = 36 + 3 = 39 < 50 \end{gathered}$$

F. Remainder Problems

Example 1.26

I have 23 chocolates to be divided among 6 children equally. Chocolates cannot be shared or divided due to *covid* restrictions. Determine the number of chocolates left over.

$$\frac{23}{6} = R5Q3 \Rightarrow 5\ chocolates\ left\ over$$

Example 1.27

Some chocolates are to be divided equally among 4 people. Only whole chocolates are to be shared.
Explain why the number of chocolates left over cannot be four, or more.

If four chocolates or more are left over, give each person one chocolate.
The number of available chocolates reduces by 1.

Keep doing this until the number of chocolates becomes less than 4.

Example 1.28
I have some chocolates to be divided among my three siblings and myself. Only whole chocolates can be shared. Determine the possible values of the number of chocolates that can be left over.

The number of people sharing the chocolate is

$$3\ Siblings + 1(myself) = 4$$

Suppose we have 4 chocolates. Then, we get

$$\frac{4}{4} = R0Q1 \Rightarrow 0\ chocolates\ left\ over$$
$$\frac{5}{4} = R1Q1 \Rightarrow 1\ chocolates\ left\ over$$
$$\frac{6}{4} = R2Q1 \Rightarrow 2\ chocolates\ left\ over$$
$$\frac{7}{4} = R3Q1 \Rightarrow 3\ chocolates\ left\ over$$
$$\frac{8}{4} = R0Q2 \Rightarrow 0\ chocolates\ left\ over$$

	Remainder			
Quotient	R0	R1	R2	R3
0	0	1	2	3
1	4	5	6	7
2	8	9	10	11
3	12	13	14	15
4	16	17	18	19

G. HCF and LCM Problems: Basics

Example 1.29
A two-digit number leaves no remainder when divided by 3, and 5. What are the possibles values of the number?

The number leaves no remainder when divided by 3.

$$\Rightarrow It\ must\ be\ divisible\ by\ 3.$$

The number leaves no remainder when divided by 5.

$$\Rightarrow It\ must\ be\ divisible\ by\ 5.$$

The number is divisible by both 3 and 5. Hence, it must be a multiple of

$$LCM(3,5) = 15$$

$$Multiples\ of\ 15 = \{15,30,45,60,75,90\} \Rightarrow 6\ Numbers$$

Example 1.30
A two-digit number leaves no remainder when divided by 4, and 6. What are the possibles values of the number?

$$LCM(4,6) = 12$$
$$Multiples\ of\ 12 = \{12,24,36,48,60,72,84\} \Rightarrow 7\ Numbers$$

Example 1.31
I have some chocolates. I can divide them into two equal parts, into three equal parts, and into four equal parts, each time with no chocolates left over. The number of chocolates I have is a three-digit number less than 200. Each chocolate costs me three dollars. What is the maximum possible value and the minimum possible of the chocolates that I have?

The number of chocolates that I have must be a multiple of
$$LCM(2,3,4) = 12$$

Further, the number must be greater than 99, and less than 200:
$$12,24,\dots,\underbrace{108}_{\substack{Smallest\ Three\\ Digit\ Number}},\dots,\underbrace{192}_{\substack{Largest\ Three\\ Digit\ Number}}$$

Cost of Chocolates
$$= 108 \times 3 = 324$$
$$= 192 \times 3 = 576$$

H. HCF and LCM Problems: Zero Remainders

1.32: HCF/LCM in Remainders
Remainder problems can often be solved using HCF/LCM concepts.

$$12 = 2 \cdot 2 \cdot 3$$
$$18 = 2 \cdot 3 \cdot 3$$

$$HCF = 2$$
$$LCM = 36$$

Example 1.33
My friends are playing a party game. The host announces a number, and participants must form groups with that many number of people. First the calls out the number 10. Then, he calls out the number 15. Each time, there no participants left over. What is the minimum number of participants at the party?

Since there are no participants left over when forming groups of ten, the number must be a multiple of 10:
$$10,20,\mathbf{30},\dots$$

Since there are no participants left over when forming groups of fifteen, the number must be a multiple of 15:
$$15,\mathbf{30},45,\dots$$

$$LCM(10,15) = 30$$

Example 1.34

I have some marbles. I am thinking of gifting my marbles. If I share them between my three siblings, there are none left over. If I share them between my four cousins, I still have none left over. If I share them with my six best friends, I still have none left over. What is the smallest number of non-zero marbles that I can have?

Note: I will gift all my marbles together: either to my siblings or to cousins, or to my friends.

When shared among my siblings, there are no marbles left over, the marbles must be a multiple of 3:

$$\{3,6,9,\mathbf{12},15,18,21,\dots,3p\}$$

When shared among my cousins, there are no marbles left over, the marbles must be a multiple of 4:

$$\{4,8,\mathbf{12},16,20,\dots,4q\}$$

When shared among my friends, there are no marbles left over, the marbles must be a multiple of 6:

$$\{6,\mathbf{12},18,24\dots,6r\}$$

Hence, the number of marbles must be

$$Multiple\ of\ 3\ \&\ Multiple\ of\ 4\ \&\ Multiple\ of\ 6$$

In other words, the smallest number of marbles is:

$$LCM(3,4,6) = 12$$

Example 1.35

I have 40 brown cupcakes and 60 green cupcakes. What is the smallest number of boxes that I can use to pack the cupcakes if:

A. A box can have brown cupcakes, or green cupcakes, but not both together.
B. Each box holds the same number of cupcakes, and no cupcakes left over.

If we put all 100 cupcakes in one box, then this violates the condition that

$$A\ box\ cannot\ have\ green\ and\ brown\ cupcakes\ together$$

If we put all 40 brown cupcakes in one box, and all 60 green boxes cupcakes in a second, this violates the condition that

$$Each\ box\ holds\ the\ same\ number\ of\ cupcakes$$

Brown								
Box Size	1	2	4	5	8	10	20	40
No. of Boxes	40	20	10	8	5	4	2	1

Green												
Box Size	1	2	3	4	5	6	10	12	15	20	30	60
No. of Boxes	60	30	20	15	12	10	6	5	4	3	2	1

The maximum box size:

$$= HCF(40,60) = 20$$

The number of boxes

$$= \frac{40 + 60}{20} = \frac{100}{20} = 5\ Boxes$$

I. HCF and LCM Problems: Remainders

Example 1.36

A number leaves a remainder of 1 when divided by 3, and 2 divided by 4. What is the smallest possible positive value of the number?

The numbers that leave a remainder of 1 when divided by 3 are:

1,4,7, **10**, …

The numbers that leave a remainder of 2 when divided by 4 are:

2,6, **10**, …

Example 1.37

A farmer leaves some gold coins and the same number of silver coins as an inheritance. The gold coins are distributed among his four children, and there is one left over. The silver coins are distributed among his three siblings, and there are two left over. Determine the smallest possible value

A. of the total number of coins
B. of the total number of coins if the number of gold coins is more than one digit.

Part A

$$5 \div 4\ has\ Remainder\ 1$$
$$5 \div 3\ has\ Remainder\ 2$$

$$5\ gold + 5\ silver = 10\ coins$$

Part B

$$5 + LCM(3,4) = 5 + 12 = 17$$

Example 1.38

A number leaves a remainder of 2 when divided by 5, and 1 divided by 7. What is the smallest possible positive value of the number?

The numbers that leave a remainder of 2 when divided by 5 are:

2,7,12,17, **22**, …

The numbers that leave a remainder of 1 when divided by 7 are:

8,15, **22**, …

Example 1.39

A number leaves a remainder of 1 when divided by 3, and 2 when divided by 4 and 3 when divided by 5. What is the smallest possible positive value of the number?

The numbers that leave a remainder of 1 when divided by 3 are:

$$1,4,7,\mathbf{10},13,16,19,\mathbf{22},25,28,31,\mathbf{34}\ldots$$

The numbers that leave a remainder of 2 when divided by 4 are:

$$2,6,\mathbf{10},14,18,\mathbf{22},26,30,\mathbf{34}\ldots$$

$$34-22=22-10=12$$

The numbers that meet the first two conditions are:

$$10,10+12,10+2(12),\ldots$$
$$10,22,34,46,\mathbf{58},\ldots$$

The answer is:

$$58$$

Example 1.40

If I divide my marbles among my three siblings, I have one left. If I divide my marbles among my five cousins, I still have one marble left. The number of marbles I have is less than 100. What are the possible values for the number of marbles that I have?

When the marbles are divided by 3, there is one left over.

$$Number\ is\ 1\ more\ than\ a\ multiple\ of\ 3.$$

When the marbles are divided by 5, there is one left over.

$$Number\ is\ 1\ more\ than\ a\ multiple\ of\ 5.$$

$$LCM(3,5)+1=15+1=16$$

$$\frac{16}{3}=\frac{15}{3}+\frac{1}{3}=5\frac{1}{3}$$
$$\frac{16}{5}=\frac{15}{5}+\frac{1}{5}=3\frac{1}{5}$$

$$15+1,30+1,45+1,60+1,75+1,90+1$$
$$16,31,46,61,76,91$$

J. HCF and LCM Problems: Numbers less than a Multiple

Example 1.41

A number leaves a remainder of 1 when divided by 3, and 2 when divided by 4 and 3 when divided by 5. What is the smallest possible positive value of the number?

Number leaves a remainder of 1 when divided by 3

$$One\ more\ than\ a\ multiple\ of\ 3=Two\ less\ than\ a\ multiple\ of\ 3$$

Number leaves a remainder of 2 when divided by 4:

$$Two\ more\ than\ a\ multiple\ of\ 4=Two\ less\ than\ a\ multiple\ of\ 4$$

Number leaves a remainder of 3 when divided by 5:

$$Three\ more\ than\ a\ multiple\ of\ 5 = Two\ less\ than\ a\ multiple\ of\ 5$$

$$LCM(3,4,5) - 2 = 60 - 2 = 58$$

K. Finding Remainders

- When finding remainders of numbers, tests of divisibility are often useful.
- Certain tests of divisibility are also tests that will you the remainder.

1.42: Remainder with 2

A number is divisible by 2 if its last digit is any of:

$$0,2,4,6,8$$

Example 1.43

Determine the remainder when each number below is divided by 2:

A. 48
B. 275
C. 17891

Part A

$$\underbrace{\frac{48}{2}}_{Divisible} \rightarrow Remainder = 0$$

Part B

$$\frac{275}{2} = \underbrace{\frac{274}{2}}_{Divisible} + \frac{1}{2}$$

23474 is divisible by 2. Hence, the remainder is:

$$1$$

Part C

$$\frac{17891}{2} = \underbrace{\frac{17890}{2}}_{Divisible} + \frac{1}{2}$$

1.44: Remainder with 4

When a number is divided by 4, the remainder can be found by only calculating the remainder for the last two digits.

Example 1.45

Determine the remainder when each number below is divided by 4:

A. 342
B. 717
C. 3913
D. 33579

Pick up the last two digits for each number, and calculate the remainders from those digits.

Part A

$$342 \rightarrow \frac{42}{4} = \frac{40}{4} + \frac{2}{4} = 10\frac{2}{4} \Rightarrow Remainder = 2$$

Part B

$$717 \rightarrow \frac{17}{4} = \frac{16}{4} + \frac{1}{4} = 4\frac{1}{4} \Rightarrow Remainder = 1$$

Part C

$$3913 \rightarrow \frac{13}{4} = \frac{12}{4} + \frac{1}{4} = 3\frac{1}{4} \Rightarrow Remainder = 1$$

Part D

$$33579 \rightarrow \frac{79}{4} = \frac{76}{4} + \frac{3}{4} \Rightarrow Remainder = 3$$

1.46: Remainder with 3

To find the remainder when a number is divided by 3, find the sum of the digits ($say\ S = Sum$), and find the remainder when S is divided by 3.

Example 1.47

Determine the remainder when each number below is divided by 4:

A. 3,475
B. 123,456,789

Part A

$$Sum\ of\ Digits = 3 + 4 + 7 + 5 = 19$$
$$\frac{19}{3} = 6\frac{1}{3} \Rightarrow Remainder = 1$$

Shortcut: Instead of adding the digits, we can take the remainder of each digit first and then add:

$$Sum\ of\ Digits = 3 + 4 + 7 + 5 \equiv 0 + 1 + 1 + 2 \equiv 4 \equiv 1$$

Part B

Sum of the digits

$$= 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45$$
$$\frac{45}{3} = 15 \Rightarrow Remainder = 0$$

Shortcut:

$$= 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9$$
$$\equiv 1 + 2 + 0 + 1 + 2 + 0 + 1 + 2 + 0$$
$$\equiv 3 + 3 + 3$$
$$\equiv 4(3) \Rightarrow Remainder = 0$$

1.48: Remainder with 11

Example 1.49

A. 7,924

$$Digits\ in\ Odd\ positions: 4 + 9 = 13$$
$$Digits\ in\ Even\ positions: 7 + 2 = 9$$

$$13 - 9 = 4$$

Example 1.50

B. 3571

$$Digits\ in\ Odd\ positions: 1 + 5 = 6$$
$$Digits\ in\ Even\ positions: 3 + 7 = 10$$

$$6 - 10 = -4 \Rightarrow 4\ less\ than\ a\ multiple\ of\ 11$$

Add 11

$$-4 + 11 = 7 \Rightarrow Remainder = 7$$

L. Even and Odd

1.51: Even and Odd

An *integer* is even if it is divisible by 2, and odd if it is not divisible by 2.

Example 1.52

Is 2.35 even or odd?

2.35 is not an integer.
Hence, the concept of odd and even does not apply to 2.35.

Example 1.53

Is 0 even or odd?

0 is even because

$$\frac{0}{2} = 0 \Rightarrow Divisible\ by\ 2 \Rightarrow Even$$

1.54: Sum of Even and Odd Numbers

$$Odd + Odd = Even$$
$$Odd + Even = Odd$$
$$Even + Odd = Odd$$
$$Even + Even = Even$$

Any odd number is one more than an even number:

$$Odd_1 = 2m + 1, \quad where\ m\ is\ any\ integer$$
$$Odd_1 = 2n + 1, \quad where\ n\ is\ any\ integer$$

Add the two odd numbers

$$(2m + 1) + (2n + 1)$$
$$= 2m + 2n + 2$$
$$= 2(m + n + 1)$$

Any even number is a multiple of 2:

$$Even = 2p, \quad where\ p\ is\ any\ integer$$

Example 1.55

Mark all correct options

I have an odd number of dogs. I have an even number of cats. If dogs and cats are the only animals in my house, which of the following can be the number of animals that I keep?

A. 23
B. 35
C. 42
D. 12

$$Odd + Even = Odd$$
$$23\ and\ 35\ are\ possible$$
$$Options\ A\ and\ B$$

Example 1.56

I have seventeen cars in my car collection. I want to distribute them among my two siblings in such a way that each one gets an equal number of cars of whole cars. In how many ways can I do this:

A. 0
B. 1
C. 2
D. None of the above
E. Cannot be determined

$$\frac{17}{2} = 8.5$$
$$Zero\ Ways$$

Example 1.57

I start an exercise routine. On the first day, I walk a kilometer. On the second day, I walk two kilometers. On the third day, I walk three kilometers. I begin on the first day of February of a leap year. On how many days of that month will I walk an odd number of kilometers.

$$Day\ 1: 1\ km\ (Odd)$$
$$Day\ 2: 2\ km\ (Even)$$
$$Day\ 3: 3\ km\ (Odd)$$

1,3,5,7,9,11,13,15,17,19,21,23,25,27,29

1.58: Product of Even and Odd Numbers

$$Odd \times Odd = Odd$$
$$Odd \times Even = Even$$
$$Even \times Odd = Even$$
$$Even \times Even = Even$$

Example 1.59

I have an odd number of friends. 2024 was a leap year, so I bought 366 chocolates (one for every day of the year), and distribute all the chocolates in such a way that each gets an equal number of odd number of chocolates.
In how many ways can I do this?

$$No.\ of\ Friends = Odd$$

$$Chocolates\ for\ each\ friend = Odd$$

$$(No.\ of\ Friends)(Chocolates\ for\ each\ friend) = Odd \times Odd = Odd$$

$$Total\ no.\ of\ Chocolates = 366 = Even$$

Hence, you cannot do this.

$$Zero\ Ways$$

M. Remainders of Sums

Example 1.60

A. What is the remainder when 100 is divided by 4?
B. Determine the remainder when $100 + 101 + 102 + 103 + 104 + 105 + 106$ is divided by 4.

Part A

$$\frac{100}{4} = 25\ R\ 0$$

Part B

$$= \frac{100}{4} + \frac{101}{4} + \frac{102}{4} + \frac{103}{4} + \frac{104}{4} + \frac{105}{4} + \frac{106}{4}$$

This has remainder

$$\equiv 0 + 1 + 2 + 3 + 0 + 1 + 2 \equiv 9 \equiv 1$$

Example 1.61

Determine the remainder in each case below:

A. $100 + 101 + 102 + 103 + 104 + 105 + 106$ is divided by 5.
B. $100 + 101 + 102 + 103 + 104 + 105 + 106$ is divided by 6.

Part A

$$100 + 101 + 102 + 103 + 104 + 105 + 106$$
$$\equiv 0 + 1 + 2 + 3 + 4 + 0 + 1 \equiv 11 \equiv 1$$

Part B

$$100 + 101 + 102 + 103 + 104 + 105 + 106$$
$$\equiv 4 + 5 + 0 + 1 + 2 + 3 + 4 \equiv 19 \equiv 1$$

Example 1.62

Determine the remainder when the expression below is divided by 4:

$$1 + 2 + 3 + \cdots + 100$$

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12 + \cdots + 100$$

Since $\frac{100}{4} = 25$, we can split the 100 numbers into 20 groups as follows:

$$\equiv \underbrace{(1 + 2 + 3 + 0)}_{Group\ 1} + \underbrace{(1 + 2 + 3 + 0)}_{Group\ 2} + \underbrace{(1 + 2 + 3 + 0)}_{Group\ 3} + \cdots + \underbrace{(1 + 2 + 3 + 0)}_{Group\ 25}$$

$$\equiv \underbrace{6}_{Group\ 1} + \underbrace{6}_{Group\ 2} + \underbrace{6}_{Group\ 3} + \cdots + \underbrace{6}_{Group\ 25}$$

$$\equiv \underbrace{2}_{Group\ 1} + \underbrace{2}_{Group\ 2} + \underbrace{2}_{Group\ 3} + \cdots + \underbrace{2}_{Group\ 25}$$

Since multiplication is repeated addition:

$$\equiv 2 \times 25 \equiv 50 \equiv 2$$

Example 1.63

Determine the remainder when the expression below is divided by 5:

$$1 + 2 + 3 + \cdots + 100$$

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + \cdots + 100$$

Since $\frac{100}{5} = 20$, we can split the 100 numbers into 20 groups as follows:

$$\equiv \underbrace{(1+2+3+4+0)}_{Group\ 1} + \underbrace{(1+2+3+4+0)}_{Group\ 2} + \cdots + \underbrace{(1+2+3+4+0)}_{Group\ 20}$$

$$\equiv \underbrace{10}_{Group\ 1} + \underbrace{10}_{Group\ 2} + \cdots + \underbrace{10}_{Group\ 20}$$

$$\equiv \underbrace{0}_{Group\ 1} + \underbrace{0}_{Group\ 2} + \cdots + \underbrace{0}_{Group\ 20}$$

Since multiplication is repeated addition:

$$\equiv 0$$

Example 1.64

Determine the remainder when the expression below is divided by 6:

$$1 + 2 + 3 + \cdots + 100$$

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 + 11 + 12 + \cdots + 100$$

Since $\frac{100}{6} = 16\frac{2}{6}$, we can split the 100 numbers into 20 groups as follows:

$$\equiv \underbrace{(1+2+3+4+5+0)}_{Group\ 1} + \underbrace{(1+2+3+4+5+0)}_{Group\ 2} + \cdots + \underbrace{(1+2+3+4+5+0)}_{Group\ 16} + \underbrace{(1+2)}_{Group\ 17}$$

$$\equiv \underbrace{15}_{Group\ 1} + \underbrace{15}_{Group\ 2} + \cdots + \underbrace{15}_{Group\ 16} + \underbrace{2}_{Group\ 17}$$

$$\equiv \underbrace{3}_{Group\ 1} + \underbrace{3}_{Group\ 2} + \cdots + \underbrace{3}_{Group\ 16} + \underbrace{2}_{Group\ 17}$$

Since multiplication is repeated addition:

$$\equiv 3 \times 16 + 2 \equiv 48 + 2 \equiv 0 + 2 \equiv 2$$

Example 1.65

Determine the remainder when the expression below is divided by 3:

$$1 + 2 + 3 + \cdots + 100$$

Since $\frac{100}{3} = 33\frac{1}{3}$, we can split the 100 numbers into 34 groups as follows:

$$\equiv \underbrace{(1+2+0)}_{Group\ 1} + \underbrace{(1+2+0)}_{Group\ 2} + \cdots + \underbrace{(1+2+0)}_{Group\ 33} + \underbrace{1}_{Group\ 34}$$

$$\equiv \underbrace{3}_{Group\ 1} + \underbrace{3}_{Group\ 2} + \cdots + \underbrace{3}_{Group\ 33} + \underbrace{1}_{Group\ 17}$$

$$\equiv \underbrace{0}_{Group\ 1} + \underbrace{0}_{Group\ 2} + \cdots + \underbrace{0}_{Group\ 33} + \underbrace{1}_{Group\ 17}$$

Since multiplication is repeated addition:

$$\equiv 1$$

Example 1.66

Determine the remainder when the expression below is divided by 3:

$$1 + 2 + 3 + \cdots + 1000$$

Since $\frac{1000}{3} = 333\frac{1}{3}$, we can split the 1000 numbers into 334 groups as follows:

$$\equiv \underbrace{(1+2+0)}_{Group\ 1} + \underbrace{(1+2+0)}_{Group\ 2} + \cdots + \underbrace{(1+2+0)}_{Group\ 333} + \underbrace{1}_{Group\ 334}$$

$$\equiv \underbrace{3}_{Group\ 1} + \underbrace{3}_{Group\ 2} + \cdots + \underbrace{3}_{Group\ 333} + \underbrace{1}_{Group\ 334}$$

$$\equiv \underbrace{0}_{Group\ 1} + \underbrace{0}_{Group\ 2} + \cdots + \underbrace{0}_{Group\ 333} + \underbrace{1}_{Group\ 334}$$

Since multiplication is repeated addition:

$$\equiv 1$$

N. Remainders of Product

Example 1.67

When I divide one million by 4, what is the remainder.

$$\frac{1{,}000{,}000}{4} \equiv 0$$

$$\frac{4{,}444{,}444}{4} \equiv 0$$

1.68: Remainder when dividing by a factor

If x is a factor of y, then when y is divided by x, the remainder is zero.

1.69: An important factorization

$$7 \times 11 \times 13 = 1001$$

Example 1.70

$$X = 1000 \times 1001 \times 1002 \times 1003$$

Let

$$A = Remainder\ when\ X\ is\ divided\ by\ 7$$
$$B = Remainder\ when\ X\ is\ divided\ by\ 11$$
$$C = Remainder\ when\ X\ is\ divided\ by\ 13$$

Find

$$A + B + C$$

$$X = 1000 \times (7 \times 11 \times 13) \times 1002 \times 1003$$

$$A + B + C \equiv \frac{X}{7} + \frac{X}{11} + \frac{X}{13} \equiv 0 + 0 + 0 \equiv 0$$

Example 1.71
Determine the remainder when X is divided by 6:

$$X = 1003 \times 1004 \times 1005 \times 1006$$

$$X \equiv 1 \times 2 \times 3 \times 4 \equiv 24 \equiv 0$$

1.2 Basics

A. Remainders

Definition
When doing long division, if a number cannot be divided evenly, we say we have a remainder.

$$41 = 39 + 2 = 13 \times 3 + 2 \Leftrightarrow 41 \div 3 = 13 \text{ Remainder } 2 = \underbrace{13\ R2}_{Notation}, \qquad \underbrace{\frac{x}{y} = a\ Rb}_{Notation}$$

Properties of Remainders
Remainders do not always increase with the value of a number. If a number x is divided by a divisor y, then we have:

$$x \div y \Rightarrow Minimum(Remainder) = 0, \qquad Maximum(Remainder) = y - 1$$

Example 1.72: Patterns
Find the sum of the remainders when the natural numbers from

A. 1 to 1000 are divided by 4.
B. 1 to 2000 are divided by 5.
C. 1 to 1000 are divided by 11.

Part A
The pattern repeats every four numbers. Hence, the cyclicity is 4.

Remainder	1	2	3	0	Divide each number in the rows to the left by 4.
Numbers	1	2	3	4	$5 = 4 \times 1 + 1 \Leftrightarrow 5 \div 4 = 1\ R1$ $9 = 4 \times 2 + 1 \Leftrightarrow 9 \div 4 = 2\ R1$ $12 = 4 \times 3 + 0 \Leftrightarrow 12 \div 4 = 3\ R0$
	$\underbrace{5}_{4\times1+1}$	$\underbrace{6}_{4\times1+2}$	$\underbrace{7}_{4\times1+3}$	$\underbrace{8}_{4\times2+0}$	
	9	$\underbrace{10}_{4\times2+2}$	11	12	

Consider the numbers:

$$\underbrace{1+2+3+4}_{1st\ Group} + \underbrace{5+6+7+8}_{2nd\ Group} + \cdots + \underbrace{997+998+999+1000}_{250th\ Group}$$

We want, not the total of the numbers, but rather the total of their remainders. Hence, divide each number by 4, and write the remainder in its place:

$$\underbrace{1+2+3+0}_{First\ Group} + \underbrace{1+2+3+0}_{2nd\ Group} + \cdots + \underbrace{1+2+3+0}_{250th\ Group}$$

Simplify:

$$\underbrace{6}_{First\ Group} + \underbrace{6}_{2nd\ Group} + \cdots + \underbrace{6}_{250th\ Group} = 6 \times 250 = 1500$$

Part B
Consider the numbers:

$$\underbrace{1+2+3+4+5}_{1st\ Group} + \underbrace{6+7+8+9+10}_{2nd\ Group} + \cdots + \underbrace{1996+1997+1998+1999+2000}_{400th\ Group}$$

$$\underbrace{1+2+3+4+0}_{First\ Group}+\underbrace{1+2+3+4+0}_{2nd\ Group}+\cdots+\underbrace{1+2+3+4+0}_{400th\ Group}$$
$$\underbrace{10}_{First\ Group}+\underbrace{10}_{2nd\ Group}+\cdots+\underbrace{10}_{400th\ Group}=10\times 400=4000$$

Part C

$$\underbrace{1+2+\cdots+0}_{1st\ Group}+\underbrace{12+13+\cdots 22}_{2nd\ Group}+\cdots+\underbrace{\ldots+999+1000+\mathbf{1001}}_{91st\ Group}$$
$$\underbrace{1+2+\cdots+0}_{1st\ Group}+\underbrace{1+2+\cdots+0}_{2nd\ Group}+\cdots+\underbrace{1+2+\cdots+\mathbf{0}}_{91st\ Group}$$
$$\underbrace{55}_{First\ Group}+\underbrace{55}_{2nd\ Group}+\cdots+\underbrace{55}_{91st\ Group}=55\times 91=5{,}005$$

Example 1.73: Remainders when divided by 5

Determine the pattern when the following is divided by 5:

A. The natural numbers
B. The squares of the natural numbers
C. The cubes of the natural numbers

Number	0	1	2	3	4	5	6	7	8	9	10			
Remainder	0	1	2	3	4	0	1	2	3	4	0			
Squares	0	1	4	9	16	25	36	49	64	81	100	.	.	.
Remainder	0	1	4	4	1	0	1	4	4	1	0			
Cubes	0	1	8	27	64	125	216	343	512	729	1000			
Remainder	0	1	3	2	4	0	1	3	2	4	0			

Part A

Any five consecutive natural numbers must be of the form:

$$5x, 5x+1, 5x+2, 5x+3, 5x+4$$

And hence they have remainders:

$$0,1,2,3,4$$

Part B

Any five consecutive natural numbers must be of the form:

$$5x, 5x+1, 5x+2, 5x+3, 5x+4$$

Hence, their squares must have remainder:

$$\frac{(5x)^2}{5}=\frac{25x^2}{5}=5x^2\Rightarrow Remainder=0$$
$$\frac{(5x+a)^2}{5}=\frac{25x^2+10ax+a^2}{5}=\frac{25x^2}{5}+\frac{10ax}{5}+\frac{a^2}{5}=\underbrace{5x^2+2ax}_{Multiple\ of\ 5}+\frac{a^2}{5}$$

Since the first two terms are a multiple of 5, we only need to check $\frac{a^2}{5}$ for $a=1,2,3,4$:

$$\frac{1^2}{5}\Rightarrow Remainder\ 1$$
$$\frac{2^2}{5}\Rightarrow Remainder\ 4$$
$$\frac{3^2}{5}\Rightarrow Remainder\ 4$$

$$\frac{4^2}{5} \Rightarrow Remainder\ 1$$

Make use of the table above to answer the questions below:

A. How many numbers less than one million are perfect squares which are two more than a multiple of 5?
B. How many natural numbers less than one thousand are perfect squares which are a multiple of 5?
C. How many perfect cubes less than one million are two more than a multiple of 5?
D. How many natural numbers less than 1000 are such that when divided by 5, the number, its square and its cube all have the same remainder?

Part A

If the number is two more than a multiple of 5, then it must have

$$Remainder\ 2\ when\ divided\ by\ 5$$

There are no such numbers.

$$Answer = 0$$

Part B

If a number is a multiple of 5, then it must have remainder zero, when divided by 5.
The remainder zero occurs every fifth number.
The largest perfect square less than 1000 is:

$$961 = 31^2$$

Hence, the perfect squares which are a multiple of 5 will be:

$$5^2, 10^2, 15^2, 20^2, 25^2, 30^2 \Rightarrow 6\ Numbers$$

Part C

$$1{,}000{,}000 = 100^3$$
$$1^3, 2^3, \mathbf{3^3}, \dots, 99^3$$

$$Remainder\ 2\ when\ divided\ by\ 5$$

Out of every five numbers, there is one number that meets the conditions:

$$\frac{99}{5} = 19\frac{4}{5}$$

And since 98^3 is in the list, we round upwards, giving us:

$$20\ Numbers$$

Part D

Consider

$$\mathbf{1}, 2, 3, 4, \mathbf{5}, \dots, 999, 1000$$

Which has 200 groups of 5.

The numbers satisfying this condition will be

$$200 \times 2 = 400$$

But 1000 is not in our consideration set.
Hence, the final answer is

$$400 - 1 = 399$$

Example 1.74: Remainders when divided by 6

Repeat the above question with 6 instead of 5.

Number	0	1	2	3	4	5	6	7	8	9	10	11
Remainder	0	1	2	3	4	5	0	1	2	3	4	5
Squares	0	1	4	9	16	25	36	49	64	81	100	121
Remainder	0	1	4	3	4	1	0	1	4	3	4	1
Cubes	0	1	8	27	64	125	216	343	512	729	1000	
Remainder	0	1	2	3	4	5						

Make use of the table above to answer the questions below:

A. How many numbers less than a billion are perfect squares which are two more than a multiple of 6?
B. Consider the six numbers $n, n+1, \dots, n+5$.
C. How many natural numbers less than one thousand are perfect squares which are a multiple of 5?
D. How many perfect cubes less than one million are two more than a multiple of 5?
E. How many natural numbers less than 1000 are such that when divided by 5, the number, its square and its cube all have the same remainder?

Example 1.75: Remainders when divided by 7

Repeat the above question with 7.

Number	0	1	2	3	4	5	6	7	8	9	10	11
Remainder	0	1	2	3	4	5	6	0	1	2	3	4
Squares	0	1	4	9	16	25	36	49	64	81	100	121
Remainder	0	1	4	2	2	1	1	0	1	4	2	2
Cubes	0	1	8	27	64	125	216	343	512	729	1000	
Remainder	0	1	1	6	1	6	6					

Example 1.76: Remainders when divided by 3

Repeat the above question with 3.

Number	0	1	2	3	4	5	6	7	8	9	10
Square	0	1	4	9	16	25	36	49	64	81	100
3	0	1	1	0	1	1	0	1	1	0	1

Suppose the number is a multiple of 3:

$$(3n)^2 = 9n^2 \Rightarrow Multiple\ of\ 3 \Rightarrow Remainder\ Zero$$

Suppose the number is one more than a multiple of 3:

$$(3n+1)^2 = (3n+1)(3n+1) = 9n^2 + 3n + 3n + 1$$
$$Remainder = 1$$

Suppose the number is two more than a multiple of 3:

$$(3n+2)^2 = (3n+2)(3n+2) = 9n^2 + 6n + 6n + 4$$
$$Remainder = 1$$

Suppose the number is three more than a multiple of 3:

$$3n + 3 = 3(n+1) = 3m$$

Part A: Remainder when divided by 4

Number	0	1	2	3	4	5	6	7	8	9	10
Squares	0	1	4	9	16	25	36	49	64	81	100
4	0	1	0	1	0	1	0	1	0	1	0

Suppose the number is one more than a multiple of 4:

$$(4n+1)^2 = (4n+1)(4n+1) = 16n^2 + 4n + 4n + 1$$
$$Remainder = 1$$

$$(4n+2)^2 = (4n+2)(4n+2) = 16n^2 + 4n + 4n + 4$$
$$Remainder = 0$$

$$(4n+3)^2 = (4n+3)(4n+3) = 16n^2 + 4n + 4n + 9$$
$$Remainder = 1$$

Division By	1	8	27	64	125	216	343	512	729	1000
3	1	2	0	1	2	0	1	2	0	1
4	1	0	3	0	1	0	3	0	1	0
5	1	3	2	4	0	1	3	2	4	0

Example 1.77: Triangular Numbers

Triangular numbers are the sum of the first n natural numbers.

$$T_1 = 1$$
$$T_2 = 1 + 2 = 3$$
$$T_3 = 1 + 2 + 3 = 6$$

A. Determine the cyclicity of the pattern when the first few triangular numbers are divided by 3, 4 and 5 respectively.
B. Find the sum of the remainders when the first 100 hundred triangular numbers are divided by 3, 4 and 5 respectively.

Division By	1	3	6	10	15	21	28	36	45	55	66	78	91	105	
3	1	0	0	1	0	0	1	0	0	1					
4	1	3	2	2	3	1	0	0	1	3					
5	1	3	1	0	0	1	3	1	0	0					

B. Mod Notation

Mod arithmetic was first studied systematically by Carl Fredrick Gauss in his book

- Mod arithmetic refers to the remainder when x is divided by y.
- Mod arithmetic works with integers

$$\underbrace{a \div b = c\ Remainder\ d}_{Conventional\ Notation} \Leftrightarrow \underbrace{a \equiv d\ (mod\ b)}_{Mod\ Notation}$$

The symbol ≡ is read “congruent to”.

Example 1.78

Write the following in mod notation:

A. $35 \div 6 = 5\ Remainder\ 5$

$$35 \div 6 = 5\ Remainder\ 5 \Leftrightarrow 35 \equiv 5\ (mod\ 6)$$

Example 1.79: Calculating mod

Evaluate

A. $23\ (mod\ 7)$
B. $82\ (mod\ 9)$
C. $48 (mod\ 7)$

$$23 \equiv \underbrace{7 \times 3}_{0\ (mod\ 7)} + 2 \equiv 2(mod\ 7)$$
$$82 \equiv \underbrace{9 \times 9}_{0\ (mod\ 9)} + 1 \equiv 1(mod\ 9)$$
$$48 \equiv \underbrace{7 \times 7}_{0\ (mod\ 7)} - 1 \equiv -1 \equiv 6(mod\ 7)$$

C. Negative Remainders

Example 1.80
Today is Monday. What is the day 1000 days from now?

You can do this with positive remainders:

$$1000 = 994 + 6 = 7y + 6$$
$$Monday + 7y + 6 = Monday + 6 = Sunday$$

You can do this faster with negative remainders:

$$1001 = 7 \times 11 \times 13$$
$$1000 = 1001 - 1 = 7x - 1$$
$$Monday + 7x - 1 = Monday - 1 = Sunday$$

Example 1.81
A team of policemen have gone for a mountaineering trip. When they form into groups of 7, the last group has 2 people less than the quorum needed to complete the group. How many members does the last group have?

$$The\ last\ group\ will\ have\ 5\ people$$

When the number of policemen is divided by 7, the remainder is

$$-2 \equiv -2 + 7 \equiv 5\ (mod\ 7)$$

Example 1.82
A. A number is 7 less than a multiple of 11. What is the remainder when it is divided by 11?
B. A number is 2 less than a multiple of 10. What is the remainder when it is divided by 10?

Part A
Consider the multiples of 11:

$$11,22,33,44, \ldots$$

Consider numbers which are 7 less than the multiples of 11:

$$4,15,26,37$$

Rewrite each of these numbers:

$$4{,}11 + 4{,}22 + 4{,}33 + 4$$

Each of these numbers when divided by 11 will have remainder 4.

$$-7 \equiv 4(mod\ 11)$$

Part B
A number which is 2 less than a multiple of 10 is:

$$8$$
$$8 \equiv 8(mod\ 10)$$

1.3 Cyclical Patterns

A. Cyclical Patterns

To identify the length of a cycle, we see when it repeats. This is a very general concept, and can be applied to a wide variety of situations, we see below.

Example 1.83

Rakesh hands out a *brown* t-shirt, then a *green* t-shirt, and then a *maroon* t-shirt. He repeats the same colours in the same sequence. What are the colors of the 35^{th} t-shirt, and the 48^{th} t-shirt?
The t-shirts are handed out in a cycle of three (because there are three colours).

	Brown	Green	Maroon
Remainder $n \div 3$	1	2	0
$T-shirt\ Number$	1^{st}	2^{nd}	3^{rd}
	4^{th}	5^{th}	6^{th}
	7^{th}	8^{th}	9^{th}

When n is divided by three, the remainder tells us the color of the t-shirt.

$$\frac{35}{3} = 11\ R2\ (\text{Green t} - \text{shirt}), \qquad \frac{48}{3} = 16\ R0\ (\text{Maroon t} - \text{shirt})$$

Example 1.84

A list of five numbers repeats to form the pattern

5,6,7,8,9,5,6,7,8,9,5,6,7,8,9

What is the 221st number in the pattern? (CEMC Gauss 7 2020/9)

$$221 \equiv 1(mod\ 5) \Rightarrow 5$$

Example 1.85

Laila writes a list of numbers. Her first number is 4. Each number after the first is 7 more than the previous number. Which of the following numbers appears in Laila's list? (CEMC Gauss 7 2020/11)

A. 45
B. 46
C. 47
D. 48
E. 49

Each number is

$$4(mod\ 7)$$

Of the options, the only one which is $4(mod\ 7)$ is Option B.
Hence, option B.

Example 1.86

What is the 1992nd letter in this sequence? (AMC 8 1992/15)

$$ABCDEDCBAABCDEDCBAABCDEDCBAABCDEDC$$

$$\underbrace{ABCDEDCBA}_{Cycle\ 1}\underbrace{ABCDEDCBA}_{Cycle\ 2}ABCDEDCBAABCDEDC$$

$$\frac{1992}{9} = 221\frac{3}{9} \Rightarrow 221\ Complete\ Cycles\ and\ 3\ Extra \Rightarrow C$$

Example 1.87

Ram's television has channels from 2 to 39. If he starts on channel 13, and surfs pushing the channel-up button 407 times, on what channel is the television when he stops? **(NMTC Primary-Final, 2005/14)**

The number of channels is:

$$39 - 2 + 1 = 38\ Channels$$

If you are at the first channel in the sequence (Channel 2), and you press the channel-up button 38 times, you come back to the first channel:

$$2,3,4,\ldots 39$$

In general, pressing the channel-up button 38 times will bring you back to the channel you were originally on. So, we have a cycle of 38, and we can ignore any multiples of 38 in 407.

$$\frac{407}{38} = \frac{380}{38} + \frac{27}{38} = 10 + \frac{27}{38}$$

The 10 does not matter, since for 10 cycles we will come back to Channel 13. Hence, we need to add:

$$13 + 27 = 13 + 26 + 1 = 39 + 1 = 2$$

Example 1.88: Defined Operations

In the set of natural numbers 1,2,3 … we define a new multiplication as follows:

For positive integers m, n, divide mn by 7 and find the remainder k, and we define $m \star n = k$

For example, $102 \star 8 = 4$, since $102 \times 8 = 816 = 7 \times 116 + 4$

Again, $84 \star 5 = 0$, since 84×5 is a multiple of 7 and the product leaves zero remainder when divided by seven.

Now, find an integer k such that $2005 \star k = 1$ in our new multiplication $\star$. **(NMTC Primary/Final 2005/13)**

$$102 \star 8 = \frac{102}{7} \times 8 = \left(14\frac{4}{7}\right) \times 8 = 14 \times 8 + \frac{4}{7} \times 8 = 14 \times 8 + \frac{32}{7} = 14 \times 8 + 4\frac{4}{7}$$

$$2005 \star k = \frac{2005}{7} \times k = \left(286\frac{3}{7}\right)k = 286k + \frac{3k}{7}$$

In 286, we have already carried out the division. So, the division only remains to be carried out in:

$$\frac{3k}{7}\ should\ have\ Remainder\ 1$$

$$k = 1 \Rightarrow \frac{3}{7} \Rightarrow Remainder\ 3$$

$$k = 2 \Rightarrow \frac{6}{7} \Rightarrow Remainder\ 6$$

$$k = 3 \Rightarrow \frac{9}{7} \Rightarrow Remainder\ 2$$

$$k = 4 \Rightarrow \frac{12}{7} \Rightarrow Remainder\ 5$$

$$k = 5 \Rightarrow \frac{15}{7} \Rightarrow Remainder\ 1 \Rightarrow \boldsymbol{Works}$$

Example 1.89

The natural numbers are arranged in a grid as shown below:

	I	II	III	IV	V
	1	2	3	4	5
	6	7	8	9	10
	11	12	13	.	.

A. Which column will each number below appear in:
   I. 27
   II. 98
   III. 46
   IV. 1234
   V. 5656

B. Find the
   I. Largest Number less than 20 that will appear in Column III
   II. Largest two-digit number that will appear in Column I
   III. Smallest three-digit number that will appear in column IV
   IV. Column that the smallest four-digit multiple of seven will appear in

C. Arshi picked a number in the first column of the table. Then she picked a number immediately below and right of the number she picked. She kept doing this till she reached the second-last column of the table. If she adds all the numbers she has got, and divides them by 5, what is the remainder that she will get?

	I	II	III	IV	V
	1	2	3	4	5
	6	7	8	9	10
	11	12	13	.	.
Remainder $n \div 5$	1	2	3	4	0

	I	II	III	IV	V
	$5x+1$				
		$5x+2$			
			$5x+3$		
				$5x+4$	
Remainder $n \div 5$					

$$\frac{(5x+1)+(5x+2)+(5x+3)+(5x+4)}{5} = \frac{20x+10}{5} = 4x+2 \Rightarrow R = 0$$

Note that since $\frac{5x}{5} = x\ R\ 0$, we can ignore each $5x$:

$$Shortcut: \frac{1+2+3+4}{5} = \frac{10}{5} = 2 \Rightarrow R = 0$$

Example 1.90

If this path is to continue in the same pattern:
then which sequence of arrows goes from point 425 to point 427? (AMC 8 1994/15)

Ans =

Example 1.91: Time

A. It is currently 7:00 (24 *hour clock*). What is the time when 26 hours have passed?
B. It is currently 5 *am*. What is the after 2022 hours have passed?

Part A

$$7{:}00 + 26\ hours = 9{:}00$$
$$7 + 26 \equiv 33 \equiv 9\ (mod\ 24)$$

Part B

$$\frac{2022}{24} = \frac{1011}{12} = \frac{337}{4}$$

We don't need to carry out the division with 4, since we only want the time. Use the divisibility for 4 (which is also a remainder test) and check the last two digits:

$$Rem\left(\frac{37}{4}\right) = 1$$

The fractional day is hence

$$\frac{1}{4}\ Day = 6\ Hours$$
$$5\ am + 6\ Hours = 11\ am$$

Example 1.92: Time

A. A contest began at noon one day and ended 1000 minutes later. At what time did the contest end? **(AMC 8 1986/4)**
B. What time was it 2011 minutes after midnight on January 1, 2011? **(AMC 8 2011/5)**

Part A

$$1000\ minutes = \frac{1000}{60} = \frac{100}{6} = 16\frac{4}{6} = 16\frac{2}{3} hours = 16\ hours\ 40\ minutes$$
$$12{:}00\ noon + 16{:}40 = 12{:}00\ midnight + 4{:}40 = 4{:}40\ am$$

Part B

$$2011\ minutes = \frac{2011}{60} = 33\frac{31}{60} = 33\ hours\ 31\ minutes$$
$$12{:}00\ Midnight\ Jan\ 1 + 33{:}31 = 12{:}00\ Midnight\ Jan\ 2 + 9{:}31 = 9{:}31\ \text{am, Jan 2}$$

B. Day of the Week/Year

1.93: Numbering the Days of the Week

Assign a number to each day of the week.

$$Mon = 1, Tue = 2, Wed = 3, Thu = 4, Fri = 5, Sat = 6, Sun = 7$$

Note that after Sunday, we get a cyclical pattern based on the remainder when the day number is divided by 7:

$$Mon = \underbrace{8}_{7+1}, Tue = \underbrace{9}_{7+2}, \ldots, Sun = \underbrace{14}_{14+0}$$

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
	I	II	III	IV	V	VI	VII
	1	2	3	4	5	6	7
	8	9	10	11	12	13	14
	15	16	17	18	19	20	21

Remainder $d \div 7$	1	2	3	4	5	6	0

Example 1.94

Use the fact that days of the week repeat every seven days to answer the following questions.

A. It is Wednesday today. What will be the day five days from now?
B. It is Thursday today. What is the day seven days from now?
C. It is Friday today. What is the day fourteen days from now?
D. If tomorrow is Tuesday, what is the day thirty-two days from now?
E. Today is Friday. What was the day of the week one hundred and twelve days before?

Part A

$$\underbrace{3}_{Wed=3} + 5 = 8 = 7 + 1 = \text{Monday},$$

Part B

$$Thu + 7 = Thu$$

Part C

$$Fri + 14 = Fri$$

Part D

$$Mon + 32 = \underbrace{7 \times 4}_{4\ Weeks} + 4 = \text{Friday}$$

Part E

The pattern also repeats in negative numbers (for example, if you are counting backwards):

$$Mon = -6, Tue = -5, Wed = -4, Thu = -3, Fri = -2, Sat = -1, Sun = 0$$

$$\underbrace{5}_{Today=Friday} - 112 = -107 = \underbrace{-105}_{15\ Weeks} - 2 \equiv -2 \equiv \text{Friday}$$

Part C – Method II: $112 \text{ days prior} = 7 \times 16 = \underbrace{16 \text{ Weeks prior}}_{Day\ will\ not\ change} \Rightarrow \text{Day} = \text{Friday}$

Example 1.95

A. Chris' birthday is on a Thursday this year. What day of the week will it be 60 days after her birthday? (AMC 8 1988/10)
B. Carlos Montado was born on Saturday, November 9, 2002. On what day of the week will Carlos be 706 days old? (AMC 8 2002/5)
C. If February is a month that contains Friday the 13, what day of the week is February 1? (AMC 8 2008/3)

Part A

Ans = Monday

Part B

Ans = Friday

Part C

Ans = Sunday

1.96: Leap Year versus Non-Leap Years

➢ A non-leap year has 28 days in February. A leap year has 29 days in February.

Example 1.97
If February 27, 2013 is a Thursday, what day of the week is 27 March of the same year?

$$Feb\ 27 + 1 = Feb\ 28$$
$$Feb\ 28 + 27 = Mar\ 27$$
$$Total\ Days = 28 = 7 \times 4 = 4\ Weeks$$

Therefore, Feb 27 is also a Thursday.

1.98: Leap Year versus Non-Leap Years
- A year is a leap year when it is a multiple of 4 (2016,2020,2024, …) are all leap years.
- There is one exception to the rule above. If the year is a multiple of 100, then it must be a multiple of 400. (1700,1800,1900) are not leap years. 2000 is a leap year.

Example 1.99

C. Days in a Year

1.100: Leap Year versus Non Leap Years

A non-leap year has 365 days in all. A leap
There are two possibilities for the number of days in a year: $\underbrace{365}_{Non-Leap\ Year}$ and $\underbrace{366}_{Leap\ Year}$.

We can find the change in the day of the week from one year to another by calculating the number of weeks, and extra days:

$$\underbrace{365\ days}_{Non-Leap\ Year(NLY)} = 52\ weeks\ and\ 1\ day, \qquad \underbrace{366\ days}_{Leap\ Year\ (LY)} = 52\ weeks\ and\ 2\ days$$

Example 1.101: Moving forward or backward years
Today is the n^{th} day of 2001 (and it is some day in May), and it is a Thursday.

A. What is the day of the week on the n^{th} day of 2002.
B. What is the day of the week on the n^{th} day of 2004.
C. What is the day of the week on the $(n + 50)th$ day of 2002.

$$A.\underbrace{2001}_{NLY} \rightarrow \underbrace{365\ days}_{52\ weeks,1\ days} \rightarrow 1\ day\ forward \rightarrow \underbrace{Friday}_{Thursday+1\ day}$$
$$B.\ \underbrace{2002}_{NLY,1day} + \underbrace{2003}_{NLY,1\ day} + \underbrace{2004}_{LY,2\ days} \rightarrow 1 + 1 + 2\ days \rightarrow 4\ days \rightarrow Monday$$
$$C.\underbrace{2001}_{NLY} \rightarrow \underbrace{365\ days}_{52\ weeks,1\ days} + \underbrace{50\ days}_{7\ weeks,1\ days} \rightarrow 1 + 1\ day \rightarrow \underbrace{Saturday}_{Thursday+2\ days}$$

Example 1.102: Finding the nature of the year when given the difference in days
Today is the n^{th} day of Year X, (and it is some day in May), and it is a Thursday. The n^{th} day of Year $(X + 1)$ is a Saturday. What kind of year is Year X (leap year or non-leap year)?

S1: $\underbrace{X}_{Year} \rightarrow \underbrace{X+1}_{Year} \rightarrow 2\ days\ forward \rightarrow \underbrace{X+1}_{LY} \rightarrow \underbrace{X}_{NLY}$

Example 1.103: Day of the Week

Ram was born some time between 1st Jan 1995 and 31st December 1999. In the year that Ram was born Jan 1st and Dec 31st were not same days of the week. (Sunday, Monday, Tuesday,...,Saturday are days of the week.) Find the year in which Ram was born. **(NMTC Primary/Final 2005/6)**

In the years 1995, 1996, ... ,1999, the only year that is a leap year is 1996. We check that first since it is different from the other years.

$$\underbrace{366\ Days = 52\ Weeks + 2\ Day}_{Jan\ 1st\ 1996 \rightarrow Jan\ 1st\ 1997} \Rightarrow +2\ Days\ of\ the\ Week$$

The number of days from Jan 1st of one year to Jan 1st of the second year is 366. Therefore, the number of days from Jan 1st 1996 to Dec 31st 1996 is:

$$\underbrace{365\ Days = 52\ Weeks + 1\ Day}_{Jan\ 1st\ 1996 \rightarrow 31st\ Dec\ 1996} \Rightarrow +1\ Day$$

For any other year in the period (not a leap year), we will have:

$$\underbrace{364\ Days = 52\ Weeks}_{Jan\ 1st\ 199X \rightarrow 31st\ Dec\ 199X} \Rightarrow Same\ Day\ of\ the\ Week$$

Challenge 1.104

In year N, the 300^{th} day of the year is a Tuesday. In year $N+1$, the 200^{th} day is also a Tuesday. On what day of the week did the 100^{th} day of year $N-1$ occur? **(AMC 12 2000/18, AMC 10 2000/25)**

We do not know which of these years, if any, is a leap year. So, we first need to decide that:

$$300\ (N) \rightarrow 300(N+1) \Rightarrow \left\{\underbrace{365}_{NLY}, \underbrace{366}_{LY}\right\}\ days$$

Subtract 100 days:

$$Day\ 300\ (Year\ N) \rightarrow Day\ 200(Year\ N+1) \Rightarrow \{265, \mathbf{266}\}\ days$$

Since the 300th day of year N, and the 200th day of year $N+1$ are both Tuesdays, the number of days in between must be a multiple of 7.
Apply the test of divisibility of 7:

$$265 \rightarrow 26 - 10 = 16 \rightarrow Not\ Divisible, \qquad 266 \rightarrow 26 - 12 = 14 \rightarrow Divisible$$

$$266\ days \Rightarrow \underbrace{(N+1)}_{Leap\ Year} \Rightarrow \underbrace{N, N-1}_{Not\ Leap\ Years}$$

$$300th\ Day\ of\ Year\ N - 300\ Days = 365th\ Day\ of\ Year\ N-1$$
$$365th\ Day\ of\ Year\ (N-1) - 265\ Days = 100th\ Day\ of\ Year\ N-1$$
$$-300 - 265 = -565 = -567 + 2 \equiv +2 \Rightarrow Tuesday + 2 \Rightarrow Thursday$$

D. Analysing Days in a Month

Example 1.105

On this monthly calendar, the date behind one of the letters is added to the date behind C. If this sum equals the sum of the dates behind A and B, then the letter is (AMC 8 1990/10)

Tue	Wed	Thu	Fri	Sat

		C	A	
		Q		
S	B	P	T	R

Logic

C is one less than A, hence for the sum to the same, the other letter must be one more than B. Hence, the letter must be P.

Algebra

$$x + C = A + B \Rightarrow x + (A - 1) = A + B \Rightarrow x - 1 = B \Rightarrow x = B + 1 = P$$

Example 1.106

In a certain year, January had exactly four Tuesdays and four Saturdays. On what day did January 1 fall that year? **(AMC 8 1985/20)**

Suppose the first day of the month is a Tuesday. What does this give us? Let us make the Calendar

Mon	Tue	Wed	Thu	Fri	Sat	Sun
	1				5	
	8				12	
	15				19	
	22				26	
	29	30	31			

This gives us five Tuesdays (one more than what we want).
So, we can fix the problem by moving the first day of the month one day forward:

So, then we get the calendar below. This gives us four Tuesdays, and four Saturdays.

Mon	Tue	Wed	Thu	Fri	Sat	Sun
		1			4	
	7				11	
	14				18	
	21				25	
	28	29	30	31		

Example 1.107

Classify the months of the year according to the number of days which repeat five times.

28 Days No Day occurs Five Times February of a Non-Leap Year								**29 Days One Day occurs Five Times February of Leap Year**						
Mon	Tue	Wed	Thu	Fri	Sat	Sun		Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7		1	2	3	4	5	6	7
8	9	10	11	12	13	14		8	9	10	11	12	13	14
15	16	17	18	19	20	21		15	16	17	18	19	20	21
22	23	24	25	26	27	28		22	23	24	25	26	27	28
								29						

30 Days Two Days occurs Five Times April, June, September, November								31 Days Days occurs Five Times Jan, Mar, May, July, Aug, Oct, Dec						
Mon	Tue	Wed	Thu	Fri	Sat	Sun		Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	7		1	2	3	4	5	6	7
8	9	10	11	12	13	14		8	9	10	11	12	13	14
15	16	17	18	19	20	21		15	16	17	18	19	20	21
22	23	24	25	26	27	28		22	23	24	25	26	27	28
29	30							29	30	31				

Example 1.108

In a February of a leap year, Thursday occurs five times.

A. Thomas likes to have an ice cream on Thursday. What are the dates in February that he had an ice cream?
B. Thomas's sister likes to go ice skating on Wednesdays. What dates did she ice skate in February?

Example 1.109

A. Find the remainders when the dates in a month are divided by 7.
B. In the previous example, you classified months based on the number of days as having 28 days, 29 days, 30 days or 31 days. For each kind of month, state how many remainders repeat five times.

Remainders						
Mon	Tue	Wed	Thu	Fri	Sat	Sun
1	2	3	4	5	6	0
1	2	3	4	5	6	0
1	2	3	4	5	6	0
1	2	3	4	5	6	0
1	2	3				

28 *Days*: *Zero Times*
29 *Days*: *One Time*
30 *Days*: *Two Times*
31 *Days*: *Three Times*

Challenge 1.110

Suppose July of year N has five Mondays. Which of the following must occurs five times in the August of year N? (Note: Both months have 31 days.) **(AMC 10B 2002/8, AMC 12B 2002/8)**

July

Version 1		Version 2		Version 3		

Mon	Tue	Wed	Thu	Mon	Tue	Wed		Mon	Tue	
1				2				3		
8				9				10		
15				16				17		
22				23				24		
29	30	31	1st	30	31	1st		31	1st	

As seen above, the only possible dates for the first Monday of July to occur are 1st, 2nd and 3rd. For example, if the first Monday of July were to occur on 4th of July, then there would only four Mondays in July $(4th, 11th, 18th, 25th)$.

Given the above dates for the first day of July, we are able to calculate the corresponding days for the first day of Aug as one of $(Thursday, Wednesday\ and\ Tuesday)$.

We now tabulate these possibilities for the first day of August

Version 1				Version 2				Version 3		
Thu	Fri	Sat		Wed	Thu	Fri		Tue	Wed	Thu
1	2	3		1	2	3		1	2	3
8	9	10		8	9	10		8	9	10
15	16	17		15	16	17		15	16	17
22	23	24		22	23	24		22	23	24
29	30	31		29	30	31		29	30	31

Independent of which Version happens to be the actual case, Thursday happens five times in all the cases. Therefore, the right answer is Thursday.

E. Up and Down Cycles

A number of cycles have an up and down pattern, rather than a clean break and resumption of the old pattern. Some of examples of these can be:

- 9 Bottles on a wall: Counting in the following manner
  $$\{1,2,3,4,5,6,7,8,9,8,7,6,5,4,3,2 \ldots\ldots\}$$
- A doctor visiting the floors of a hospital in the following manner
  $$\{Ground, 1st, 2nd, 3rd, 2nd, 1st, Ground, 1st, 2nd, \ldots\ldots\}$$

Example 1.111: Counting on the fingers of a hand

Vihaan is counting on the fingers (and thumb) of his hand:
Method I: Start with the thumb, go to the index finger, middle finger, ring finger and little finger. After reaching the little finger, start again with the thumb.
Method II: Start with the thumb, go to each finger as in the previous method, but then from the little finger start backwards.
Which digit (of the hand) will the counting finish if he counts to the 35th finger (under each of the methods)?

Method I: There are five fingers in the cycle. So, the length of the cycle is five.

	Thumb	Index	Middle	Ring	Little
Remainder$\left(\frac{n}{5}\right)$	1	2	3	4	0

$$\frac{35}{5} = 7\ R0 \text{ (Little finger)}$$

Method II

Solution 1: When he reaches the thumb again, he will count nine. This means the cycle is 8.
Solution 2: There are four jumps forward to reach the little finger, and four jumps backward to again reach the thumb – for a total of eight jumps.
Verification: The thumb is reached when counting 1, 9, 17, 25.
The length of the cycle is the difference between any two of these numbers $= 9 - 1 = 8$

	Thumb	Index	Middle	Ring	Little	
Remainder$\left(\frac{n}{8}\right)$	1	2	3	4	5	→ (Going forward)
Remainder$\left(\frac{n}{8}\right)$		0	7	6		← (Going Backward)

$$\frac{35}{8} = Q4\ R3 \text{ (Middle Finger, Going Forward)}$$

1.4 Finding Remainders

A. Finding Remainders

We can find remainders of many numbers using their tests of divisibility. For many numbers, the test of divisibility is actually a test of remainders. If the remainder is zero, then the number is divisible.

Divisibility	Divisibility Test	Remainder Test
2,4,8, … , 2^n	Divide last n digits by 2^n	The remainder on dividing last n digits is the same as the remainder when dividing x
3,9	Sum of digits should be divisible by 9	The remainder when dividing sum of digits by 3(or 9), is the same as the remainder when dividing x by 3(or 9).
11	Difference of digits in odd positions and digits in even positions should be divisible by 11.	The difference is also the remainder when x is divided by 9.

Example 1.112

A. When 487512 is divided by 5, what is the remainder?
B. Find the remainder when 84,345 is divided by 2.
C. Find the remainder when 2410 is divided by 4.
D. Find the remainder when 523,791 is divided by 11.

Part A

Rewrite the given number:

$$487512 = 487510 + 2 = (48751)(2)(5) + 2$$

Divide the above by 5:

$$\frac{(48751)(2)(5)}{5} + \frac{2}{5} = (48751)(2) + \frac{2}{5}$$

Part B

$$84{,}345 = 84{,}340 + 5$$

Divide by 2:

$$\frac{84{,}340}{2} + \frac{5}{2} \equiv 0 + 1 \equiv 1(mod\ 2)$$

Alternate Method

We only need to check the last digit:

$$5 \div 2\ has\ remainder\ 1$$

$$\therefore 84{,}345 \div 2 \; has \; remainder$$

We can write this in *mod* notation as:

$$5 \equiv 1(mod\ 2) \Rightarrow 84{,}345 \equiv 1(mod\ 2)$$

Part C

$$\frac{2410}{4} = \frac{2400}{4} + \frac{10}{4} = 600 + 2\frac{2}{4} \Rightarrow Remainder\ is\ 2$$

Alternate Method

We need to check the last two digits.

$$10 \equiv 2(mod\ 4) \Rightarrow 2410 \equiv 2(mod\ 4)$$

Part D

$$523{,}791$$
$$Digits\ in\ Odd\ Positions\ from\ the\ right: 2 + 7 + 1 = 10$$
$$Digits\ in\ Even\ Positions\ from\ the\ right: 5 + 3 + 9 = 17$$
$$Difference = 10 - 17 = -7 \equiv 4(mod\ 11)$$

Example 1.113

A. Find the remainder when 510234 is divided by 8.
B. When 34517 is divided by 3, what is the remainder?
C. When 127,957 is divided by 9, what is the remainder?

Part A

$$234 \equiv 2(mod\ 8) \Rightarrow 510{,}234 \equiv 2(mod\ 8)$$

Part B

$$3 + 4 + 5 + 1 + 7 = 20 \equiv 2(mod\ 3) \Rightarrow 34517 \equiv 2(mod\ 3)$$
$$\frac{34517}{3} = \frac{34515}{3} + \frac{2}{3} = x + \frac{2}{3}$$

Part C

$$1 + 2 + 7 + 9 + 5 + 7 = 31 \equiv 4(mod\ 9) \Rightarrow 127{,}957 \equiv 4(mod\ 9)$$

Example 1.114

When the number 1204851 is divided by 2^n,where n is a whole number from 0 to 5, the remainder is 3. Find the sum of possible values of n.

$$n = 0 \Rightarrow 2^0 = 1 \Rightarrow 1204851 \equiv 0\ (mod\ 1)$$
$$n = 1 \Rightarrow 2^1 = 2 \Rightarrow 1204851 \equiv 1\ (mod\ 2)$$
$$n = 2 \Rightarrow 2^2 = 4 \Rightarrow 1204851 \equiv 3\ (mod\ 4) \Rightarrow \boldsymbol{Valid}$$
$$n = 3 \Rightarrow 2^3 = 8 \Rightarrow 1204851 \equiv 3\ (mod\ 8) \Rightarrow \boldsymbol{Valid}$$
$$n = 4 \Rightarrow 2^4 = 16 \Rightarrow 1204851 \equiv 3\ (mod\ 16) \Rightarrow \boldsymbol{Valid}$$
$$n = 5 \Rightarrow 2^5 = 32 \Rightarrow 1204851 \equiv 19\ (mod\ 32) \Rightarrow \boldsymbol{Not\ Valid}$$

$$51 - 3 = 48 = 3 \times 16$$

Example 1.115

A. Find the largest possible remainder when $35x$ is divided by 2, where x is a natural number.
B. Let $a = 10x, b = 3y$. Find the largest possible remainder when ab is divided by 12.

Part A

$$35x = 34x + x$$

Divide the above by 2:

$$\frac{34x}{2}+\frac{x}{2}=17x+\frac{x}{2}$$

Hence, we need to find the maximum remainder for $\frac{x}{2}$, which is 1.

Part B

$$ab=(10x)(3y)=30xy=24xy+6xy$$

Divide it by 12:

$$\frac{24xy}{12}+\frac{6xy}{12}=2xy+\frac{6xy}{12}$$

If either x or y is even, the remainder is zero:

$$\frac{6xy}{12}=\frac{6(2n)(y)}{12}=nxy$$

If both x and y are odd, then the remainder will be 6.

Maximum possible remainder is 6.

Example 1.116

B. Not All Divisibility Tests are Remainder Tests

The test of divisibility by seven is not a remainder test. Subtract twice the last digit of a number from the truncated number (truncated number is the number without the last digit)

$$Eg: 245 \to 24-\underbrace{5\times 2}_{Last\ Digit(5)\times 2}=24-10=\underbrace{14}_{Divisible\ by\ 7}\Rightarrow 245\ divisible\ by\ 7$$

Example 1.117: Finding Remainders

Find the remainders indicated on each element of the set $\left\{\frac{234589}{10},\frac{9741}{100},\frac{289456}{4},\frac{2891745}{11}\right\}$

$$R\left(\frac{234589}{10}\right)=Last\ Digit=9, R\left(\frac{9741}{100}\right)=Last\ Two\ Digits=41, R\left(\frac{289456}{4}\right)=R\left(\frac{56}{4}\right)=0$$

We use the test of divisibility by 11, but the digits in the even positions (from the rightmost) need to be subtracted (not added).

Example 1.118: Finding Remainders on divisibility by 11

Find the remainders indicated on each element of the set

$$\left\{\frac{2{,}891{,}745}{11},\frac{891745}{11}\right\}$$

$$R\left(\frac{2891745}{11}\right)=\underbrace{23}_{2+9+7+5}-\underbrace{13}_{8+1+4}=10$$

$$\underbrace{R\left(\frac{891745}{11}\right)=\underbrace{21}_{9+7+5}-\underbrace{13}_{8+1+4}=8}_{13-21=-8\equiv 3\ would\ be\ wrong}$$

C. Basics

In many situations, the complexity of a calculation prevents from getting the answer easily. However, we can derive information about the answer which can be quite useful.
These questions can very troublesome without the appropriate properties.

Example 1.119: Calculating the Last Digit

Find the remainder when $238{,}917{,}349^2$ is divided by 10.
Finding the remainder is the same as finding the last digit.

Method I: Multiplication Algorithm

The last digit of a number is going to depend only on the two units digits of the numbers being multiplied.

Carryover								8	
	2	3	8	9	1	7	3	4	9
×	2	3	8	9	1	7	3	4	9
									1
									0
								0	0
							0	0	0
						More Zeros			
					Total				1

We can see why from the partial multiplication of 238917349, where the units digit only depends on the multiplication of respective units digits. All other numbers below are zeroes.

Method II: Mod Arithmetic

$$238917349^2 \equiv \underbrace{238917349}_{\equiv 9\ (mod\ 10)} \times \underbrace{238917349}_{\equiv 9\ (mod\ 10)} \equiv \underbrace{9 \times 9}_{Distributive\ Property} \equiv (-1)(-1) \equiv 1 (mod\ 10)$$

D. Calculating the last two digits

The ideas involved in calculating the last two digits are similar to those for calculating the last digit. The calculations are a little more involved.

Example 1.120: Calculating the Last Two Digits

Find the remainder when $238{,}917{,}349^2$ is divided by 100.
Finding the remainder is the same as finding the last two digits.

Method I: Multiplication Algorithm

The last two digits of a number are going to depend only on last two digits of the numbers being multiplied.

							3		
Carryover							4	8	
	2	3	8	9	1	7	3	4	9
×	2	3	8	9	1	7	3	4	9
								4	1
								6	0
								0	0
							0	0	0
						More Zeros			
					Carryover		1		
					Total			0	1

We can see why from the partial multiplication of 238917349, where the last two digits only depend on the multiplication of last two digits. All other numbers below are zeroes.

Method II: Mod Arithmetic

$$238917349^2 \equiv \underbrace{238917349}_{\equiv 49\ (mod\ 10)} \times \underbrace{238917349}_{\equiv 49\ (mod\ 10)} \equiv \underbrace{49 \times 49}_{Distributive\ Property} \equiv 7^2 \times 7^2 \equiv 7^4 \equiv 2401 \equiv 01(mod\ 100)$$

Example 1.121

The product of the two 99-digit numbers 303,030,303,…,030,303 *and* 505,050,505,…,050,505 has thousands digit A and units digit B. What is the sum of A and B? **(AMC 8 2007/18)**

Ans = 8

E. Units Digit of Perfect Squares

Are 12,12,201 and 12,12,202 are perfect squares. We can't check their square roots without a calculator. But, we can see which are the possible Units Digits.

11	121	21	441
12	144	22	484
13	169	23	524
14	196	24	576
15	225	25	625
16	256	26	676
17	289	27	729
18	324	28	784
19	361	29	841
20	400	30	900

Last Digit of			
No.	Square	No.	Square
0	0		
1	1	9	1
2	4	8	4
3	9	7	9
4	6	6	6
5	5		

$$0, \underbrace{1,4,9,6}_{Set\ 1}, 5, \underbrace{6,9,4,1}_{Set\ 2}$$

1.122: Last Digit Candidates for Perfect Squares

Certain digits can never be the last digit for a perfect square.

$$\underbrace{\{2,3,7,8\}}_{\text{Can never be the last digit of a perfect square}} \quad , \quad \underbrace{\{0,1,4,5,6,9\}}_{\text{Can be the last digit of a perfect square}}$$

This test is used for rejection, not selection. If a digit falls among the set of digits on the right, it is not necessary that it is a perfect square.

Example 1.123: Rejecting Perfect Square Candidates

One of the following numbers is a perfect square? Which one is it?

$$p = 2{,}46{,}713, \quad q = 5{,}49{,}081, \quad r = 3{,}33{,}222, \quad s = 9{,}16{,}787$$

3, 2 and 7 can never be the last digit of a perfect square.

Since one of the numbers is a perfect square, it must be 5,49,081.

Example 1.124: Rejecting Perfect Square Candidates

Which of the following could not be the unit's digit [one's digit] of the square of a whole number? **(AMC 8 1990/4)**

Ans = 8

F. Estimating Square Roots

It is possible to estimate the range (most significant digit) of a square root by looking at the squares between which it lies.
The table above can be used to identify the unit's digit (least significant digit), or at least bring down the number of possibilities to maximum of 2.

Example 1.125: Estimating the square root of a perfect square

We saw in the previous question that 5,49,081 is a perfect square. Calculate its square root.

Unit's Digit: *From the table only* 1 *and* 9 *are possible*.
Hundred's Digit: $\underbrace{4{,}90{,}000}_{700^2} < 5{,}49{,}081 < \underbrace{6{,}40{,}000}_{800^2}$
We will need to do some guesswork for the tens's digit, which should be near the middle of 0-9, because 5,49,081 is roughly halfway between 4,90,000 and 6,40,000.

After some trial and error, we find that

$$741^2 = 5{,}49{,}081$$

G. Cyclicity of Digits Under Multiplication

The table that we calculated for the last digit of a perfect square can be extended to higher powers. Looking at the table, we find that the powers repeat in a pattern.

The length of the pattern of a number is called its cyclicity.

				Last Digit of No.	Last Digit of				Cyclicity
					Square	Cube	4th Power	Pattern	
0	0	0	0	0	0	0	0	0	1
1	1	1	1	1	1	1	1	1	1
2	4	8	16	2	4	8	6	2, 4, 8, 6	4
3	9	27	81	3	9	7	1	3, 9, 7, 1	4
4	16	64	256	4	6	4	6	4, 6	2
5	25	125	625	5	5	5	5	5	1
6	36	216	1296	6	6	6	6	6	1
7	49	343	2401	7	9	3	1	7, 9, 3, 1	4
8	64	512	4096	8	4	2	6	8, 4, 2, 6	4
9	81	729	6561	9	1	9	1	9, 1	2

Example 1.126: Calculating the last digit

Calculate the first eight powers of two, and show that the last digit as per actual calculation matches the last digit as predicted by the pattern.

$n(mod\ 4)$	2^n	x	2^n	x	Last Digit
1	2^1	2	2^5	32	2
2	2^2	4	2^6	64	4
3	2^3	8	2^7	128	8
0	2^4	16	2^8	256	6

H. Calculating the Last Digit

We can use the table above to calculate the last digit for numbers raised to any power.

Example 1.127

If we multiply 2 by itself repeatedly four times, we get $2 \times 2 \times 2 \times 2 = 16$, and its units digit is 6. Suppose we multiply 2 with itself repeatedly 2005 times we get a big number B. What is the unit digit of B? **(NMTC Final/Primary 2005/3)**

$$2^{2005} = 2^{2004} \times 2 \Rightarrow Units\ Digits = 2$$

Example 1.128

A. When 1999^{2000} is divided by 5, the remainder is **(AMC 8 1999/24)**
B. What is the units digit of $19^{19} + 99^{99}$? **(AMC 8 2000/14)**

Odd	Even
Last Digit 9	*Last Digit* 1
$9^1 = 9$	$9^2 = 81$
$9^3 = 729$	$9^4 = 6561$

Odd Powers of 9 have units digit 9, even powers of 9 have units digit 1.

Part A

$$1999^{2000} \Rightarrow 2000\ is\ even, hence\ the\ last\ digit\ is\ 1.$$

When you divide a number with last digit 1, by 5, the remainder is

1.

Part B

$$19^{99} \Rightarrow 99\ is\ odd \Rightarrow Last\ Digit\ 9$$
$$99^{99} \Rightarrow 99\ is\ odd \Rightarrow Last\ Digit\ 9$$

Hence, the last digit we want is

$$9 + 9 = 18 \Rightarrow Last\ Digit\ 8$$

Example 1.129: Creating Zeroes

The unit's digit (one's digit) of the product of any six consecutive positive whole numbers is **(AMC 8 1994/6)**

Any two consecutive whole numbers will always have an even number.
Any six consecutive whole numbers will always have a five.

Their product will always be

$$5 \times Even = Some\ Number\ ending\ in\ Zero$$
$$Ans\ =\ 0$$

Example 1.130

Two natural numbers, p and q, do not end in zero. The product of any pair, p and q, is a power of 10 (that is, 10, 100, 1000, 10 000 , ...). If $p > q$, the last digit of $p - q$ cannot be **(Gauss Grade 7 1998/25)**

$$pq = 10^n = (2 \times 5)^n = 2^n \times 5^n$$

Since $p > q$:

$$p = 5^n, q = 2^n$$

$$5-2=3$$
$$5-4=1$$
$$15-8=7$$
$$15-6=9$$

And the cycle repeats. Only the digit 5 does not occur. Hence, the last digit cannot be:

5

I. Applications

Example 1.131: Calculating the Last Digit

All of the even numbers from 2 to 98 inclusive, excluding those ending in 0, are multiplied together. What is the rightmost digit (the units digit) of the product? (AMC 8 1997/25)

Ans = 6

Consider the 1-digit numbers:

$$2\times4\times6\times8=384\Rightarrow Last\ Digit=4$$

Like the above, there will nine other sets of numbers, each of will have last digit

$$2\times4\times6\times8=384\Rightarrow Last\ Digit=4$$

Hence, we want the last digit of

$$4^{10}=(4^2)^5=(16)^5\Rightarrow Last\ Digit\ 6$$

Example 1.132: Calculating the last digit

Find the last digit of $2^x+3^x+4^x+7^x+8^x+9^x, x=2020$.

First classify the numbers

$$\underbrace{2,3,7,8}_{Cyclicity\ of\ 4}\quad,\quad\underbrace{4,9}_{Cyclicity\ of\ 2}$$

$$2020\ (mod\ 4)=0\Rightarrow \underbrace{LD(2^{2020})}_{=6}+\underbrace{LD(3^{2020})}_{=1}+\underbrace{LD(7^{2020})}_{=1}+\underbrace{LD(8^{2020})}_{=6}\equiv 6+1+1+6\equiv 14\equiv 4$$

$$2020\ (mod\ 2)=0\Rightarrow \underbrace{LD(4^{2020})}_{=6}+\underbrace{LD(9^{2020})}_{=1}\equiv 6+1\equiv 7$$

$$Final\ Mod\equiv 4+7\equiv 11\equiv 1$$

J. Cyclicity of 7

Last Two Digits	7	49	43	01
Power of 7	7^1	7^2	7^3	7^4

Example 1.133

What is the tens digit of 7^2011? (AMC 8 2011/22)

$$7^{2011}=7^{2008}\times7^3\Rightarrow Tens\ Digit=4$$

K. Cyclicity of 2

02	04	08	16	32	64	28	56	12	24	48	96	92	84	68	36	72	44	88	76	52	4
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	

L. Multiplying Remainders

Example 1.134

Suppose the English Alphabet letters $A, B, C, \dots, Z$ are denoted by the remainders obtained on dividing the numbers $2^0, 2^1, 2^2, \dots, 2^{25}$ respectively by 29, then the letter "K" would be denoted by: (JMET 2011/88)

Logic

$$\frac{2^{10}}{29} = \frac{2^5 \times 2^5}{29}$$

To find the remainder we can find the individual remainders, and multiply:

$$\frac{2^5}{29} = \frac{32}{29} = 1\frac{3}{29} \Rightarrow Remainder = 3$$
$$3 \times 3 = 9$$

Mod Arithmetic

$$2^{10} \equiv (2^5)^2 \equiv (32)^2 \equiv 3^2 \equiv 9 \ (mod\ 29)$$

M. Remainders of Factors

Example 1.135

A number when divided by 255 gives a remainder 23. What will be the remainder when the same number is divided by 17?

We want to divide a number of the form $255x + 23$ by 17:

$$\frac{255x + 23}{17} = \frac{255x}{17} + \frac{23}{17} = 15x + 1 + \frac{6}{17}$$

And, hence the final remainder is 6.

N. HCF/LCM with Remainders

Example 1.136

The letters A, J, H, S, M, E and the digits 1, 9, 8, 9 are "cycled" separately as follows and put together in a numbered list:\[\begin{tabular}[t]{lccc} & & AJHSME & 1989 \\ & & & \\ 1. & & JHSMEA & 9891 \\ 2. & & HSMEAJ & 8919 \\ 3. & & SMEAJH & 9198 \\ & & ..... & \end{tabular}\]
What is the number of the line on which AJHSME 1989 will appear for the first time? (AMC 8 1989/22)
Ans = 12

Example 1.137

On this monthly calendar, the date behind one of the letters is added to the date behind C. If this sum equals the sum of the dates behind A and B, then the letter is (AMC 8 1990/10)

Tues.	Wed.	Thurs.	Fri.	Sat.
		C	A	
		Q		
S	B	P	T	R

		C	$C+1$	
		$C+7$		
$C+12$	$C+13$	$C+14$	$C+15$	$C+16$

$$A+B=(C+1)+(C+13)=2C+14$$
$$C+X=2C+14 \Rightarrow X=C+14=P$$

Challenge 1.138

Seven students count from 1 to 1000 as follows:
•Alice says all the numbers, except she skips the middle number in each consecutive group of three numbers. That is, Alice says 1, 3, 4, 6, 7, 9, ..., 997, 999, 1000.
•Barbara says all of the numbers that Alice doesn't say, except she also skips the middle number in each consecutive group of three numbers.
•Candice says all of the numbers that neither Alice nor Barbara says, except she also skips the middle number in each consecutive group of three numbers.
•Debbie, Eliza, and Fatima say all of the numbers that none of the students with the first names beginning before theirs in the alphabet say, except each also skips the middle number in each of her consecutive groups of three numbers.
•Finally, George says the only number that no one else says.
What number does George say? **(AMC 10A 2011/23)**

Alice does not say the numbers

$$2,5,8,\ldots \Rightarrow Remainder\ 2\ when\ divided\ by\ 3$$

Barbara does not say the numbers:

$$5,14,\ldots \Rightarrow Remainder\ 2+3=5\ when\ divided\ by\ 9$$

Candice does not say the numbers:

$$14,41,\ldots \Rightarrow Remainder\ 5+9=14\ when\ divided\ by\ 27$$

Debbi does not say the numbers:

$$41,122\ldots \Rightarrow Remainder\ 14+27=41\ when\ divided\ by\ 81$$

Eliza does not say the numbers:

$$122,365\ldots \Rightarrow Remainder\ 41+81=122\ when\ divided\ by\ 243$$

Fatima does not say the numbers:

$$365,1094,\ldots \Rightarrow Remainder\ 122+243=365\ when\ divided\ by\ 729$$

We now have only one number less than 1000, which is 365.
This is the answer.

A. Diophantine Equations

1.139: Diophantine Equation

- A Diophantine equation is an equation that is to be solved in natural numbers or in integers.
- Usually, a Diophantine equation has more variables than equations.
  - ✓ If natural numbers are allowed, there will (usually) be multiple solutions
  - ✓ If integers are allowed, there will (usually) be infinite solutions.

- The equations are Diophantine after Diophantus, a Greek mathematician who studied equations.

Example 1.140

Find the solutions to $x + 3y = 100$ if x and y are natural numbers. Count the number of solutions also.

Trial and Error

$x = 1$:

$$1 + 3y = 100 \Rightarrow 3y = 99 \Rightarrow y = 33$$

$x = 2$:

$$2 + 3y = 100 \Rightarrow 3y = 98 \Rightarrow y = \frac{98}{3} \Rightarrow Not\ Valid$$

$x = 3$:

$$3 + 3y = 100 \Rightarrow 3y = 97 \Rightarrow y = \frac{97}{3} \Rightarrow Not\ Valid$$

$x = 4$:

$$4 + 3y = 100 \Rightarrow 3y = 96 \Rightarrow y = 32$$

Solution using Multiples

$$x + 3y = 100$$

$$\underbrace{x}_{Remainder} + \underbrace{3y}_{\substack{Multiple \\ of\ 3}} = \underbrace{99}_{\substack{Multiple \\ of\ 3}} + \underbrace{1}_{Remainder}$$

The values that work for x are one more than a multiple of 3:

$$x \in \{1,4,7,10,13, \dots ,97\}$$

We can rewrite this more formally as:

$$x \in \{1 + 3k, 0 \leq k \leq 33\}\ where\ k \in \mathbb{W}$$

$$y \in \{33,32,31, \dots ,1\} = \{1 \leq y \leq 33\}\ where\ y \in \mathbb{N}$$

We can use the above to write ordered pairs (x, y) for the solutions:

$$(1,33), (4,32), (7,31), \dots , (97,1) \Rightarrow 33\ Numbers$$

Solution using Rearrangement

Instead of solving for many values, we can solve the equation for y, in general:

$$x + 3y = 100$$

$$3y = 100 - x$$

$$y = \frac{100 - x}{3}$$

Since $y \in \mathbb{N}$, we want the LHS to be a natural number. Hence, the RHS must also be a natural number. In the current form, it is difficult to decide what values give a natural. Hence, we rewrite it:

$$y = \frac{99 + 1 - x}{3} = \frac{99}{3} + \frac{1 - x}{3} = 33 + \frac{1 - x}{3}$$

The values that work for x are when x is one more than a multiple of 3. And then the solution proceeds as before.

Example 1.141

Find the solutions to the following equations in natural numbers. Write your answers as ordered (x, y) pairs. Count the number of solutions also.

A. $x + 4y = 200$
B. $x + 2y = 50$
C. $x + 7y = 500$

$$(4,49), (8,48), (12,47), \dots , (196,1) \Rightarrow 49\ Solutions$$

$$(2,24), (4,23), (6,22), \dots , (48,1) \Rightarrow 24\ Solutions$$

$$(3,71), (10,70), (17,69), \dots (493,1) \Rightarrow 71\ Solutions$$

Example 1.142

Solve the following equation for natural number values of x and y. Write your answers as ordered (x, y) pairs. Find the number of solutions also.

$$2x - 3y = 101$$

Using Parity

Since $2x$ is even, we can solve this using parity (odd and even):

$$\underbrace{2x}_{Even} - \underbrace{3y}_{\substack{Must\ be \\ Odd}} = \underbrace{101}_{Odd}$$

From the above, we can conclude that:

$$\underbrace{3}_{Odd} \times \underbrace{y}_{\substack{Must\ be \\ Odd}} = Odd$$

The smallest odd number for y that we can try:

$y = 1 \Rightarrow 2x - 3(1) = 101 \Rightarrow 2x = 104 \Rightarrow x = 52$

$y = 3 \Rightarrow 2x - 3(3) = 101 \Rightarrow 2x = 110 \Rightarrow x = 55$

$(52,1), (55,2), (58,3), \ldots \Rightarrow Infinite\ Solutions$

Using Rearrangement

$$2x = 101 + 3y$$

$$x = \frac{101 + 3y}{2} = \frac{100}{2} + \frac{1 + 3y}{2} = 50 + \frac{1 + 3y}{2}$$

$$\underbrace{1}_{Odd} + \underbrace{3y}_{\substack{Must \\ be\ Odd}} = Even$$

Example 1.143

60 pennies were used to buy some twopenny stamps, six times as many penny stamps, and the rest twopence-halfpenny stamps. Find the number of stamps of each type?

B. Remainders of Perfect Squares

Example 1.144

Remainders of perfect squares when divided by 3.

Consider numbers with respect to their remainders when they are divided by 3. There are exactly three different kinds of numbers

$$3k: Divisible\ by\ 3$$
$$3k + 1$$
$$3k + 2$$

$$(3k)^2 = 9k^2 \Rightarrow Multiple\ of\ 3$$
$$(3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1 \Rightarrow Remainder\ of\ 1$$
$$(3k + 2)^2 = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1 = 3(3k^2 + 4k + 1) + 1 \Rightarrow Remainder\ of\ 1$$

Example 1.145

Remainders of perfect squares when divided by 4.

Consider numbers with respect to their remainders when they are divided by 4. There are exactly three different kinds of numbers

$$4k: Divisible\ by\ 3$$
$$4k + 1$$
$$4k + 2$$
$$4k + 3$$

$$(4k)^2 = 16k^2 \Rightarrow Multiple\ of\ 4$$
$$(4k + 1)^2 = 16k^2 + 8k + 1 \Rightarrow Remainder\ of\ 1$$
$$(4k + 2)^2 = 16k^2 + 16k + 4 \Rightarrow Remainder\ of\ 0$$
$$(4k + 3)^2 = 16k^2 + 24k + 9 \Rightarrow Remainder\ of\ 1$$

C. Application: Divisibility

Example 1.146

Explain why the test of divisibility by 8 works.

$$xyz \dots pqrs$$

Write the number in expanded notation:

$$xyz \dots p \times 1000 + qrs$$
$$= 8(xyz \dots p \times 125) + qrs$$

The first term is divisible by 8. Hence, we only to check divisibility for the second term, which represents the last three digits.

2. Mod Arithmetic

2.1 Mod Arithmetic-I: Addition and Subtraction

A. Some Basic Example

Example 2.1: Clock Arithmetic

$$Use\ 24-hour\ clock$$

A. What is the time 2 hours after 23:00?
B. What is the time 24 hours after 23:00?
C. What is the time 242 hours after 23:00?

$$23{:}00 + 2{:}00 = 25{:}00 = 24{:}00 + 1{:}00 = 1{:}00$$
$$23{:}00 + 24{:}00 = 23{:}00$$
$$23{:}00 + 242{:}00 = 24{:}00 + 241{:}00 = \underbrace{24{:}00}_{One\ Day} + \underbrace{240{:}00}_{Ten\ Days} + 1{:}00 = 1{:}00$$

Example 2.2

A. Today is Monday. What is the day 4 days from now?
B. Today is Monday. What is the day 7 days from now?
C. Today is Monday. What is the day 700 days from now?
D. Today is Monday. What is the day 701 days from now?

$$Mon + 4 = FridayMon + 7 = Monday$$
$$Mon + 700 = Monday$$
$$Mon + 701 = Mon + 1 = Tuesday$$

B. Notation and Definition

2.3: Mod Notation

The notation

$$\equiv$$

Is used in mod arithmetic and is read

$$"congruent\ to"$$

- The equality symbol (=) is written with two lines, whereas the mod symbol is written with three lines (≡)
- The symbol ≡ is used to indicate that two expressions have the same remainder when divided by a quantity.

2.4: Meaning of ≡ Notation

If we write

$$a \equiv b\ (mod\ c)$$

It means that a divided by c, and b divided by c have the same remainder.

Example 2.5

Find the smallest positive values of the following expressions:

A. $7\ (mod\ 4)$
B. $25\ (mod\ 7)$

C. $125\ (mod\ 10)$
D. $25675(mod\ 3)$
E. $25673(mod\ 9)$

$$\underbrace{7}_{Dividend} = \underbrace{1}_{Quotient} \times \underbrace{4}_{Divisor} + \underbrace{3}_{Remainder}$$
$$7(mod\ 4) \equiv 3(mod\ 4)$$

And in shortform, we do not need to write the mod multiple times:

$$7 \equiv 3(mod\ 4)$$

$$25 \equiv 4(mod\ 7)$$

$$125 \equiv 5(mod\ 10)$$

$$25{,}675 \equiv 1(mod\ 3)$$
$$2 + 5 + 6 + 7 + 5 = 25 \equiv 1(mod\ 3)$$

$$25673(mod\ 9)$$
$$2 + 5 + 6 + 7 + 3 = 23 \equiv 5(mod\ 9)$$

2.6: Fractions and Decimals

Mod Arithmetic does not have fractions, or decimals. It is an arithmetic only of integers.

2.7: Negative Numbers in Mod Arithmetic

$$\underbrace{3(mod\ 7)}_{\textbf{3 more than a multiple of 7}} \equiv \underbrace{-4(mod\ 7)}_{\textbf{4 less than a multiple of 7}}$$

Negative values are particularly useful when the absolute values of the negative numbers are much smaller than the positive values.

Example 2.8

A. A number is five more than a multiple of 7. How many less is it than the next multiple of seven?
B. Shyam was distributing muffins in the local school. There were seventeen children in the class, and Shyam had 4 muffins left over. How more muffins does he need so that he can give one more muffin to every child?

Part A

$$\underbrace{7x + 5}_{\substack{Five\ more\ than \\ a\ multiple\ of\ 7}} = 7x + 7 - 5 = \underbrace{7(x + 1) - 2}_{\substack{Two\ less\ than \\ a\ multiple\ of\ 7}}$$
$$12 = 7 + \underbrace{5}_{mod\ 7} = 14 - \underbrace{2}_{mod\ 7}$$
$$5 \equiv -2(mod\ 7)$$

Part B

$$17x + 4 = 17(x + 1) - 13$$
$$4 \equiv -13(mod\ 17)$$

Example 2.9: Conversion

Convert the following statements given into language, algebra, and mod notation (one of the three is given).

A. A number is three more than a multiple of 12.

B. A number is five less than a multiple of 99.
C. $23c + 4$
D. $19d - 3$
E. $-1(mod\ 100)$

Language	*Algebra*	*Mod Notation*
Three more than a multiple of 12.	$12a + 3$	$3(mod\ 12)$
Five less than a multiple of 99.	$99b - 5$	$-5(mod\ 99)$
Four more than a multiple of 23.	$23c + 4$	$4(mod\ 23)$
Three less than a multiple of 19.	$19d - 3$	$-3(mod\ 19)$
One less than a multiple of 100.	$100e - 1$	$-1(mod\ 100)$

Example 2.10: Mod Equations

Solve each equation below. Give two positive and one negative values for answers.

A. $x \equiv 3(mod\ 11)$
B. $y \equiv -1(mod\ 99)$

Part A

$$11 \times 1 = 11 \Rightarrow 11 + 3 = 14$$
$$11 \times -1 = -11 \Rightarrow -11 + 3 = -8$$
$$x = -8,3,14$$

Part B

Multiples of 99 are:

$$\{0,99,198\}$$
$$y = -1,98,197$$

2.11: General Solution to Mod Equations

The solution to the equation $x \equiv a(mod\ b)$ is given by:

$$\dots, a - nb, \dots, a - 2b, a - b, a, a + b, a + 2b, \dots, a + nb, \dots$$

Unlike linear algebraic equations, which usually have one solution, mod linear equations have an infinite number of solutions.

Example 2.12: General Equations

Find the general solution to each equation below. Write it as set in roster form, and also set builder form.

A. $x \equiv 3(mod\ 11)$
B. $y \equiv 2(mod\ 7)$
C. $z \equiv 110(mod\ 4)$

Part A

x is three more than a multiple of 11.

$$\{x: x = 11n + 3, n \in \mathbb{Z}\}$$
$$x \in \{\dots, -30, \mathbf{-19}, -8,3,14,25,36,47, \mathbf{58}, \dots\}$$

Part B

y is two more than a multiple of 7.

$$\{y: y = 7n + 2, n \in \mathbb{Z}\}$$
$$y \in \{\dots, \mathbf{-19}, -12, -5,2,9,16, \dots\}$$

Part C

Example 2.13: General Equations

A. Find the smallest positive number that is three more than a multiple of 11, and two more than a multiple of 7.

$$x \equiv 3(mod\ 11) \Leftrightarrow x \in \{\dots, -30, \mathbf{-19}, -8, 3, 14, 25, 36, 47, \mathbf{58}, \dots\}$$
$$y \equiv 2(mod\ 7) \Leftrightarrow y \in \{\dots, \mathbf{-19}, -12, -5, 2, 9, 16, \dots\}$$

Example 2.14

Find the greatest negative number that satisfies each modular arithmetic relation below:

A. $70(mod\ 71)$
B. $341(mod\ 343)$

$$70 \equiv 71 - 1 \equiv 0 - 1 \equiv -1\ (mod\ 71)$$
$$341 \equiv -2(mod\ 343)$$

C. Divisibility in Mod

Since mod refers to remainders, many tests of divisibility (which also give the remainder) are useful in calculating mod.

Example 2.15: Divisibility in calculating mod

Evaluate:

A. $98413(mod\ 2)$
B. $67132(mod\ 4)$
C. $735(mod\ 10)$
D. $89134(mod\ 100)$
E. $34567(mod\ 5)$
F. $3451(mod\ 9)$
G. $12873(mod\ 3)$

Use the Test of Divisibility of 2 and 4:

$$98413 \equiv \underbrace{3 \equiv 1(mod\ 2)}_{\because 98{,}410 \equiv 0(mod\ 2)}$$
$$67132 \equiv \underbrace{32 \equiv 0\ (mod\ 4)}_{\because 67{,}100 \equiv 0(mod\ 4)}$$

Use the last digit (for 5 and 10), and the last two digits (for 100):

$$735 \equiv \underbrace{5(mod\ 10)}_{\because 730 \equiv 0(mod\ 10)}$$
$$89134 \equiv \underbrace{34(mod\ 100)}_{\because 89{,}100 \equiv 0(mod\ 100)}$$
$$34567 \equiv \underbrace{2(mod\ 5)}_{\because 34565 \equiv 0(mod\ 5)}$$

Use the sum of digits test of divisibility for 3 and 9:

$$\underbrace{3451 \equiv 13 \equiv 4(mod\ 9)}_{\because 3541 \equiv 3+4+5+1 \equiv 13\ (mod\ 9)}$$
$$\underbrace{12873 \equiv 21 \equiv 0(mod\ 3)}_{\because 12873 \equiv 1+2+8+7+3 \equiv 21\ (mod\ 3)}$$

Example 2.16

Simplify the following. Write a positive answer, except where specified.

A. $11x(mod\ 5)$

B. $12y(mod\ 5)$
C. $13z(mod\ 5)$ (Negative Answer)
D. $18a + 23b(mod\ 4)$
E. $12x + 17y + 22z(mod\ 9)$
F. $412p + 237q + 58r(mod\ 10)$

$$11x \equiv 10x + x \equiv 0 + x \equiv x\ (mod\ 5)$$
$$12y \equiv 10y + 2y \equiv 0 + 2y \equiv 2y(mod\ 5)$$
$$13z + 2z - 2z \equiv 15z - 2z \equiv 0 - 2z \equiv -2z\ (mod\ 5)$$

For the rest, we do not show the working, but the idea is the same:

$$18a + 23b(mod\ 4) \equiv 2a + 3b\ (mod\ 4)$$
$$12x + 17y + 22z \equiv 3x + 8y + 4z\ (mod\ 9)$$
$$412p + 237q + 58r \equiv 2p + 7q + 8r\ (mod\ 10)$$

2.17: Addition/Subtraction Property I (One-Sided)

$$a \pm \underbrace{xb}_{\equiv 0} \equiv a(mod\ b), x \in \mathbb{N}$$

Adding, or subtracting, multiples of the mod value is valid.

Note that this is a one-sided property.
You can do this on the left side of the congruence, or the right side of the congruence. You can also do this on both sides (if you want).

We will later on look at two-sided properties, which affect both sides of the congruence.

Example 2.18

Explain the mistake in the "calculation" using mod arithmetic below:

$$5 \equiv 5 + \frac{1}{2}(8) \equiv 5 + 4 \equiv 9 \equiv 1(mod\ 8)$$

Mod arithmetic does not have fractions and decimals.
Hence, we can add and subtract multiples of 8.
We cannot add $\frac{1}{2}(8) = 4$.
b

Example 2.19

Identify different numbers that have the same value as

$$3(mod\ 11)$$

At least one of them should have a variable.

$$\underbrace{3 \equiv 14 \equiv 25 \equiv 113 \equiv -8 \equiv 3 + 11y \equiv 1004 + 1001x}_{\textit{Same Congruence Class}}\ (mod\ 11)$$

2.20: Congruence Class

Numbers which have the same remainder when divided by x, have the same congruence class mod x.

In the example above, the numbers

$$\{3, 14, 25, 113, -8, 3 + 11y, 1004 + 1001x\}$$

all belong to the same congruence class.

Example 2.21

A. Are 2 and 5 in the same congruence class $mod\ 2$.
B. Are $2 + 4x$ and $8 + 12x$ in the same congruence class $mod\ 2$.
C. Find the smallest number greater than $4 + 7x$ that is in the same congruence class $mod\ 11$ as $4 + 7x$.
D. Find the greatest number smaller than $24 - 56x$ that is in the same congruence class $mod\ 8$ as $24 - 56x$.

Part A

$$2 \equiv 0(mod\ 2)$$
$$5 \equiv 1(mod\ 2)$$
$$0 \neq 1 \Rightarrow Not\ in\ the\ same\ congruence\ class$$

Part B

$$2 + 4x \equiv 0(mod\ 2)$$
$$8 + 12x \equiv 0(mod\ 2)$$
$$In\ the\ same\ congruence\ class$$

Part C

$$11 + 4 + 7x = 15 + 7x$$

Part D

$$16 - 56x$$

2.22: Number of Congruence Classes

The number of congruence classes mod x is also x.

Example 2.23

A. How many congruence classes are there $mod\ 3$. List the smallest non-negative values of each congruence class.
B. How many congruence classes are there $mod\ 2023$?

Part A

The congruence classes $mod\ 3$:

$$\{0,1,2\} \Rightarrow 3\ Values$$

Part B

$$2023$$

Example 2.24

Find, mod 7, the number of distinct congruence classes among the numbers in the following set:

$$\{4,1001,-4,7x + 12,11\}$$

The question is asking how many unique remainders exist in the set above, when the numbers in the set are divided by 7. In order to ensure that congruence classes do not repeat, we are going to consider the simplest set of congruence classes mod 7, which is $0 \leq x \leq 6$.

$$4 \equiv 4$$
$$1001 \equiv 0$$
$$-4 \equiv 3$$
$$7x + 12 \equiv 12 \equiv 5$$
$$11 \equiv 4$$

All values are distinct except 4, which is repeated twice. Hence, the Distinct Congruence classes:

$$\{0,3,4,5\} = 4\ classes$$

Example 2.25

Find five positive numbers and three negative numbers that are in the same congruence class as

A. $7(mod\ 11)$
B. $12\ (mod\ 3)$

Part A

Use the addition property to add multiples of 11 to change the number, without changing the congruence class:

$$7 \equiv \underbrace{18}_{=7+11} \equiv 29 \equiv 40 \equiv 51(mod\ 11)$$

Subtract multiples of eleven:

$$7 \equiv \underbrace{-4}_{=7-11} \equiv -15 \equiv -26(mod\ 11)$$

Part B

Similarly, first subtract 12, and then add multiples of 3:

$$12 \quad \underbrace{\equiv 0}_{Subtract\ 12} \quad \underbrace{\equiv 3}_{Adding\ 3} \equiv 6 \equiv 9(mod\ 3)$$

Subtract multiples of three:

$$12 \equiv 0 \equiv -3 \equiv -6 \equiv -9(mod\ 3)$$

Example 2.26: Counting

A. How many positive numbers less than 1000 are $3(mod\ 12)$

We get a list of numbers, which we can count using the principles of counting lists:

$$n\left\{\underbrace{3}_{0\times12+3}, 15, 27, \ldots, \underbrace{999}_{83\times12+3}\right\} \Rightarrow n\left\{\underbrace{0}_{12\times0}, 12, 24, \ldots, \underbrace{996}_{12\times83}\right\} \Rightarrow 83 - 0 + 1 \text{ terms} = 84 \text{ terms}$$

2.27: Difference from Equations

Equations have two sided properties only.
Congruences have two-sided properties (which we will see next), and also one-sided properties.

For example, given the equation

$$x + 5 = 9 \Rightarrow x + 5 - \mathbf{5} = 9 - \mathbf{5}$$

We can subtract 5 from both sides.

2.28: Addition/Subtraction Property I (Two-Sided)

Adding, or subtracting, the same number to both sides of a congruence is valid.

$$\boldsymbol{a \equiv b(mod\ c) \Leftrightarrow a + x \equiv b + x(mod\ c)}$$

This is similar to the property we use for solving algebraic equations, where we can add (or subtract) the same number from both sides of a linear equation.
We can use the above property to solve simple linear congruences with variables where the coefficient is one.

Example 2.29

A. Find the smallest four-digit number in the same congruence class as $3(mod\ 7)$.
B. Find the greatest three-digit number in the same congruence class as $4(mod\ 15)$.

Part A

$1001 = 7 \times 11 \times 13$:

$$1001 \equiv 0(mod\ 7)$$

Add 3 to both sides:

$$1004 \equiv 3(mod\ 7)$$

Smallest 4-digit number is:

$$1004$$

Part B

We will work with multiples of 15 that are easy to identify:

$$105 = 7 \times 15$$

Multiply by 10:

$$1050 = 70 \times 15$$

Subtract 60:

$$990 = 66 \times 15$$

Convert to mod notation:

$$990 \equiv 0(mod\ 15)$$

Add 4 to both sides:

$$994 \equiv 4(mod\ 15)$$

D. Variables: Solving Congruences

We can use the properties that we have learnt so far to solve simple congruences that involve variables.

Example 2.30

Solve

$$x + 4 \equiv 3(mod\ 7)$$

Add 3 to both sides:

$$x + 7 \equiv 6(mod\ 7)$$
$$x \equiv 6(mod\ 7)$$

Example 2.31

When seven is subtracted from a number, it becomes a three-digit number which is three more than a multiple of 8. Find the smallest value possible of the number.

Method I: Mod Arithmetic

$$x - 7 \equiv 3(mod\ 8)$$

Add 7 to both sides:

$$x - \mathbf{7} + \mathbf{7} \equiv 3 + \mathbf{7}(mod\ 8)$$

Simplify:

$$x \equiv 10(mod\ 8)$$

Subtract 8 from RHS:

$$x \equiv 2(mod\ 8)$$

Method II: Logic

The number is two more than a multiple of 8. To meet the three-digit restriction, we find the smallest three-digit multiple of 8:

$$104 = 8 \times 13 \Rightarrow x = 104 + 3 + 7 = 114$$

We can check that 114 does meet the requirements given in the question:

$$114 - 7 = 107 \rightarrow 107 - 3 = 104 = 13 \times 8$$

Example 2.32

Find the solutions to $x + 3y = 100$ if x and y are natural numbers. Count the number of solutions also.

$$x + 3y = 100$$
$$\underbrace{3y}_{\text{Multiple of 3}} = 100 - x$$

Since we have a multiple of three on the LHS, we will work $mod\ 3$. Since the LHS is a multiple of three, the RHS must also be a multiple of three. In other words, it must have a remainder of zero, when divided by three.

We can convert this into a congruence equation:

$$100 - x \equiv 0\ (mod\ 3)$$

Add 2 to both sides:

$$102 - x \equiv 2\ (mod\ 3)$$

But note that $102 \equiv 0(mod\ 3)$

$$-x \equiv 2\ (mod\ 3)$$

Multiply by -1 both sides:

$$x \equiv -2\ (mod\ 3)$$

Since we don't want a negative number, add three only to the RHS:

$$x \equiv 1\ (mod\ 3)$$
$$x \in \{1,4,7,10, \dots, 97\}$$

Example 2.33

Solve the following equation for natural number values of x and y. Write your answers as ordered (x, y) pairs. Find the number of solutions also.

$$2x - 3y = 101$$

$$\underbrace{2x}_{\text{Multiple of 2}} = 101 + 3y$$

Since the LHS is a multiple of 2, we work $mod\ 2$:

$$0 \equiv 101 + 3y\ (mod\ 2)$$

Add 1 to both sides:

$$1 \equiv 102 + 3y\ (mod\ 2)$$
$$1 \equiv 3y\ (mod\ 2)$$

Split the RHS:

$$1 \equiv 2y + y\ (mod\ 2)$$
$$1 \equiv y\ (mod\ 2)$$
$$y\ is\ odd$$

Example 2.34

There are various ways to make \$207 using only \$2 coins and \$5 bills. One such way is using one \$2 coin and forty-one \$5 bills. Including this way, in how many different ways can \$207 be made using only \$2 coins and \$5 bills? **(CEMC Grade 8 2007/23)**

$$2x + 5y = 207$$

Work $mod\ 2$:

$$0 + y \equiv 1\ (mod\ 2) \Rightarrow y\ is\ odd$$
$$(x, y) = (1,41), (6,39), \dots, (101,1)$$

To count the solutions:

$$(41,39, \dots, 1) \rightarrow (42,40, \dots, 2) \rightarrow (21,20, \dots, 1) \Rightarrow 21\ Solutions$$

Example 2.35

- Hodge told Jakes, "I'll give you six of my pigs for one of your horses, and then you'll have twice as many

animals here as I've got."
- Durrant told Hodge, "I'll give you fourteen of my sheep for a horse, and then you'll have three times as many animals as I."
- Jakes told Durrant; "I'll give you four cows for a horse, and then you'll have six times as many animals as I've got here."

How many animals did Jakes, Hodge, and Durrant take to the cattle market? **(Amusements in Mathematics, H. E. Dudeney, Adapted)**

Let the number of animals with

$$Hodge = h, \quad Jake = j, \quad Durrant = d$$

First Condition

$$2(h-5) = j+5$$
$$2h-10 = j+5$$
$$2h = j+15$$

Second Condition

$$3(d-13) = h+13$$
$$3d = h+52$$

The LHS is a multiple of 3. Hence, work $mod\ 3$:

$$3d \equiv h+52 \ (mod\ 3)$$
$$0 \equiv h+1 \ (mod\ 3)$$

Add 2 to both sides:

$$2 = h \ (mod\ 3)$$

Also, note that from $3d = h+52$, we get

$$d = \frac{h}{3}+\frac{52}{3} = \frac{h}{3}+17\frac{1}{3} \Rightarrow \underbrace{d \geq 18}_{Result\ I}$$

Third Condition

$$6(j-3) = d+3$$
$$6j = d+21$$

Note that the LHS is a multiple of 6. Hence, work $mod\ 6$:

$$6j \equiv d+21 \ (mod\ 6)$$
$$0 \equiv d+3 \ (mod\ 6)$$

Add 3 to both sides:

$$\underbrace{3 \equiv d \ (mod\ 6)}_{Result\ II}$$

Since $d \geq 18$ and $d \equiv 3 \ (mod\ 6)$, the smallest value of d that we can try is:

$$d = 21$$

$$6j = d+21 = 21+21 = 42 \Rightarrow j = \frac{42}{6} = 7$$

$$2h = j+15 = 7+15 = 22 \Rightarrow h = \frac{22}{2} = 11$$

$$(h, j, d) = (11, 7, 21)$$

E. Additive Inverses

2.36: Additive Inverses: Regular Arithmetic

If two numbers add up to zero, they are called the additive inverse for each other.

$$x+y = 0 \Rightarrow x = -y \Rightarrow (x, y)\ are\ additive\ inverses$$
$$4+(-4) = 0 \Rightarrow (4, -4)\ are\ additive\ inverses$$

- A positive number has a negative additive inverse.
- A negative number has a positive additive inverse.

Example 2.37

In regular arithmetic, find the additive inverse of

A. 7
B. 0
C. z

-7
0

$$-z$$

Example 2.38
In regular arithmetic, which are the numbers whose additive inverse is the same as the number itself.

$$x = -x \Rightarrow x = 0$$

Example 2.39
Consider the additive inverse of

$$z = p + q + r$$

Decide for each of the below whether the expression is positive, negative, or neither:

A. Additive inverse of z, given that z is negative.
B. Additive inversse of z, given that z is positive.
C. Additive inverse of z, given that z is neither positive nor negative.

$$Part\ A: additive\ inverse\ is\ +ve$$
$$Part\ B: additive\ inverse\ is -ve$$
$$Part\ C: additive\ inverse\ is\ \ neither$$

Example 2.40
Consider the number 5. How many additive inverses does it have?

$$Additive\ inverse\ of\ 5 = -5$$
$$No.\ of\ additive\ inverses = 1$$

2.41: Additive Inverse is Unique (Regular Arithmetic)
The additive inverse of a number is unique.

- This is in direct contrast to additive inverses in mod arithmetic, where there are an infinite number of additive inverses.

2.42: Additive Inverses: Modular Arithmetic
In mod arithmetic, there are an infinite number of additive inverses.

$$a + b \equiv m \equiv 0(mod\ m) \Rightarrow (a, b) \text{ are additive inverses}$$

- It is not necessary that the additive inverse has a sign opposite that of the number.
- A number has an infinite sequence of additive inverses. Once we find one additive inverse, all numbers that belong to the same congruence class are also additive inverses.

Example 2.43
Find the smallest positive additive inverse of each number in the following set:

A. $5\ (mod\ 11)$
B. $20(mod\ 34)$
C. $785\ (mod\ 800)$

$$5 + 6 \equiv 11 \equiv 0(mod\ 11) \Rightarrow 6 \text{ is the additive inverse of } 5\ (mod\ 11)$$
$$20 + 14 \equiv 34 \equiv 0(mod\ 34) \Rightarrow 14 \text{ is the additive inverse of } 20\ (mod\ 34)$$
$$785 + 15 \equiv 800 \equiv 0(mod\ 800) \Rightarrow 15 \text{ is the additive inverse of } 785\ (mod\ 800)$$

Example 2.44
Find the largest negative additive inverse of each number in the following set:

A. $5\ (mod\ 11)$
B. $20(mod\ 34)$
C. $785\ (mod\ 800)$

$$-5$$
$$-20$$
$$-785$$

Example 2.45
Find the sum of the smallest positive additive inverse and the largest negative additive inverse of $12\ (mod\ 17)$.

$$12 + 5 \equiv 0\ (mod\ 17)$$
$$12 - 12 \equiv 0\ (mod\ 17)$$
$$5 + (-12) = -7$$

2.46: Additive Inverses: Modular Arithmetic
Since adding the additive inverse to a number results in $0(mod\ x)$, we can use additive inverses to "remove" a number from a linear congruence.

Example 2.47
Find the smallest positive value that satisfies:

A. $x + 4 \equiv 3(mod\ 7)$
B. $x + 4 \equiv 10(mod\ 6)$
C. $x + 4 \equiv 7(mod\ 8)$
D. $7x + 3 \equiv 1(mod\ 6)$
E. $26x + 4 \equiv 9(mod\ 5)$

Part A
Add 3 to both sides:
$$x \underbrace{+7}_{\equiv 0} \equiv 6(mod\ 7)$$
$$x \equiv 6(mod\ 7)$$

Part B
Add 2 to both sides:
$$x \equiv 12 \equiv 0(mod\ 6)$$

Part C
Add 4 to both sides:
$$x \equiv 11 \equiv 3(mod\ 8)$$

Part D
$$6x + x + 3 \equiv 1(mod\ 6)$$
$$x + 3 \equiv 1(mod\ 6)$$
Add 3 to both sides:
$$x \equiv 4(mod\ 6)$$

Part E
$$25x + x + 4 \equiv 9(mod\ 5)$$
$$x + 4 \equiv 9(mod\ 5)$$
Add 1 to both sides:
$$x \equiv 10 \equiv 0(mod\ 5)$$

F. Congruences

Example 2.48
$$2x \equiv 5\ (mod\ 7)$$

A. Find the smallest positive value of x that satisfies.
B. Write the congruence class of x, using Part A

Part A

Try various values of x:

x	$2x$	$2x(mod\ 7)$
1	2	2
2	4	4
3	6	6
4	8	1
5	10	3
6	12	5

$x = 6$ works as a solution. Since we are solving $mod\ 7$, we can write our solution as

$$2x \equiv 5\ (mod\ 7) \Rightarrow x = 6(mod\ 7)$$

Part B

From the above, we have found not just a single solution, but actually an entire congruence class, any of which will serve as the solution.

$$x \equiv 6(mod\ 7) \Rightarrow x \in \{\dots, -1, 6, 13, 20, \dots\}$$

In further examples, we are not going to illustrate the entire table used for trying the out the values of x. We will directly write the solution, but they will have to come through a process of trial and error.

Example 2.49

Solve each congruence *independently*. State the answer as both:
the smallest positive value that satisfies the congruence
the set of values that satisfies the congruence

$$3x \equiv 1\ (mod\ 9)$$
$$3x \equiv 9\ (mod\ 3)$$
$$7x \equiv 6\ (mod\ 9)$$
$$8x \equiv 5\ (mod\ 11)$$

$$3x \equiv 1\ (mod\ 9) \Rightarrow No\ Solutions\ (\because \gcd(3,9) = 3)$$

$$3x \equiv 9\ (mod\ 3) \Rightarrow 3x \equiv 0(mod\ 3) \Rightarrow x \in \{\dots, -1, 0, 1, 2, \dots\}$$

x can be any natural number.
Smallest positive value of x is 1.

$$7x \equiv 6\ (mod\ 9) \Rightarrow x \equiv 6(mod\ 9) \Rightarrow x \in \{\dots -3, 6, 15, 24, \dots\}$$
$$8x \equiv 5\ (mod\ 11) \Rightarrow x \equiv 2(mod\ 11) \Rightarrow x \in \{\dots -9, 2, 13, 25, \dots\}$$

Example 2.50

In the set of natural numbers 1,2,3 … we define a new multiplication as follows: For positive integers m, n, divide mn by 7 and find the remainder k, and we define $m \star n = k$. For example:
$102 \star 8 = 4$, since $102 \times 8 = 816 = 7 \times 116 + 4$
$84 \star 5 = 0$, since 84×5 is a multiple of 7 and the product leaves zero remainder when divided by seven.
Find an integer k such that $2005 \star k = 1$ in our new multiplication $\star$.
(NMTC Primary/Final 2005/13)

$$2005k \equiv 1(mod\ 7)$$

Subtract $2002k \equiv 0\ (mod\ 7)$ from both sides:

$$3k \equiv 1(mod\ 7)$$
$$k = 5 + 7n, n \in \mathbb{Z}$$

Example 2.51: Real Life Problems

The number of days in a year is either 365 (for a non-leap year), or 366 (for a leap year). If the day today is Monday, and the day exactly x years($x < 10$) hence is Saturday, find the possible value(s) of x.

$$365 \equiv 1(mod\ 7), 366 \equiv 2\ (mod\ 7)$$
$$Day\ will\ go\ forward\ by\ either\ 1\ day, or\ 2\ days\ each\ year$$

$$Monday + 5\ days = Saturday$$

If the period under consideration happens to include a century which is a multiple of 4, and hence not a leap year, then it is possible to have five consecutive years which add up to 5:

$$x = 5:\ 1 + 1 + 1 + 1 + 1$$

The position of the leap year does not matter. The value of x remains 4:

$$x = 4: 1 + 1 + 1 + 2$$

$$x \in \{4,5\} \Rightarrow Possible\ Values\ of\ x = 2$$

Example 2.52

A cluster of star systems is called *eccentric* if each star system in the cluster has planets which are a multiple of three. The Sonotoran Special Space Service is invading an *eccentric* cluster, and decides to invade each planet, and also two planetoids extra across the entire cluster. Each planet or planetoid has a dedicated invasion ship. If the invasion ships are grouped in fleets of seven each, there are 4 ships left over. If the number of star systems in the cluster is a two-digit number, find the smallest number of invasion ships that could have been sent over.

Let the number of planets and planetoids be p. Let the number of invasion ships be I.

$$p \equiv 2(mod\ 3) \Rightarrow \{2,5,8, \mathbf{11}, \dots\}$$
$$I \equiv 4(mod\ 7) \Rightarrow \{4, \mathbf{11}, \dots\}$$

If there are 11 ships, then the number of planets

$$No.of\ Planets = 11 - 2 = 9 \Rightarrow No.of\ Star\ systems = 3$$

So, we look for the next number:

$$11 + LCM(3,7) = 11 + 21 = 32$$
$$No.of\ Planets = 32 - 2 = 30 \Rightarrow No.of\ Star\ systems = 10$$

Example 2.53

Riddhi distributes four food packets to each person she meets, but is only able to give three food packets to the last person she meets. If the number of people she gives food packets to is a two-digit number, find the possible values of the people to whom she distributed food packets.

2.2 Mod Arithmetic-II: Distributive Property

A. Distributive Property

2.54: Distributive Property

$$(a \pm b)(mod\ x) = a(mod\ x) \pm b(mod\ x)$$

- We can distribute taking the mod over addition. Instead of doing the addition or the subtraction first, we can take the mod first. This can greatly simplify calculations.
- Using this property is equivalent to adding up remainders.

Example 2.55

$$x = 1257 + 1258 + 1259 + 1260$$

A. Find $x(mod\ 5)$
B. Find $x(mod\ 3)$
C. Find $x(mod\ 9)$

Part A

$$1257 + 1258 + 1259 + 1260(mod\ 5)$$

Use the distributive property:

$$\equiv 1257(mod\ 5) + 1258(mod\ 5) + 1259(mod\ 5) + 1260(mod\ 5)$$
$$\equiv 2(mod\ 5) + 3(mod\ 5) + 4(mod\ 5) + 0(mod\ 5)$$

Use the reverse of the distributive property:

$$\equiv 2 + 3 + 4 + 0 \equiv 9 \equiv 4(mod\ 5)$$

Part B

$$0 + 1 + 2 + 0 \equiv 3 \equiv 0(mod\ 3)$$

Part C

Working with negative numbers is easier for this part:

$$-3 - 2 - 1 - 0 \equiv -6 \equiv 3(mod\ 9)$$

Example 2.56

Find the remainder when $34517 + 34518 + 34519 + 34520$ is divided by 11.

$$34517(mod\ 11) = \underbrace{15}_{7+5+3} - \underbrace{5}_{1+4} = 10 \equiv -1(mod\ 11)$$

Apply the distributive property:

$$34517 + 34518 + 34519 + 35520 \equiv \mathbf{-1} + 0 + \mathbf{1} + 2 \equiv 2(mod\ 11)$$

Negative numbers help simplify calculations when we get numbers like $-1, -2$, with small absolute values. Note the use of negative numbers in the prior example.

B. Patterns in Mod

2.57: Cyclicity of Mod

The remainders repeat in a cyclical pattern. This concept is connected to congruence classes.

Example 2.58

Find the remainder when the sum of the first 100 natural numbers is divided by 6.

We can group the expression that we want to find as follows:

$$\underbrace{1 + 2 + 3 + 4 + 5 + 6}_{\equiv 1+2+3+4+5+0 \equiv 15 \equiv 3(mod\ 6)} + \underbrace{7 + 8 + 9 + 10 + 11 + 12}_{\equiv 1+2+3+4+5+0 \equiv 15 \equiv 3(mod\ 6)} + \cdots + \underbrace{97 + 98 + 99 + 100}_{\equiv 1+2+3+4 \equiv 10 \equiv 4(mod\ 6)}\ (mod\ 6)$$

Since $100 = 6 \times 16 + 4$, we have 16 groups of 6 numbers, and 4 left over.

$$\therefore 3 \times 16 + 4 \equiv 6 \times 8 + 4 \equiv 4(mod\ 6)$$

Example 2.59
Find the remainder when the sum of the first 33,333,334 natural numbers is divided by 3.

Since we are finding $(mod\ 3)$, there are only three congruence classes.

$$1^{st}\ Congruence\ Class \rightarrow 1 \equiv 4 \equiv 7(mod\ 3)$$
$$2^{nd}\ Congruence\ Class \rightarrow\ 2 \equiv 5 \equiv 8(mod\ 3)$$
$$3^{rd}\ Congruence\ Class \rightarrow \underbrace{3 \equiv 6 \equiv 9 \equiv 0(mod\ 3)}_{\textbf{3rd Congruence Class}}$$

We can group the expression that we want to find as follows:

$$\underbrace{1+2+3}_{\equiv 1+2+3\equiv 6\equiv 0} + \underbrace{4+5+6}_{\equiv 1+2+3\equiv 6\equiv 0} + \cdots + \underbrace{33{,}333{,}334}_{\equiv 1}\ (mod\ 3) \equiv 0+0+\cdots+0+1 \equiv 1(mod\ 3)$$

Except for the last number (33,333,334) all the numbers can be divided into groups of three.

C. Using the Distributive Property and Tests of Divisibility

Some congruences can need simplification using the properties of congruences that we learnt. The next set of congruences relies on using the:

- Distributive property to apply the mod to each term instead of the entire expression
- Tests of divisibility which are also remainder tests to simplify otherwise complicated divisions

Example 2.60: mod 5
Solve for the smallest positive value that satisfies:

$$729x + 234 \equiv 531\ (mod\ 5)$$

Each term here is large, and finding values $mod\ 5$ is easy, so reduce each term $mod\ 5$.

$$\left(\underbrace{725x}_{\equiv 0(mod\ 5)} + 4x\right) + \left(\underbrace{230}_{\equiv 0(mod\ 5)} + 4\right) \equiv \underbrace{530}_{\equiv 0(mod\ 5)} + 1(mod\ 5)$$
$$4x + 4 \equiv 1\ (mod\ 5)$$

Add 1 to both sides:

$$4x + 5 \equiv 2\ (mod\ 5)$$
$$4x \equiv 2\ (mod\ 5)$$

Try various values of $x = 1,2,3, \ldots \Rightarrow 3\ works$:

$$x \equiv 3(mod\ 5)$$

Example 2.61: mod 3
Solve for the smallest positive value that satisfies:

$$457x + 271 \equiv 567(mod\ 3)$$

Use test of divisibility of three (which is also a test of the remainder by 3). As before, apply the mod to each term since the test of three is easy to apply:

$$\underbrace{457x}_{4+5+7\equiv 1(mod\ 3)} + \underbrace{271}_{2+7+1\equiv 1(mod\ 3)} \equiv \underbrace{567}_{5+6+7\equiv 18\equiv 0(mod\ 3)}\ (mod\ 3)$$

Simplify:

$$x + 1 \equiv 0(mod\ 3)$$

Add 2 to both sides:

$$x \equiv 2(mod\ 3)$$

Smallest positive value

$$x = 2$$

Example 2.62
Solve for the smallest positive value that satisfies:

$$55x + 12 \equiv 32x + 7 \ (mod\ 6)$$

$$x + 0 \equiv 2x + 1 \ (mod\ 6)$$

Subtract x, and add 5 to both sides:

$$5 \equiv x \ (mod\ 6)$$

Smallest positive value:

$$x = 5$$

Example 2.63
Solve for the smallest positive value that satisfies:

$$76459x + 84512 \equiv 82301x + 1 (mod\ 4)$$

Recall that the remainder on dividing by 4 is the same as the last two digits of a number.
Hence, reduce each term $mod\ 4$:

$$59x + 12 \equiv 1x + 1$$
$$3x + 0 \equiv x + 1 (mod\ 4)$$

Subtract x from both sides:

$$\underbrace{2x}_{Even} \equiv \underbrace{1}_{Odd} \ (mod\ 4) \Rightarrow \textbf{\textit{No Solutions}}$$

D. Congruence Systems
Questions on modular arithmetic can at times be related to simple concepts like HCF and LCM. We begin by focusing on these connections, and then broadening to the **Chinese Remainder Theorem** in the next chapter. Questions on HCF require calculating the possible value, or values, of the mod that meet the conditions of the problem.

2.64: Chinese Remainder Theorem

$$\underbrace{where\ \{m_1, m_2, m_3\}\ are\ pairwise\ coprime}_{} \Leftrightarrow \underbrace{n\ is\ unique\ mod\ m_1 m_2 m_3}_{}$$

Suppose I have a number x such that

$$x \equiv a (mod\ m_1)$$
$$x \equiv b (mod\ m_2)$$
$$x \equiv c (mod\ m_3)$$

Where m_1, m_2, m_3 are pairwise coprime.

$$HCF(m_1, m_2) = HCF(m_2, m_3) = HCF(m_1, m_3) = 1$$

Then there is a unique number n such that:

$$x \equiv n (mod\ m_1 m_2 m_3)$$

There exists a solution to the system of linear congruences above (so long as the coprime condition on the mod is met), and there is only one congruence class $mod\ m_1 m_2 m_3$ that satisfies the system.
Once we find one solution, we can find more solutions by finding numbers that belong to the same congruence class as the original solution.

Example 2.65
I have a positive number which is one more than a multiple of 3, and one more than a multiple of 4.

A. What is the smallest such number?

B. What are all such numbers?

The number is one more than a multiple of 3:

$$x \equiv 1(mod\ 3) \Rightarrow x \in \{\mathbf{1}, 4,7,10, \mathbf{13}, 16,19,22, \mathbf{25}, \dots\}$$

The number is one more than a multiple of 4:

$$x \equiv 1(mod\ 4) \Rightarrow x \in \{\mathbf{1}, 5,9, \mathbf{13}, 17,21, \mathbf{25}, \dots\}$$

The numbers which satisfy both the conditions are:

$$\{1,13,25, \dots, 1 + 12n\}, n \in \mathbb{W}$$

And note that

$$12 = LCM(3,4)$$

Example 2.66

Find all the numbers that satisfy the conditions given below for each part.

A. A positive number which is one more than a multiple of 5, and one more than a multiple of 6.
B. A positive number which is one more than a multiple of 2, one more than a multiple of 3, one more than a multiple of 4?
C. A positive number that has remainder 1 when divided by 4, and remainder 1 when divided by 6.

Part A

$$x \equiv 1(mod\ 5)$$
$$x \equiv 1(mod\ 6)$$
$$x \equiv 1(mod\ 30) \Rightarrow x = 1 + 30n, n \in \mathbb{W}$$

Part B

$$x \equiv 1(mod\ 2)$$
$$x \equiv 1(mod\ 3)$$
$$x \equiv 1(mod\ 4)$$
$$x \equiv 1(mod\ 12) \Rightarrow x = 1 + 12n$$

Part C

$$x \equiv 1(mod\ 4)$$
$$x \equiv 1(mod\ 6)$$
$$x \equiv 1(mod\ 12)$$

Example 2.67

A group of students went for a picnic. They played a game where they divided themselves into equal groups. When they made groups of three, their teacher had no group to join. When they made groups of four, their teacher could not find a group to join. When they made a group of five, their teacher was able to join a group.

A. Find the smallest possible value of the number of students.
B. Find all possible values of the number of students.

$$p \equiv 1(mod\ 3)$$
$$p \equiv 1(mod\ 4)$$

Combine the first two conditions to get:

$$p \equiv 1(mod\ 12) \Rightarrow \{1,13,25, \dots\}$$
$$p \equiv 0(mod\ 5)$$

We now need to solve the above two equations. Note that

$$Smallest\ possible\ value = 25$$

And to get further values we want

$$x \equiv 25(mod\ 60) \Rightarrow x = 25 + 60n$$

Where

$$60 = LCM(12,5)$$

Example 2.68

A. A positive number that is four less than a multiple of 5, and three less than a multiple of 4.

A number that is four less than a multiple of five is also a number that is one more than a multiple of five:

$$y \in \{1,6,11,16, \dots\} \Rightarrow y \equiv 1(mod\ 5)$$

A number that is three less than a multiple of five is also a number that is one more than a multiple of four:

$$\{1,5,9,13,\} \Rightarrow y \equiv 1(mod\ 4)$$

$$y \equiv 1(mod\ 20) \Rightarrow \{1,21,41, \dots\}$$

Example 2.69

A. I have a two digit number in mind such that the sum of 1 and the number is divisible by 2, the sum of 2 and the number is divisible by 3, the sum of 3 and the number is divisible by 4, and the sum of 4 and the number is divisible by 5. Find the number. **(Pradnya 5, 1987/9)**

B. Find all such numbers.

Let the number be x.

$$x + 1 \equiv 0(mod\ 2) \Rightarrow x \equiv 1(mod\ 2)$$
$$x + 2 \equiv 0(mod\ 3) \Rightarrow x \equiv 1(mod\ 3)$$
$$x + 3 \equiv 0(mod\ 4) \Rightarrow x \equiv 1(mod\ 4)$$
$$x + 4 \equiv 0(mod\ 5) \Rightarrow x \equiv 1(mod\ 5)$$

$$LCM(2,3,4,5) = 60$$

The two digit number is

$$1 + 60 = 61$$

And all such numbers are:

$$x \equiv 1(mod\ 60) \Rightarrow x = 1 + 60n$$

Example 2.70

Find the smallest number which when divided by 3, 7 and 11 leaves remainders 1, 6 and 5 respectively. **(Pradnya 5, 1991/8, Adapted)**

$$I: x \equiv 1(mod\ 3)$$
$$II: x \equiv 6(mod\ 7) \Rightarrow \{6,13,20,\mathbf{27}, \dots\}$$
$$III: x \equiv 5(mod\ 11) \Rightarrow \{16,\mathbf{27}, \dots\}$$

Combine condition II and condition III:

$$LCM(7,11) = 77$$
$$x \equiv 27\ (mod\ 77)$$

$$27 \equiv 0(mod\ 3)$$
$$104 \equiv 2(mod\ 3)$$
$$181 \equiv 1(mod\ 3) \Rightarrow$$

2.71: HCF

We can rewrite HCF using the language of mod arithmetic.
Suppose, on dividing a, b, and c by x, we get no remainder. We can write

$\underbrace{a \equiv 0\ (mod\ x)}_{x\ |\ a}$, $\underbrace{b \equiv 0\ (mod\ x)}_{x\ |\ b}$, $\underbrace{c \equiv 0\ (mod\ x)}_{x\ |\ c} \Leftrightarrow a, b, c$ are multiples of $x \Leftrightarrow x$ is a factor of a, b, c

To find the

- Largest such x, we find $HCF(a, b, c)$.
- Number of values that x can take, we find the number of factors of $HCF(a, b, c)$.
- Values that x can take, we find the factors of $HCF(a, b, c)$.
- Specific value of x, we find the factors of $HCF(a, b, c)$, any of which can be x, and then narrow down based on additional conditions given in the question

Example 2.72

What is the largest number x that divides 12, 18 and 20, while leaving no remainder?

$$12 \equiv 0(mod\ x) \Rightarrow x\ is\ a\ factor\ of\ 12$$
$$18 \equiv 0(mod\ x) \Rightarrow x\ is\ a\ factor\ of\ 18$$
$$20 \equiv 0(mod\ x) \Rightarrow x\ is\ a\ factor\ of\ 20$$

Hence, x is a factor of each of 12, 18 and 20.
Hence, the largest such x is:

$$HCF(12, 18, 20) = 2$$

Example 2.73

Sixteen white chocolates, twelve dark chocolates, and thirty-six brown chocolates are to be packed. Each box has exactly one type of chocolate. The number of chocolates in each box is equal. What is the minimum cost of packing, if each box costs one dollar and fifty cents?

Let the number of chocolates in each box be x.

$$12 \equiv 0(mod\ x) \Rightarrow x\ is\ a\ factor\ of\ 12$$
$$18 \equiv 0(mod\ x) \Rightarrow x\ is\ a\ factor\ of\ 12$$
$$36 \equiv 0(mod\ x) \Rightarrow x\ is\ a\ factor\ of\ 36$$

There are two parameters in this question:

$$Chocolates\ per\ box$$
$$No.\ of\ Boxes\ used$$

The no. of boxes will be *maximum* when the no. of chocolates per box is *minimum*.
The no. of boxes will be *minimum* when the no. of chocolates per box is *maximum*.

Hence, we need to keep maximum number of chocolates in each box.

Also, we need to satisfy the condition that the number of chocolates in each box is equal:

$$Max\left(\frac{Chocolates}{Box}\right) = HCF(16, 12, 36) = 4$$
$$Min(Boxes) = \frac{Chocolates}{Chocolates\ per\ box} = \frac{16 + 12 + 36}{4} = \frac{64}{4} = 16$$
$$Min(Cost\ of\ Packing) = Cost\ per\ Box \times No.\ of\ Boxes = 1.5 \times 16 = 24$$

Example 2.74: Number of Values of x

x divides 192, 108 and 24, leaving no remainder. What is the number of possible value(s) of x?

$$192 \equiv 0(mod\ x)$$
$$108 \equiv 0(mod\ x)$$
$$24 \equiv 0(mod\ x)$$

Hence, x must be a factor of each of the three.
Hence, x must be a factor of the HCF of the three numbers.

$$HCF(192,108,24) = HCF(2^6 \times 3, 2^2 \times 3^3, 2^3 \times 3) = 2^2 \times 3^1 = 12$$

The factors of 12 are:

$$\{1,2,3,4,6,12\} \Rightarrow 6\ Numbers$$

Alternate:

$$\text{Number of values of } x = \tau\big(HCF(192,108,24)\big) = \tau(12) = \tau(2^2 \times 3^1) = (2+1)(1+1) = 3 \times 2 = 6$$

Example 2.75

Find the greatest number such that the same remainder is obtained when 494,726, and 1045 are divided by it. **(Pradnya 5, 1986/5)**

Let the greatest number be x. Let the same remainder be r.

$$\underbrace{494 \equiv r\ (mod\ x)}_{Equation\ I}, \quad \underbrace{726 \equiv r\ (mod\ x)}_{Equation\ II}, \quad \underbrace{1045 \equiv r\ (mod\ x)}_{Equation\ III}$$

Subtract Equation I from Equation II:

$$232 \equiv 0(mod\ x)$$

Subtract Equation II from Equation III:

$$319 \equiv 0(mod\ x)$$

Subtract Equation I from Equation III:

$$551 \equiv 0(mod\ x)$$

$$HCF(232,319) = HCF(232,87) = \underbrace{HCF(58,87)}_{232-87\times2=58} = 29$$
$$HCF(551,29) = 29$$

Example 2.76: Finding the Values that x can take

A group of schools goes to a theme park. The first school has 96 students. The second school has 48 students. The third school has 54 students. The theme park has a ride with cars allowing different numbers of students to sit. Each car has capacity for more than one student, and the cars comes in three sizes: small, medium and large. Independent of the choice of size of car, it is found that the students of each school can exactly fit (filling up each car) into an integer number of cars (so long as students of one school each choose to sit in the same size car). What are the possible sizes of the car?

Let the size of car be s

$$\underbrace{96 \equiv 0(mod\ s)}_{s\ |\ 96}, \quad \underbrace{48 \equiv 0(mod\ s)}_{s\ |\ 48}, \quad \underbrace{54 \equiv 0(mod\ s)}_{s\ |\ 54}$$

$$\underbrace{HCF(96,48,54) = HCF(2^5 \times 3, 2^4 \times 3, 2 \times 3^3) = 2 \times 3 = 6}_{x\ must\ be\ a\ factor\ of\ HCF(96,48,54)} \Rightarrow \text{Factors of } 6 = \{\mathbf{1}, 2,3,6\} \Rightarrow \text{Car size} = \{2,3,6\}$$

Example 2.77: Finding the value of x

x is a two-digit number that divides 230, 345 and 805, leaving no remainder. What is the value of x?

$$\underbrace{230 \equiv 0(mod\ x)}_{x \mid 230},\quad \underbrace{345 \equiv 0(mod\ x)}_{x \mid 345},\quad \underbrace{805 \equiv 0(mod\ x)}_{x \mid 805}$$

$$\underbrace{HCF(230,345,805) = HCF(2\times 5\times 23, 3\times 5\times 23, 5\times 7\times 23) = 5\times 23 = 115}_{x\ must\ be\ a\ factor\ of\ HCF(230,345,805)}$$

$$\text{Factors of } 115 = \{1,5,23,115\} \Rightarrow x = 23$$

Example 2.78

If the remainder is non-zero, but common, it can be converted into zero by subtraction from each number.
x is a number that divides 22, 42 and 72, while leaving remainder 2? Find the:

A. Values that x can take.
B. Number of values that x can take
C. Largest value that x can take
D. Value of x if it is an odd prime number

$$22 \equiv 2(mod\ x), 42 \equiv 2(mod\ x), 72 \equiv 2(mod\ x)$$

Subtract 2 from each congruence to get:

$$20 \equiv 0(mod\ x), 40 \equiv 0(mod\ x), 70 \equiv 0(mod\ x)$$

$$HCF(22-2, 42-2, 72-2) = HCF(20,40,70) = 10 \Rightarrow Factors\ of\ 10 = \{\mathbf{1}, \mathbf{2}, 5, 10\}$$

$$Part\ A: Values\ that\ x\ can\ take = \{5, \mathbf{10}\}$$

$$Part\ B: Number\ of\ Values = 2$$

$$Part\ C: Largest\ Value = 10$$

$$Part\ D: Value\ of\ x\ if\ it\ is\ an\ odd\ prime\ number = 5$$

E. LCM Properties

Questions on LCM require calculating the possible value, or values, of the number that is being divided.

Smallest Number

Suppose, on dividing x by a, b, and c, we get no remainder. We can write

$\underbrace{x \equiv 0\ (mod\ a)}_{a \mid x}$, $\underbrace{x \equiv 0\ (mod\ b)}_{b \mid x}$, $\underbrace{x \equiv 0\ (mod\ c)}_{c \mid x} \Leftrightarrow a, b, c$ are factors of $x \Leftrightarrow x$ is a multiple of a, b, c

Smallest such x

$$= \boldsymbol{Min(x) = LCM(a,b,c).}$$

x is also valid if it is a multiple of the LCM. That is x satisfies

$$\boldsymbol{z \times LCM(a,b,c), z \in N}$$

- We can use the property above to find values of x larger than the smallest.
- Values which satisfy x form an arithmetic progression
  - ✓ Recall that the difference two values of arithmetic progression is constant.
  - ✓ We can use this to find the number of values of x.
- If we are given information restricting the value of x, we can find one or more values satisfying x.

Smallest Number

Suppose, on dividing x by a, b, and c, we get common remainder r. We can write

$\underbrace{x \equiv r\ (mod\ a)}_{a \mid x-r}$, $\underbrace{x \equiv r\ (mod\ b)}_{b \mid x-r}$, $\underbrace{x \equiv r\ (mod\ c)}_{c \mid x-r} \Rightarrow \underbrace{a, b, c \mid x-r}_{a,b,c\ divide\ (x-r)} \Rightarrow x - r$ is a multiple of a, b, c

Smallest such x

$$= \boldsymbol{LCM(a,b,c) + r.}$$

Numbers Larger than the Smallest

If the remainders on dividing x by a, b, and c are r, but we no longer want the smallest number then we will need to add multiples of the LCM till we get to the number that we want.

Example 2.79

What is the smallest positive number that is divisible by 12, 16 and 20?

$$\underbrace{x \equiv 0(mod\ 12)}_{x=12a}, \quad \underbrace{x \equiv 0(mod\ 16)}_{x=16b}, \underbrace{x \equiv 0(mod\ 20)}_{x=20c} \Rightarrow Min(x) = LCM(12,16,20) = 240$$

Example 2.80: Numbers beyond the smallest

x is a positive number that is divisible by 4, 5 and 6. What is the:

A. smallest value of x?
B. third smallest value of x?
C. sum of the smallest four-digit value of x, and the largest three-digit value of x?

We must find x which satisfies the following three equations:

$$\underbrace{x \equiv 0(mod\ 4)}_{x=4a}, \quad \underbrace{x \equiv 0(mod\ 5)}_{x=5b}, \quad \underbrace{x \equiv 0(mod\ 6)}_{x=6c}$$

This means that

$$x = z \times lcm(4,5,6) = 60z$$

Hence, the smallest value is at

$$z = 1 \Rightarrow x = 60$$

And the third smallest value is at:

$$z = 3 \Rightarrow \ x = 180$$

$$16 \times 6 = 96 \Rightarrow 16 \times 60 = 960$$

$$Part\ C\text{: } \underbrace{x_1 = 16 \times 60 = 960}_{Largest\ 3-digit\ Value}, \quad \underbrace{x_2 = 17 \times 60 = 1020}_{Smallest\ 4-digit\ Value} \Rightarrow Sum = x_1 + x_2 = 960 + 1020 = 1980$$

Example 2.81: Non-zero, but common Remainder

x is a positive number that leaves remainder one when divided by 5, 6 and 10. What is the:

A. smallest possible value of x?
B. third smallest possible value of x?
C. sum of the smallest two-digit value of x, and the largest three-digit value of x?

$$x \equiv 1(mod\ 5), \quad x \equiv 1(mod\ 6), x \equiv 1(mod\ 10)$$

Subtract 1 from both sides of each congruence above:

$$x - 1 \equiv 0(mod\ 5), \quad x - 1 \equiv 0(mod\ 6), \quad x - 1 \equiv 0(mod\ 10)$$

Since $x - 1$ must be a multiple of each of these numbers:

$$x - 1 = 5a = 6b = 10c = z \times lcm(5,6,10)$$

$$\underbrace{x - 1 = 0 \Rightarrow x = 1}_{Part\ A\text{: } z=0}, \quad \underbrace{2 \times lcm(5,6,10) + 1 = 2 \times 30 + 1 = 61}_{Part\ B\text{: } z=2}$$

$$Part\ C\text{: } \underbrace{lcm(5,6,10) + 1 = 30 + 1 = 31}_{Smallest\ Two\ Digit\ Value\text{:}z=1}, \quad \underbrace{990 + 1 = 991}_{Largest\ Three\ Digit\ Value} \Rightarrow Sum = 31 + 991 = 1022$$

F. Converting Shortfall to Remainder

If the numbers are expressed in terms of shortfall to reach the next multiple (they can sometimes be converted into having the same remainder) by adding the mod value.
Shortfall can be represented conceptually using negative values of mod, which can then be converted into

positive values of mod, if required.

Example 2.82
Madhav packed chocolates in boxes of five, and found that he had two less than needed to fill the last box. What is the number of chocolates in the last box?

$c \equiv -2(mod\ 5) \Rightarrow c \equiv 3(mod\ 5) \Rightarrow$ Last box had 3 chocolates

Example 2.83
A school has students in three different classrooms. The first classroom has benches with a capacity of three students each. The second classroom and the third classroom have benches with a capacity of four, and five students each. All benches in all classrooms are occupied. Three packets of sweets (each with x sweets) are distributed, one in each classroom, with one sweet handed out to each student. The sweets are one less than required in the first classroom, two less than required in the second classroom, and three less than required in the third classroom. What is the minimum number of students in the school?

$$x \equiv -1(mod\ 3) \Rightarrow \underbrace{x \equiv 2(mod\ 3)}_{\textit{Add 3 on the RHS}} \Rightarrow \underbrace{x-2 \equiv 0(mod\ 3)}_{\textit{Subtract 2 from both sides}}$$
$$x \equiv -2(mod\ 4) \Rightarrow \underbrace{x \equiv 2(mod\ 4)}_{\textit{Add 4 on the RHS}} \Rightarrow \underbrace{x-2 \equiv 0(mod\ 4)}_{\textit{Subtract 2 from both sides}}$$
$$x \equiv -3(mod\ 5) \Rightarrow \underbrace{x \equiv 2(mod\ 5)}_{\textit{Add 5 on the RHS}} \Rightarrow \underbrace{x-2 \equiv 0(mod\ 5)}_{\textit{Subtract 2 from both sides}}$$

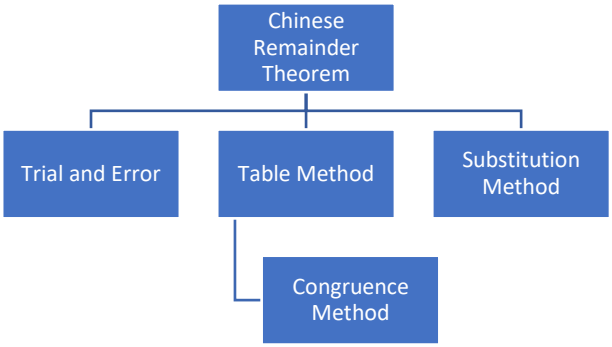
$$\underbrace{(x-2) = 3a = 4b = 5c}_{\textit{(x−2) is a multiple of 3,4,and 5}} \Rightarrow Min(x-2) = lcm(3,4,5) = 60 \Rightarrow x = 60 + 2 = 62\ Sweets$$
$$\underbrace{x+1}_{\substack{\textit{Student}\\ \textit{1st Classroom}}} + \underbrace{x+2}_{\substack{\textit{Students}\\ \textit{2nd Classroom}}} + \underbrace{x+3}_{\substack{\textit{Students}\\ \textit{3rd Classroom}}} = 63 + 64 + 65 = 192$$

G. Chinese Remainder Theorem
Till now, we were looking at how to solve linear congruences. There are some similarities, and some differences between linear congruences, and linear equations.

- Not all rules that apply to linear equations apply to linear congruences.
  - ✓ Division on both sides of a linear congruence is not allowed.
- Also, there are some additional rules that do not apply to linear equations, but apply to linear congruences.
  - ✓ Adding only the value of a mod to either side of a linear congruence is allowed.

Just as we can solve systems of linear equations simultaneously, we can also solve systems of congruences simultaneously. In the prior two sections, we have been doing with the help of HCF and LCM. HCF and LCM only work in special cases, but reduce our work when we are able to apply them.
We now turn our attention to the general case, where we are not in a position to use HCF/LCM.

H. Methods of Solving for x
While the Chinese Remainder Theorem, guarantees a solution, it does not provide an algorithm for arriving at the solution. There are multiple methods of finding the value of x, and the choice of method depends on the question and the preference of the solver.



I. Arithmetic Series (using Table Method)

If you have two arithmetic sequences:

$$\left\{\underbrace{a_1, a_1+d_1, a_1+2d_1, \dots.}_{First\ Term=a_1, Common\ Difference=d_1}\right\}, \quad \left\{\underbrace{a_2, a_2+d_2, a_2+2d_2, \dots.}_{First\ Term=a_2, Common\ Difference=d_2}\right\}$$

First Common Term

To find the first common term, you will need to either:

- Engage in some trial and error
- Use the Chinese Remainder Theorem

Common difference of Common Sequence

Once you find the first common term, finding further common terms is easier.

Terms common to both arithmetic sequences form an arithmetic sequence with common difference

$$\boldsymbol{lcm\ (d_1, d_2)}$$

Example 2.84: Common Arithmetic Sequence using Chinese Remainder Theorem

Find the $\underbrace{\text{smallest number}}_{x}$ greater than 500 that belongs to both arithmetic sequences below:

$$S_1 = \{3,7,11,15, \dots\}, \qquad S_2 = \{5,12,19,26, \dots\}$$

Trial and Error: First Term and Common Difference

Let the sequence of terms which are common to both sequences have first term a_c, and common difference d_c

$$\underbrace{\{3,7,11,15, \mathbf{19}, \dots\}}_{a_1=3, d_1=4}, \qquad \underbrace{\{5,12, \mathbf{19}, 26, \dots\}}_{a_2=5, d_2=7} \Rightarrow a_c = 19 \in \{S_1, S_2\}, \qquad d_c = lcm(4,7) = 28$$

The further common terms will be:

$$\{19 + 28 \times 0, 19 + 28, 19 + 28 \times 2, \dots\} = \{19, 47, 75, \dots\}$$

Note that each term in the sequence is $19 (mod\ 28)$.

Therefore, we find the multiple of 28 closest to 500.

$$28 \times 1 = 28 \Rightarrow \underbrace{28 \times 10 = 280}_{Multiply\ by\ 10} \Rightarrow \underbrace{28 \times 20 = 560}_{Multiply\ by\ 2} \Rightarrow \underbrace{28 \times 20 + 19 = 579}_{Add\ 19} \Rightarrow \underbrace{28 \times 18 + 19 = 523}_{\substack{Subtract\ 28\times 2=56 \\ from\ both\ sides}}$$

Chinese Remainder Theorem: Table Method

We use the Chinese Remainder Theorem to find the first common term. Other parts of the solution are the same as the prior method.

$$S_1 = \underbrace{\{3, 3+4, 3+8, 3+12 \dots\}}_{a_1=3, d_1=4}, \qquad S = \underbrace{\{5, 5+7, 5+12, 5+19, \dots\}}_{a_2=5, d_2=7}$$

A number in the first sequence satisfies:

$$x \equiv 3 (mod\ 4)$$

A number in the second sequence satisfies:

$$x \equiv 5 (mod\ 7)$$

A number in both sequences satisfies both simultaneously:

$$\underbrace{x \equiv 19(mod\ 28)}_{\textit{See table for working}}$$

Satisfying the First Condition:

We want a number which is $3(mod\ 4)$. But we also want the number to be $5(mod\ 7)$. It is difficult to find numbers that satisfy both conditions directly.
So, we break the problem down.
We first find a number that satisfies $3(mod\ 4)$, without disturbing the value $mod\ 7$. The only number that not change the $mod\ 7$ is $0(mod\ 7)$.

Hence, we need to find a number (call it y) that satisfies:

$$0(mod\ 7)\ and\ 3(mod\ 4)$$

Satisfying the Second Condition:

Similar to the earlier logic, we want a number that is $5(mod\ 7)$. If I add multiples of 4 to it, the value $mod\ 4$ will not change. Hence, let's find a number (call it z) that satisfies:

$$5(mod\ 7)\ and\ 0(mod\ 4)$$

$$\therefore y + z = 5(mod\ 7)\ and\ 3(mod\ 4)$$

We use the table below to find y and z:

Final Number	Number	$(mod\ 4)$	Number	$(mod\ 7)$	Final Number
$y = 7$	7	**3**	4	4	
	14	2	8	1	
	21	1	12	5	$z = 12$
		7		5	7+12=19

Chinese Remainder Theorem: Congruence Method

We can do the same calculations as the table method, but present them differently:

$$\mathbf{7 \equiv 3(mod\ 4)}$$

$$4 \equiv 4(mod\ 7), \qquad 4 \times 2 \equiv 8 \equiv 1(mod\ 7), \qquad 4 \times 3 \equiv \mathbf{12 \equiv 5(mod\ 7)}$$

$$x \equiv 7 + 12 \equiv 19 \equiv 3(mod\ 4) \equiv 5\ (mod\ 7)$$

By the Chinese Remainder Theorem, any value of x that we find is unique $mod\ (4 \times 7) = mod\ 28$

$$\therefore x \equiv 19(mod\ 28)$$

Chinese Remainder Theorem: Substitution Method

First Congruence

The first congruence that we need to satisfy is given below. This congruence can be converted into an equation:

$$x \equiv 3(mod\ 4) \Rightarrow x = 3 + 4t, \qquad t \in \mathbb{Z}$$

Second Congruence

The number that we want to find must also satisfy a second congruence. Substitute the value of x from the first congruence into the second congruence:

$$x \equiv 5(mod\ 7) \Rightarrow 3 + 4t \equiv 5(mod\ 7) \Rightarrow 3 + 4t \mathbf{-3} \equiv 5 \mathbf{-3}(mod\ 7) \Rightarrow 4t \equiv 2(mod\ 7)$$

Divide both sides of the congruence by 2, and hence also divide the mod by $HCF(2,7)$:

$$\frac{4t}{2} \equiv \frac{2}{2}\left(mod\ \frac{7}{HCF(2,7) = 1}\right) \Rightarrow 2t \equiv 1(mod\ 7) \Rightarrow t = 4$$

Substitute Value of t in the first congruence

$$x = 3 + 4t = 3 + 4 \times 4 = 19$$

By the Chinese Remainder Theorem, any value of x that we find is unique $mod\ (4 \times 7) = mod\ 28$

$$\therefore x \equiv 19(mod\ 28)$$

J. Word Problems

Example 2.85

I have x chocolates (where x is a two-digit number). One chocolate would be left over when they are shared among three people. Two chocolates would be left over when they are shared among four people. Find the number and the sum of the possible values of chocolates.

$$x \equiv 1 \equiv -2(mod\ 3), x \equiv 2 \equiv -2(mod\ 4) \Rightarrow x \equiv -2 \equiv 10(mod\ 12)$$

Chinese Remainder Theorem: Table Method

$$x \equiv 2(mod\ 4), x \equiv 1(mod\ 3)$$

Final Number	Number	Number $(mod\ 4)$	Number	Number $(mod\ 3)$	Final Number
	3	**3**	4	1	4
6	6	2			
		2		1	6+4=10

Chinese Remainder Theorem: Substitution Method

$$x \equiv 2(mod\ 4) \Rightarrow \underbrace{3m+1}_{x=3m+1} \equiv 2\ (mod\ 4) \Rightarrow \underbrace{3m \equiv 1(mod\ 4)}_{Subtract\ 1\ from\ both\ sides} \Rightarrow m = 3$$

$$m \equiv 3 \equiv 7 \equiv 11 \equiv \cdots \equiv 31(mod\ 4)$$

$$x = 3m + 1 \in \{3 \times 3 + 1, 3 \times 7 + 1, 3 \times 11 + 1, \dots\} = \{10, 22, 34, \dots, 94\}$$

Difference in successive values of x is $LCM(3,4) = 12$.

$$Number\ of\ values = n\{3, 7, 11, \dots 31\} = n\{4, 8, 12, \dots, 32\} = n\{1, 2, 3, \dots, 8\} = 8$$

$$\underbrace{10 + 22 + 34 + \cdots + 94}_{\substack{Arithmetic\ Series \\ a=10, d=12, n=8}} \Rightarrow Sum = n\left(\frac{f+l}{2}\right) = 8\left(\frac{10+94}{2}\right) = 8 \times 52 = 416$$

K. Restrictions on the solution

Example 2.86

The marching band has more than 100 members but fewer than 200 members. When they line up in rows of 4 there is one extra person; when they line up in rows of 5, there are two extra people, and when they line in rows of seven there are three extra people. How many members are there in the marching band? (Mathcounts 2008 National Teams)

Manipulation Method

$$x \equiv 1 \equiv -3(mod\ 4), x \equiv 2 \equiv -3(mod\ 5) \Rightarrow x \equiv -3 \equiv 17(mod\ 20)$$

$$17 \equiv 3(mod\ 7)$$

Hence, 17 is the smallest number that satisfies all three congruences above. The next number that satisfies all three congruences will be

$$17 + lcm(4,5,7) = 17 + 140 = 157$$

This also satisfies the condition that

$$100 < x < 200$$

Hence, the final answer is

$$157$$

Chinese Remainder Theorem: Congruence Method

$$x \equiv 1(mod\ 4), \qquad x \equiv 2(mod\ 5), \qquad x \equiv 3(mod\ 7)$$

$$5 \times 7 \equiv 35 \equiv 3(mod\ 4) \Rightarrow 3 \times 3 \equiv 9 \equiv 1(mod\ 4) \Rightarrow 35 \times 3 \equiv \mathbf{105} \equiv 1(mod\ 4)$$
$$4 \times 7 \equiv 28 \equiv 3(mod\ 5) \Rightarrow 3 \times 4 \equiv 12 \equiv 2(mod\ 5) \Rightarrow 28 \times 4 \equiv \mathbf{112} \equiv 2(mod\ 5)$$
$$4 \times 5 \equiv 20 \equiv 6 \equiv -1(mod\ 7) \Rightarrow (-3)(20) \equiv \mathbf{-60} \equiv (-1)(-3) \equiv 3(mod\ 7)$$

$$x \equiv 105 + 112 - 60 \equiv 157(mod\ 140)$$

L. Removing the co-prime condition

If the co-prime condition does not hold, we are not guaranteed a solution. However, if a solution does exist, then it is unique.

Example 2.87

M. Creating Congruence Systems

So far we have seen how to use the Chinese Remainder Theorem to solve a system of congruences. However, the theorem can also be used to solve questions that are not directly framed in terms of solving systems. For example, we can break a question on remainders to remainders of smaller co-prime factors. First, we see this method in action in the familiar context of divisibility, and then apply it to remainders.

Divisibility is done by checking numbers that:

- Multiply together to get the number that we want
- Are pair-wise co-prime.

To find these numbers, we find the prime factors of each number

- In most cases, checking for each prime separately is best
- In some special cases (for example, 10 or 100), mixing the primes works

2.88:

$$x = p_1^a p_2^b \dots p_n^z$$
$$\boldsymbol{Divisibility\ by\ x \Leftrightarrow Divisibility\ by\ co-prime\ factors\ of\ x\ that\ multiply\ to\ x}$$

So, to check for divisibility, we need to **break the number into co-prime factors**.

Example 2.89: Stating the Divisibility Test

State the divisibility test for the following three numbers: 88; 18; 180
$88 = 2^3 \times 11$, check for divisibility by 8 and 11
$18 = 2 \times 3^2$, check for divisibility by 2 and 9
$180 = 2^2 \times 3^2 \times 5$, check for divisibility by 4, 9 and 5

2.90:

To find the remainder

$$x(mod\ m), m = p_1 \times p_2$$

We find

$$x(mod\ p_1) = a \Rightarrow x \equiv a(mod\ p_1)$$
$$x(mod\ p_2) = b \Rightarrow x \equiv b(mod\ p_1)$$

And then apply the Chinese Remainder Theorem to find c such that

$$x \equiv c(mod\ p_1p_2) \Leftrightarrow x \equiv c(mod\ m)$$

Example 2.91: Remainders

When is the remainder when $x = 12345678987654322$ is divided by 495?

$$495 = 5 \times 9 \times 11$$

Find Remainders for Co-prime Factors

Find the remainder when x is divided by each prime factor above:

$$\text{Divided by 5: } x \equiv 2(mod\ 5)$$
$$\text{Divided by 9: } \underbrace{x \equiv 1(mod\ 9)}_{Sum\ of\ Digits}$$
$$\text{Divided by 11: } x \equiv \underset{+1}{\underbrace{1}}\ \underset{+1}{\underbrace{23}}\ \underset{+1}{\underbrace{45}}\ \underset{+1}{\underbrace{67}}\ \underset{+1}{\underbrace{89}}\ \underset{-1}{\underbrace{87}}\ \underset{-1}{\underbrace{65}}\ \underset{-1}{\underbrace{43}}\ \underset{0}{\underbrace{22}} \equiv 2(mod\ 11)$$

Apply the Chinese Remainder Theorem

Combine the above three using the Chinese Remainder Theorem:

$$\underbrace{x \equiv 442(mod\ 495)}_{See\ Table\ Below\ for\ Working}$$

Final Number	Number	Number (mod 5)	Final Number	Number	Number (mod 9)	Number	Number (mod 11)	Final Number
	99	4	55	55	**1**	45	1	
	198	3				90	2	
297	297	2						
		2			1		2	442

Example 2.92: General Number Bases

2.93: Euler's Totient Theorem

If a and n are coprime positive integers, then

$$a^{\phi(n)} \equiv 1\ (mod\ n)$$

Example 2.94

Determine the ten's digit of 17^{1993}. (MathCounts 1994 Workout 10)

We find the last two digits, which is the same as finding mod 100. Factorize 100 into two coprime factors:

$$17^{1993}(mod\ 100) = 17^{1993}(mod\ 4 \times 25)$$

Working mod 4 is short:

$$17^{1993} \equiv 1^{1993} \equiv 1(mod\ 4)$$

Working mod 25 is lengthier. By Euler's Totient Theorem $17^{\phi(25)} \equiv 17^{25\left(1-\frac{1}{5}\right)} \equiv 17^{20} \equiv 1(mod\ 25)$:

$$17^{1993} \equiv 17^{1993\ (mod\ 20)} \equiv 17^{13}(mod\ 25)$$

Split into an even power and an odd power and reduce twice:

$$17^{13} \equiv (-8)^{13} \equiv (-8)^{12}(-8) \equiv 64^6(-8) \equiv (-11)^6(-8) \equiv 121^3(-8)(mod\ 25)$$

Simplify 121 (mod 25), cube and simplify:

$$(-4)^3(-8) \equiv (-64)(-8) \equiv (-14)(-8) \equiv 112 \equiv 12$$

By the Chinese Remainder Theorem, we need to find the unique value $n\ mod$ 100 that satisfies

$$n \equiv 1\ (mod\ 4), n \equiv 12(mod\ 25)$$
$$12 \equiv 0\ (mod\ 4)$$
$$12 + 25 = 37 \equiv 1(mod\ 4) \Rightarrow Works$$

Hence,

$$Last\ two\ digits\ of\ 17^{1993} = 37$$
$$Ten's\ Digit = 3$$

Example 2.95
What is the hundreds digit of 2011^{2011}? **(AMC 10B 2011/23)**

Since $2011 \equiv 11\ (mod\ 1000)$:
$$2011^{2011} \equiv 11^{2011} (mod\ 1000)$$
Since $\phi(1000) = 1000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 400$:
$$\equiv 11^{2011\ (mod\ 400)} \equiv 11^{11} (mod\ 1000) \equiv 11^{11} (mod\ 8 \times 125)$$
Working $mod\ 8$ and using $\phi(8) = 4 \Rightarrow 3^4 \equiv 1 (mod\ 8)$:
$$11^{11} \equiv 3^{11} \equiv 3^{11\ (mod\ 4)} \equiv 3^3 \equiv 27 \equiv 3$$
Working $mod\ 125$:
$$11^{11} \equiv (11^{10})(11) \equiv (121^5)(11) \equiv (-4)^5(11) \equiv (-1024)(11) \equiv (-24)(11) \equiv (-264) \equiv 111$$
By the Chinese Remainder Theorem, we need to find the unique value $n\ mod\ 1000$ that satisfies
$$n \equiv 3\ (mod\ 8), n \equiv 111 (mod\ 125)$$
Note that
$$111 \equiv 7 (mod\ 8)$$
$$125 \equiv 5 (mod\ 8)$$
Since $7 + 5 \times 4 = 27 \equiv 3 (mod\ 8)$:
$$111 + 125 \times 4 = 111 + 500 = 611\ satisfies\ both\ conditions$$
Hence:
$$2011^{2011} \equiv 611 (mod\ 1000) \Rightarrow Last\ Digit\ is\ 6.$$

N. Congruences with more than one Variable

2.3 Multiplication and Exponentiation

2.96: Property I: Multiplying Both Sides
Multiplying both sides of a congruence by the same number is valid.
$$\boldsymbol{a \equiv b (mod\ x) \Rightarrow \underbrace{ma \equiv mb (mod\ x)}_{\text{Multiply both sides by m}}}$$

Example 2.97
If $x \equiv 3 (mod\ 11)$, then find $10x (mod\ 11)$

Multiply both sides by 10
$$\mathbf{10} \times x \equiv 3 \times \mathbf{10}\ (mod\ 11)$$
$$10x \equiv 30 \equiv -3 \equiv 8 (mod\ 11)$$

Example 2.98
Eight pirates are sharing seven boxes of gold coins (with each box having x coins), and have two gold coins left over after the equal sharing. If each gold coin is split into seven smaller gold coins, what is the number of gold coins that will be left over after sharing equally?

Method I: Mod Arithmetic
$$7x \equiv 2 (mod\ 8)$$

Multiply both sides by 7:

$$49x \equiv 2 \times 7 (mod\ 8)$$
$$49x \equiv 14 \equiv 6 (mod\ 8)$$

Method II: Logic

$$2\ coins\ extra\ from\ 7\ boxes \rightarrow 14\ coins\ extra\ from\ 49\ boxes$$

Give one coin to each pirate from the 14 extra:

$$\underbrace{6\ coins\ extra}_{Six\ coins\ left\ over}$$

Example 2.99

A bank issued credit card numbers and the corresponding PIN (Personal Identification Number). Both are 3-digit numbers upto 996. Pinaki was the last to get the card, and so he had the last possible credit card number. He was afraid of forgetting his PIN. He wrote down number 123 in his diary to remember his PIN. He also wrote out the way to calculate 123: "Multiply the card number by PIN. Divide the product by 997. The remainder is 123." Once Prafull saw his diary in which Pinaki wrote this number 123. Prafull did a lot of purchasing, as he now knows Pinaki's PIN. What is Pinaki's PIN? **(JMET)**

We know that

$$\frac{996p}{997}\ has\ Remainder\ 123$$

Hence:

$$996p - 123\ is\ divisible\ by\ 997$$

Hence,

$$997p - x - 123\ is\ also\ divisible\ by\ 997$$
$$997p - (x + 123)\ is\ also\ divisible\ by\ 997$$

Hence, since 997p is divisible by 997, so must the remaining term be:

$$p + 123 = 997k$$

Smallest value of x is

$$p = 997 - 123 = 874$$

Solve the above question using Mod Arithmetic

$$996p \equiv 123\ (mod\ 997)$$

Add p:

$$-p \equiv 123\ (mod\ 997)$$
$$p \equiv -123\ (mod\ 997)$$

Add 997 to both sides:

$$p \equiv 874\ (mod\ 997)$$

2.100: Property I: Distributive

$$xy (mod\ n) \equiv [x (mod\ n) \times y (mod\ n)]$$

You can distribute the taking of a mod over a product. Instead of taking the product first, take the mod of each term, and then multiply the products.

Example 2.101

Find

$$2021 \times 2022 \times 2023 \times 2024 (mod\ 202)$$

Apply the distributive property:

$$\underbrace{2021(mod\ 202)}_{2021\equiv 2020+1\equiv 1} \times \underbrace{2022(mod\ 202)}_{\equiv 2} \times \underbrace{2023(mod\ 202)}_{\equiv 3} \times \underbrace{2024(mod\ 202)}_{\equiv 4}$$

Simplify:

$$1 \times 2 \times 3 \times 4 \equiv 4! \equiv 24\ (mod\ 202)$$

Example 2.102

Find

$$271^2(mod\ 273)$$

$$271^2 \equiv 271 \times 271 \equiv \underbrace{(-2) \times (-2)}_{\textit{Using the distributive property}} \equiv 4(mod\ 273)$$

A. Combining Distributive Properties

Expressions involving a combination of multiplication and addition can be solved by coming the two distributive properties.

Example 2.103: Distributive Property

Find

$$31543^2 + 31544^2 + 31545^2 + 31546^2(mod\ 11)$$

Apply the distributive properties of multiplication and addition to get:

$$6^2 + 7^2 + 8^2 + 9^2 \equiv (-5)^2 + (-4)^2 + (-3)^2 + (-2)^2 \equiv 25 + 16 + 9 + 4 \equiv 3 + 5 - 2 + 4 \equiv 10(mod\ 11)$$

B. Algebra with Modular Arithmetic: Substituting Variables

Similar to regular algebra, we can make use of variables in modular arithmetic expressions and congruences. Pay special attention to the second example below where the substitution is not immediately obvious.

Example 2.104

Find the remainder in $\frac{x(x+1)(x+2)(x+3)}{x-2}$ if $x = 2020$

Finding the remainder of $\left(\frac{p}{q}\right)$ is equivalent to finding $p\ (mod\ q)$.

$$R\left(\frac{x(x+1)(x+2)(x+3)}{x-2}\right) = [x(x+1)(x+2)(x+3)]\ \big(mod\ (x-2)\big)$$

Substitute the value of x:

$$\equiv 2020 \times 2021 \times 2022 \times 2023(mod\ 2018)$$

Apply the distributive property:

$$2 \times 3 \times 4 \times 5 \equiv 5! \equiv 120(mod\ 2018)$$

Example 2.105: Substituting variables in congruences

For a certain natural number n, n^2 gives a remainder of 4 when divided by 5, and n^3 gives a remainder of 2 when divided by 5. What remainder does n give when divided by 5? (MathCounts 2003 State Sprint)

Start with the second statement, and expand it:

$$n^3 \equiv 2(mod\ 5)$$
$$n \times n^2 \equiv 2(mod\ 5)$$
$$\underbrace{4n \equiv 2(mod\ 5)}_{n^2\equiv 4(mod\ 5)}$$
$$-n \equiv 2(mod\ 5)$$

$$n \equiv 3(mod\ 5)$$

C. Breaking up an exponent

Example 2.106

For natural numbers x and y, write $73^{123,456}$ in the form

$$(73^{10})^x \times 73^y$$

$$123{,}456 \equiv 6(mod\ 10) \Rightarrow 123{,}456 = 12345 + 6$$

$$(73^{10})^{12345} \times 73^6$$

2.107: Exponentiation Property I

$$a \equiv b(mod\ c) \Leftrightarrow \underbrace{a^m \equiv b^m(mod\ c)}_{\substack{Converting\ multiplication \\ into\ exponentiation}}$$

Exponentiation is repeated multiplication. Multiplication (on both sides of a congruence) is allowed, therefore, by repeated application of multiplication, exponentiation is also allowed.

Let

$$a \equiv b(mod\ c)$$

Multiply both sides repeatedly by a and b (which we can since they are equal $(mod\ c)$):

$$a \cdot a \cdot \ldots \cdot a \equiv b \cdot b \cdot \ldots \cdot b(mod\ c)$$

Rewrite the multiplication as exponentiation:

$$\boldsymbol{a^m \equiv b^m(mod\ c)}$$

D. Finding 1

If some power gives 1 $(mod\ m)$, then it becomes easy to work with.
Hence, this is often the strategy that we are looking for.

2.108: Squaring Powers to get 1

$$x^y \equiv -1(\text{mod } p) \Rightarrow (x^y)^2 \equiv (-1)^2 \Rightarrow x^{2y} \equiv 1(\text{mod } p)$$

If we are able to find a power of x that gives us -1 $(mod\ p)$, we can square that power to give us $1(mod\ p)$:

Example 2.109

Find the values of x that satisfy

A. $5^x \equiv 1(mod\ 6)$
B. $5^x \equiv 1(mod\ 7)$
C. $7^x \equiv 1\ (mod\ 11)$

Part A

$$5 \equiv -1\ (mod\ 6)$$

Square both sides of the above congruence:

$$5^2 = 25 \equiv 1\ (mod\ 6)$$

Part B

$$5 \equiv -2 \ (mod\ 7)$$
$$5^2 \equiv (-2)(5) \equiv -10 \equiv -3 \ (mod\ 7)$$
$$5^3 \equiv (-3)(5) \equiv -15 \equiv -1 \ (mod\ 7)$$

Square the first and the last:

$$5^6 \equiv 1 \ (mod\ 7)$$

Part C

$$7^2 \equiv 49 \equiv 5 \ (mod\ 11)$$
$$7^3 \equiv 5(7) \equiv 35 \equiv 2 \ (mod\ 11)$$
$$7^4 \equiv 2(7) \equiv 14 \equiv 3 \ (mod\ 11)$$
$$7^5 \equiv 3(7) \equiv 21 \equiv -1 \ (mod\ 11)$$
$$7^{10} \equiv (-1)(-1) \equiv \ (mod\ 11)$$

Example 2.110

$$a^x \equiv -1(\text{mod } 219)$$

Given the above, find n such that

$$a^n \equiv 1(\text{mod } 219)$$

Square both sides:

$$a^x \times a^x \equiv (-1)(-1)(\text{mod } 219)$$
$$a^{2x} \equiv 1(\text{mod } 219)$$
$$n = 2x$$

2.111: Cyclicity of Mod

$$x^y \equiv 1(mod\ m) \Rightarrow \underbrace{(x^y)^n \equiv 1(mod\ m)}_{Exponentiate\ both\ sides\ n\ times}$$

Example 2.112

Find R if $R = \{0,1,2,3,4\}$ and

$$\frac{3^{100,000}}{5} = 5Q + R,$$

Check the powers of $3(mod\ 5)$ in order to try to get 1, or -1.

$$3 \equiv 3(\text{mod } 5)$$
$$3^2 = 9 \equiv 4 \equiv -1(\text{mod } 5)$$
$$3^3 = 27 \equiv 2(\text{mod } 5)$$
$$3^4 \equiv 81 \equiv 1(\text{mod } 5)$$

Method I: $3^{100,000} = (3^4)^{25,000} \equiv \underbrace{(1)^{25,000}}_{Substitute\ 3^4 \equiv 1(mod\ 5)} \equiv 1 \ (\text{mod } 5)$

Method II: $3^{100,000} = (3^2)^{50,000} \equiv \underbrace{(-1)^{50,000}}_{Substitute\ 3^2 \equiv -1(mod\ 5)} \equiv 1 \ (\text{mod } 5)$

Example 2.113

Find

$$5^{100,000}(\text{mod } 7)$$

$5^2 = 25 \equiv 4(\text{mod } 7), \quad 5^3 = 125 \equiv -1(\text{mod } 7)$

$$5^{100,000} = \underbrace{5^{99,999} \times 5}_{\textit{Breaking up } 5^{100,000}} = (5^3)^{33,333} \times 5 \equiv (-1)^{33,333} \times 5 \equiv -1 \times 5 \equiv -5 \equiv 2 \ (\text{mod } 7)$$

Example 2.114

Find the cyclicity of $4(mod\ 11)$

So far, we have been finding the mod of the powers of x, as below:

Regular Method	x	x^2	x^3	x^4	x^5	x^6
Number	4	16	64	256	1024	4096
mod 11	4	5	9	3	1	4

However, instead of finding the mod of the power, we can just multiply each mod by the number at each stage of the calculations. These removes the need to calculate large numbers:

$$4 \equiv 4(mod\ 11)$$
$$4^2 \equiv 16 \equiv 5(mod\ 11)$$
$$5 \times 4 \equiv 20 \equiv 9(mod\ 11)$$
$$9 \times 4 \equiv 36 \equiv 3(mod\ 11)$$
$$3 \times 4 \equiv 12 \equiv 1(mod\ 11)$$

E. Fermat's Little Theorem

Fermat's theorem is one of the key results of Number Theory, useful in many, many places. A large number of questions that may or may not seem to be related to the theorem, can be solved by making use of it.

2.115: Fermat's Little Theorem

If p is a prime that does not divide a, *then* $a^{p-1} \equiv 1(\text{mod } p)$

The theorem is very useful because it gives us a number that is $1(mod\ p)$. And once we get 1, we can use it to simplify our calculations.

Proof.

Example 2.116

Show, using the first few numbers, that the Fermat's theorem works for $p = 3$

Let $p = 3 \Rightarrow\ p - 1 = 2$

$$a^{p-1}(mod\ p) = a^2(mod\ 3)$$

Let's try the $(p-1)^{th}$ powers of the first few numbers:

$$\underbrace{2^2 = 4 \equiv \mathbf{1}(\text{mod } 3)}_{a=2},$$
$$\underbrace{3^2 = 9 \equiv 0(\text{mod } 3)}_{a=3}$$
Theorem doesn't apply
$$\underbrace{4^2 = 16 \equiv \mathbf{1}(\text{mod } 3)}_{a=4}$$
$$\underbrace{5^2 = 25 \equiv \mathbf{1}(\text{mod } 3)}_{a=5}$$
$$\underbrace{6^2 = 36 \equiv 0(\text{mod } 3)}_{\textit{Theorem doesn't apply}}$$

Example 2.117

Find $5^{99,939} \pmod{97}$

We could try various powers of 5 (mod 97), but finding a power that gives 1 (mod 97) is not so easy.
By Fermat's Little Theorem:

$$\underbrace{5^{96} \equiv 1 \pmod{97}}_{\because \textit{Fermat's Little Theorem: } a=5, p=97}$$

$$5^{99,939} = \underbrace{(5^{96})^{1041} \times 5^3}_{\textit{Breaking up } 5^{99,939}} \equiv (5^{96})^{1041} \times 5^3 \equiv (1)^{1041} \times 5^3 \equiv 1 \times 5^3 \equiv 125 \equiv 28 (\text{mod } 97)$$

Shortcut: You don't need $99,939 = 96 \times 1041 + 3$. All that matters is the remainder.

$$5^{99,939} \equiv \underbrace{5^3}_{99,939 \equiv 3 (\textit{mod } 96)} \equiv 125 \equiv 28 (\text{mod } 97)$$

F. Euler's Totient Theorem

2.118: Euler's Totient Function

If n is a positive integer, than $\phi(n)$ is the number of positive integers less than or equal to n that are coprime to n.

Example 2.119

Find $\phi(n)$ for the following values of n.

A. $\phi(8)$

$$x \leq 8 \Rightarrow \{1,2,3,4,5,6,7,8\}$$
$$x \leq 8 \;\&\; x \textit{ coprime to } 8 \Rightarrow \{1,3,5,7\}$$
$$\phi(8) = n\{1,3,5,7\} = 4$$

2.120: Euler's Totient Function

If the prime factorization of n is $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Note that the powers in the prime factorization do not appear in the formula. That is, the formula is independent of

$$a_1, a_2, \dots, a_k$$

Example 2.121

Find $\phi(n)$ for the following values of n.

A. 1000

$$1000 = 8 \times 125 = 2^3 \times 5^3$$
$$\phi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 1000\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 400$$

2.122: Euler's Totient Theorem

If a and n are coprime positive integers, then:

$$a^{\phi(n)} \equiv 1 \ (mod\ n)$$

Example 2.123

Determine the ten's digit of 17^{1993}. (MathCounts 1994 Workout 10)

Work $mod\ 100$:

$$100 = 4 \times 25 = 2^2 \times 5^2$$

$$\phi(100) = 100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 40$$

Substitute $a = 17, n = 100$ in Euler's Totient Theorem:

$$17^{\phi(100)} \equiv 1 \ (mod\ 100)$$

$$\underbrace{17^{40} \equiv 1 \ (mod\ 100)}_{Equation\ I}$$

Hence, split 1993 as a multiple of 40, and the remainder:

$$17^{1993} = 17^{1960} \times 17^{33} = (17^{40})^{49} \times 17^{33} \ (mod\ 100)$$

Substitute using Equation I:

$$\equiv 1^{49} \times 17^{33} \equiv 1 \times 17^{33} \equiv 17^{33} \ (mod\ 100)$$

$$17^2 = 289 \equiv 89 \equiv -11 \ (mod\ 100)$$

$$17^3 = (17^2)(17) \equiv (-11)(17) \equiv -187 \equiv 13 \ (mod\ 100)$$

$$17^{33} \equiv (17^3)^{11} \equiv 13^{11}$$

$$\equiv 13^9 \times 13^2 \equiv (13^3)^3 \times 169 \equiv (97)^3 \times 69 \equiv (-3)^3 \times 69 \equiv (-27) \times 69 \equiv -63 \equiv 37 \ (mod\ 100)$$

G. Polynomials

Before starting this section, you should have some background on polynomials. For example, the note on Polynomials in Algebra.

The examples in this section are equivalent to what you can do, with the Remainder Theorem, and the Factor Theorem. However, the presentation is in terms of mod arithmetic, rather than in terms of Algebra.

Example 2.124

Find the remainder when $2x$ is divided by $x - 3$.

$$x - 3 \equiv 0 \ (mod\ x - 3)$$

$$x \equiv 3 \ (mod\ x - 3)$$

$$2x \equiv 6 \ (mod\ x - 3)$$

$$\frac{2x}{x-3} = \frac{2x-6}{x-3} + \frac{6}{x-3} = 2 + \frac{6}{x-3} \Rightarrow Remainder = 6$$

H. Factors

Example 2.125

Find the value of a if $x^2 + 5x + a$ is divisible by $x + 2$.

$$x + 2 \equiv 0 \ (mod\ x + 2)$$

$$x \equiv -2 \ (mod\ x + 2)$$

Since $x^2 + 5x + a$ is divisible by $x + 2$:

$$x^2 + 5x + a \equiv 0 \ (mod\ x + 2)$$

$$(-2)^2 + 5(-2) + a \equiv 0 \ (mod\ x+2)$$
$$-6 + a \equiv 0 \ (mod\ x+2)$$
$$a \equiv 6 \ (mod\ x+2)$$

2.4 Applications of Mod Arithmetic

A. Comparing last digit with mod n

When we found the last digits of numbers in the previous section, we were working mod 10. The same ideas will apply when working with any mod.
We can calculate the cyclicity of numbers for any mod.
0 will have always have cyclicity 1 for any mod.
1 will have always have cyclicity 1 for any mod.

Example 2.126: Calculating the cyclicity

Calculate the cyclicity (and the actual cycle) of the numbers mod 7.

$x(mod\ 7)$	$x^2(mod\ 7)$	$x^3(mod\ 7)$	$x^4(mod\ 7)$	$x^5(mod\ 7)$	$x^6(mod\ 7)$	Cycle	Length of Cycle
0	0	0	0	0	0	0	1
1	1	1	1	1	1	1	1
2	4	$8 \equiv 1$				2,4,1	3
3	$9 \equiv 2$	6	4	5	1	3,2,6,4,5,1	6
4	2	1				4,2,1	3
5	4	6	2	3	1	5,4,6,2,3,1	6
6	1					6,1	3

Application: Primitive Root

In the previous example, we calculated the cyclicity of numbers mod 7. This cyclicity came out to be:

$$\{1,1,3,6,3,6,3\}$$

If a number $x(mod\ n)$ has a cycle of length $n-1$, then all the $n-1$ numbers less than n will be represented in the cycle.
Such a number is called a primitive root of $mod\ n$.

Example 2.127: Calculating the cyclicity

What are the primitive roots mod 10?
As we saw in the table, mod 10 has a maximum cycle of 4. Hence, there are no primitive roots mod 10.

Example 2.128: Working with powers

$$4^{457} \ (mod\ 5)$$
$$4^1 \equiv 4, \quad 4^2 \equiv 1 \Rightarrow Cyclicity = 2$$
$$4^{457} \equiv 4^{456} \times 4 \equiv (4^2)^{228} \times 4 \equiv (1)^{228} \times 4 \equiv 4(mod\ 5)$$

$$2^{341} \ (mod\ 7)$$
$$2^1 \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 1 \Rightarrow Cyclicity = 3$$
$$2^{341} \equiv 2^{339} \times 2^2 \equiv (2^3)^{113} \times 4 \equiv (1)^{113} \times 4 \equiv 1 \times 4 \equiv 4 \ (mod\ 7)$$

$$5^{371} \ (mod\ 8)$$
$$5^1 \equiv 5, \quad 5^2 \equiv 1 \Rightarrow Cyclicity = 2$$
$$5^{371} \equiv 5^{370} \times 5 \equiv (5^2)^{185} \times 5 \equiv (1)^{185} \times 5 \equiv 1 \times 5 \equiv 5(mod\ 8)$$

Example 2.129: Lengthier Calculations

$$6^{718}\ (mod\ 11)$$
$$6^1 \equiv 6, \quad 6^2 \equiv 36 \equiv 3, \quad 6^3 \equiv 6^2 \times 6 \equiv 3 \times 6 \equiv 18 \equiv 7, \quad 6^4 \equiv 6^3 \times 6 \equiv 7 \times 6 \equiv 42 \equiv 9$$
$$6^5 \equiv 6^4 \times 6 \equiv 9 \times 6 \equiv 54 \equiv 10 \equiv -1$$
$$6^{718} \equiv 6^{\overbrace{Odd}^{715}} \times 6^3 \equiv -1 \times 7 \equiv -7 \equiv 4\ (mod\ 11)$$

$$7^{910}\ (mod\ 13)$$
$$7^1 \equiv 7, \quad 7^2 \equiv 10 \equiv -3, \quad 7^3 \equiv 7^2 \times 7 \equiv -3 \times 7 \equiv -21 \equiv 5$$
$$7^4 \equiv 7^3 \times 7 \equiv 5 \times 7 \equiv 35 \equiv -4$$
$$7^5 \equiv 7^4 \times 7 \equiv -4 \times 7 \equiv -28 \equiv -2$$
$$7^6 \equiv 7^5 \times 7 \equiv -2 \times 7 \equiv -14 \equiv -1$$

$$7^{910} \equiv 7^{906} \times 7^4 \equiv (7^6)^{151} \times 7^4 \equiv (-1)^{151} \times 7^4 \equiv -1 \times -4 \equiv 4$$

B. Working with the Base

Example 2.130

C. Base and the Powers

Example 2.131

$$347^{234} - 234^{347}\ (mod\ 7) \equiv 1 - 5 \equiv -4 \equiv 3$$

$$4^{234} \equiv (4^3)^{78} \equiv (1)^{78} \equiv 1$$
$$3^{347} \equiv (3^3)^{115} \times 3^2 \equiv (-1)^{115} \times 3^2 \equiv -1 \times 9 \equiv -9 \equiv 5$$

$$4^1 \equiv 4, \quad 4^2 \equiv 16 \equiv 2, \quad 4^3 \equiv 4^2 \times 4 \equiv 2 \times 4 \equiv 8 \equiv 1$$
$$3^1 \equiv 3, \quad 3^2 \equiv 9 \equiv 2, \quad 3^3 \equiv 2 \times 3 \equiv 6 \equiv -1$$

2.132: Finding mod of squares, cubes, and powers

To find the possible values $x^n(mod\ y)$, we only need to find the values of
$$x^n(mod\ y), 1 < x < y$$
$$0^n \equiv 0(mod\ y), 1^n \equiv 1(mod\ y)$$

Example 2.133: Perfect Squares

Calculate the possible values of a perfect square

A. $mod\ 3$
B. $mod\ 4$

Part A

A number can only be 0,1,2 $(mod\ 3)$. Therefore, any number can be written in one of the forms:

$$3x, \quad 3x+1, \quad 3x+2; x \in N$$

Now we find the squares of the above numbers

$$(3x)^2 \equiv 9x^2 \equiv 0 \ (mod\ 3)$$
$$(3x+1)^2 \equiv 9x^2 + 6x + 1 \equiv 1 \ (mod\ 3)$$
$$(3x+2)^2 \equiv 9x^2 + 12x + 4 \equiv 1 \ (mod\ 3)$$

Any perfect square has to be either $0\ (mod\ 3)$ or $1(mod\ 3)$

Part B

Calculate the possible values of a perfect square $mod\ 3$

$$(4x)^2 \equiv 16x^2 \equiv 0 \ (mod\ 4)$$
$$(4x+1)^2 \equiv 16x^2 + 8x + 1 \equiv 1 \ (mod\ 4)$$
$$(4x+2)^2 \equiv 16x^2 + 16x + 4 \equiv 0 \ (mod\ 4)$$
$$(4x+3)^2 \equiv 16x^2 + 24x + 9 \equiv 1 \ (mod\ 4)$$

Any perfect square has to be either $0\ (mod\ 4)$ or $1(mod\ 4)$

Example 2.134: Perfect Squares *mod* 8

Calculate the possible values of a perfect square $mod\ 8$

$$2^2 \equiv 4 \ (mod\ 8\ )$$

$$3^2 \equiv 9 \equiv 1 \ (mod\ 8\ )$$
$$4^2 \equiv 16 \equiv 0 \ (mod\ 8\ )$$
$$5^2 \equiv 25 \equiv 1 \ (mod\ 8\ )$$
$$6^2 \equiv (-2)^2 \equiv 4 \ (mod\ 8\ )$$
$$7^2 \equiv (-1)^2 \equiv 1 \ (mod\ 8\ )$$

Any perfect square has to be either $0\ (mod\ 8)$ or $1(mod\ 8)$ or $4(mod\ 8)$

Example 2.135: Perfect Cubes

Calculate the possible values of perfect cubes

A. $mod\ 4$
B. $mod\ 6$

Part A

$$2^3 \equiv 8 \equiv\ 0(mod\ 4\ )$$
$$3^3 \equiv (-1)^3 \equiv -1 \equiv 3 \ (mod\ 4\ )$$

Any perfect cube has to be either $0\ (mod\ 4)$ or $1(mod\ 4)$ or $3(mod\ 4)$.
It cannot be $2(mod\ 4)$

Part B

$$2^3 \equiv 8 \equiv 2(mod\ 6\ )$$
$$3^3 \equiv 27 \equiv 3 \ (mod\ 6\ )$$
$$4^3 \equiv (-2)^3 \equiv -8 \equiv 4 \ (mod\ 6\ )$$
$$5^3 \equiv (-1)^3 \equiv -1 \equiv 5 \ (mod\ 6\ )$$

Also, don't forget:

$$0^3 \equiv 0(mod\ 6), 1^3 \equiv 1(mod\ 6)$$

The cube of a number $mod\ 6$ has the same value as the original number.

Example 2.136: Perfect Cubes *mod* 6

$$1^3 + 2^2 + 3^3 + \cdots + 1000^3 (mod\ 6)$$

A number $mod\ 6$ is the same as its cube $mod\ 6$. Therefore, the original expression simplifies to:

$$1 + 2 + 3 + \cdots + 1000 (mod\ 6)$$

We make groups of six:

$$\underbrace{1 + 2 + 3 + 4 + 5 + 6}_{\equiv 1+2+3+4+5+0 \equiv 15 \equiv 3 (mod\ 6)} + \cdots \underbrace{+997 + 998 + 999 + 1000}_{\equiv 1+2+3+4 \equiv 10 \equiv 4 (mod\ 6)} (mod\ 6)$$

Final Answer:

$$3 \times 166 + 4 \equiv 3 \times 4 + 4 \equiv 12 + 4 \equiv 4 (mod\ 6)$$

D. Using Mod in Divisibility

Earlier, we saw examples of how we can use divisibility tests to calculate mod. In this section, we will do it the other way around. We will use the properties of mod, in order to calculate the remainder for numbers which do have a test of divisibility which is very popular.

We are going to look at divisibility by:

- Numbers which consists of only 9's

$$\underbrace{9}_{Nine}, \quad \underbrace{99}_{Ninety-Nine}, \quad \underbrace{999}_{Nine\ Hundred\ Ninety\ Nine}$$

- Numbers which consists of two 1's, with a number of optional zeros in between:

$$\underbrace{11}_{Eleven}, \quad \underbrace{101}_{Hundred\ and\ One}, \quad \underbrace{1001}_{Thousand\ and\ One}$$

Example 2.137: Mod 9

Check the first few powers of ten $mod\ 9$

$$\underbrace{10 \equiv 1 (mod\ 9)}_{10=9+1}, \quad \underbrace{100 \equiv 1 (mod\ 9)}_{100=99+1=9\times 11+1}, \quad \underbrace{1000 \equiv 1 (mod\ 9)}_{1000=999+1=9\times 111+1}$$

This gives a pattern. All powers of ten are $1\ (mod\ 9)$. This can also be proved as below

$$10^n \underbrace{\equiv (10)^n \equiv 1^n}_{Substitute\ 10 \equiv 1 (mod\ 9)} \equiv 1 (mod\ 9)$$

Find $98765\ (mod\ 9)$

$$98765 = \underbrace{9 \times 10^4 + 8 \times 10^3 + 7 \times 10^2 + 6 \times 10^1 + 5}_{Write\ in\ expanded\ notation}$$

Since $10^n \equiv 1 (mod\ 9)$, we can make the substitution:

$$\equiv 9 \times \underbrace{10^4}_{\equiv 1} + 8 \times \underbrace{10^3}_{\equiv 1} + 7 \times \underbrace{10^2}_{\equiv 1} + 6 \times \underbrace{10^1}_{\equiv 1} + 5 \equiv 9 + 8 + 7 + 6 + 5 \equiv 35 \equiv 8 (mod\ 9)$$

Example 2.138

Check the first few even powers of ten $mod\ 99$

$$\underbrace{100 \equiv 1 (mod\ 99)}_{100=99+1}, \quad \underbrace{10{,}000 \equiv 1 (mod\ 99)}_{10{,}000=9{,}999+1=99\times 101+1}, \quad \underbrace{1{,}000{,}000 \equiv 1 (mod\ 99)}_{1{,}000{,}000=999{,}999+1=99\times 10101+1}$$

As with $mod\ 9$, this gives a pattern. All even powers of ten are $1\ (mod\ 99)$. Again, this can also be proved as below

$$10^{2n} \underbrace{\equiv (10^2)^n \equiv 1^n}_{Substitute\ 10^2 \equiv 100 \equiv 1 (mod\ 99)} \equiv 1 (mod\ 99)$$

Find $4718929\ (mod\ 99)$

Write 4718929 in expanded notation, two digits at a time, starting from the $\underbrace{rightmost\ digit}_{not\ leftmost}$:

$$4{,}718{,}929 = 4\,\underbrace{71}\,\underbrace{89}\,\underbrace{29} = 4\times10^6 + 71\times10^4 + 89\times10^2 + 29$$

Since $10^{2n} \equiv 1(mod\ 99)$, we can make the substitution:

$$\equiv 4\times\underbrace{10^6}_{\equiv 1} + 71\times\underbrace{10^4}_{\equiv 1} + 89\times\underbrace{10^2}_{\equiv 1} + 29 \equiv 4\times1 + 71\times1 + 89\times1 + 29 \equiv 4 + 71 + 89 + 29 \equiv 193 \equiv 94$$

If we had expanded starting from the leftmost digit, we would have got:

$$\underbrace{4{,}718{,}929 = \underbrace{47}\,\underbrace{18}\,\underbrace{92}\,9 = 47\times10^5 + 18\times10^3 + 92\times10^1 + 9}_{\textit{All odd powers. }\textbf{Problem}!!}$$

Example 2.139

Check the first few third powers of ten $mod\ 999$

$$\underbrace{1000 \equiv 1(mod\ 999)}_{1000=999+1},\qquad \underbrace{1{,}000{,}000 \equiv 1(mod\ 999)}_{1{,}000{,}000=999{,}999+1=999\times1001+1}$$

Again this gives a pattern and the pattern is proved below:

$$10^{3n} \underbrace{\equiv (10^3)^n \equiv 1^n}_{\textbf{Substitute } 10^3\equiv1000\equiv1(\textbf{mod } 999)} \equiv 1(mod\ 999)$$

Find $8{,}210{,}495{,}129\ (mod\ 999)$

Write 8,210,495,129 in expanded notation, three digits at a time, starting from the $\underbrace{rightmost\ digit}_{not\ leftmost}$:

$$8{,}210{,}495{,}129 = 8\,\underbrace{210}\,\underbrace{495}\,\underbrace{129} = 8\times10^9 + 210\times10^6 + 495\times10^3 + 129$$

Since $10^{3n} \equiv 1(mod\ 999)$, we can make the substitution:

$$\equiv 8\times\underbrace{10^9}_{\equiv 1} + 210\times\underbrace{10^6}_{\equiv 1} + 495\times\underbrace{10^3}_{\equiv 1} + 129 \equiv 8 + 210 + 495 + 129 \equiv 842(mod\ 999)$$

2.140: Numbers which are only 9's

Remainder on dividing $\boldsymbol{x}$ by a number which consists of $\boldsymbol{n}$ 9's, is given by the sum of digits of the number, $\boldsymbol{n}$ digits at a time, starting rightmost.

Example 2.141

$\because\ x = 1234567891$, find $\{x\ (mod\ 9), x\ (mod\ 99), x\ (mod\ 999)\}$

$$\underbrace{1234567891 \equiv 1+2+3+4+5+6+7+8+9+1 \equiv 45+1 \equiv 1(mod\ 9)}_{\textbf{Sum of Digits}}$$

$$\underbrace{1234567891 \equiv 12+34+56+78+91 \equiv 271 \equiv 73(mod\ 99)}_{\textbf{Sum of Digits,taken 2 at a time,starting rightmost}}$$

$$\underbrace{1234567891 \equiv 1+234+567+891 \equiv 1693 \equiv 694(mod\ 999)}_{\textbf{Sum of Digits,taken 3 at a time,starting rightmost}}$$

Example 2.142

Check the first few powers of ten $mod\ 11$

$$\underbrace{10^1 \equiv -1(mod\ 11)}_{10=11-1},\qquad \underbrace{10^2 \equiv 100 \equiv 1(mod\ 11)}_{100=99+1=9\times11+1},\qquad \underbrace{10^3 \equiv 1000 \equiv -1(mod\ 11)}_{1000=1001-1}$$

This gives a pattern. All odd powers of ten are $(-1)\ (mod\ 11)$. All even powers of ten are $1(mod\ 11)$. This can be proved as below:

$$10^n \underbrace{\equiv (10)^n \equiv (-1)^n}_{\textbf{Substitute } 10\equiv-1(\textbf{mod } 11)} \equiv \underbrace{\pm1(mod\ 11)}_{\substack{+1,\textit{if } n \textit{ is even}\\ -1,\textit{if } n \textit{ is odd}}}$$

$\because\ x = 1234567891$, find

$$\{x\ (mod\ 11), x\ (mod\ 101), x\ (mod\ 1001)\}$$

$$1234567891 \equiv -1 + \underbrace{2-3}_{=-1} + \underbrace{4-5}_{=-1} + \underbrace{6-7}_{=-1} + \underbrace{8-9}_{=-1} + 1 \equiv -4 \equiv 7(mod\ 11)$$

Example 2.143

$$10^{2n} \equiv (10^2)^n \equiv (-1)^n \equiv \underbrace{\pm 1(mod\ 101)}_{\substack{+1, even\ n \\ -1, odd\ n}}$$

$$1234567891(mod\ 101) \equiv 12 \times \underbrace{10^8}_{\equiv 1} + 34 \times \underbrace{10^6}_{\equiv -1} + 56 \times \underbrace{10^4}_{\equiv 1} + 78 \times \underbrace{10^2}_{\equiv -1} + 91 \times \underbrace{10^0}_{\equiv 1}$$
$$\equiv +12 - 34 + 56 - 78 + 91 \equiv 47(mod\ 101)$$

Shortcut: Sum of Digits, taken 2 at a time, alternating in sign, starting rightmost

Example 2.144

$$10^{3n} \equiv (10^3)^n \equiv (-1)^n \equiv \underbrace{\pm 1(mod\ 1001)}_{\substack{+1, even\ n \\ -1, odd\ n}}$$

$$1234567891(mod\ 1001) \equiv 1 \times \underbrace{10^9}_{\equiv -1} + 234 \times \underbrace{10^6}_{\equiv 1} + 567 \times \underbrace{10^3}_{\equiv -1} + 891 \times \underbrace{10^0}_{\equiv 1}$$
$$\equiv +1 - 234 + 56 - 567 + 891 \equiv 557(mod\ 1001)$$

Shortcut: Sum of Digits, taken 3 at a time, alternating in sign, starting rightmost

Example 2.145: Mod $\underbrace{100\ldots1}_{x\ 0's}$

$$10^{(x+1)n} \equiv (10^{x+1})^n \equiv (-1)^n \equiv \underbrace{\pm 1\left(mod\ \underbrace{100\ldots1}_{x\ 0's}\right)}_{\substack{+1, even\ n \\ -1, odd\ n}}$$

E. Divisibility Proofs

F. Divisibility in Number Bases

2.5 Division and Inverses

A. Congruence Cancellation and Division

We wish to solve

$$a \equiv b(mod\ x)$$

If a and b have a common factor, our calculations will be simpler if divide by the common factor. However, we have to be careful. When dividing, we need to divide:

- not just the LHS and RHS
- but also the number x with respect to which we are calculating the mod.

$$10a \equiv 10b(mod\ 10c) \Leftrightarrow\ 10c \mid [10b - 10a] \Leftrightarrow c \mid [b - ax] \Leftrightarrow b \equiv a(mod\ c).$$

Example 2.146

$$2x \equiv 0\ (mod\ 20)$$

Convert to algebra. If a number is 0 $(mod\ 20)$, then it is an integral multiple of 20:

$$2x = 20k, \qquad k \in \mathbb{Z}$$

This is now an equation in Algebra, and not a congruence in mod arithmetic. Division is valid. Divide by 2 both sides:

$$x = 10k, \qquad k \in \mathbb{Z}$$

Convert back to mod arithmetic. Note that the division divided our mod by 2:

$$x \equiv 0(mod\ 10)$$

And convert back into mod 20:

$$x \in \{0,10\}\ (mod\ 20)$$

Example 2.147

$$2x \equiv 4\ (mod\ 20)$$

Convert to algebra. If a number is 0 $(mod\ 20)$, then it is an integral multiple of 20:

$$2x = 4 + 20k, \qquad k \in \mathbb{Z}$$
$$x = 2 + 10k, \qquad k \in \mathbb{Z}$$

Convert back to mod arithmetic:

$$x \equiv 2(mod\ 10)$$

And convert back into mod 20:

$$x \in \{2,12\}(mod\ 20)$$

Example 2.148

$$4x \equiv 2\ (mod\ 6)$$

Convert into the language of algebra:

$$4x = 2 + 6k, \qquad k \in \mathbb{Z}$$

Divide by 2:

$$2x = 1 + 3k, \qquad k \in \mathbb{Z}$$
$$2x \equiv 1(mod\ 3)$$
$$2 \cdot 2x \equiv 1 \cdot 2(mod\ 3)$$
$$x \equiv 2\ (mod\ 3)$$
$$x \in \{2,5\}\ (mod\ 6)$$

Shortcut:

$$4x \equiv 2\ (mod\ 6)$$
$$\frac{4x}{2} \equiv \frac{2}{2}\left(mod \frac{6}{\gcd(2,6)}\right)$$
$$2x \equiv 1\ \left(mod \frac{6}{2}\right)$$

$$2x \equiv 1\ (mod\ 3)$$

Example 2.149

Solve: $54x \equiv 27(mod\ 7)$

Divide both sides by 27. Remember to divide the 7 by gcd(7,27)

$$\frac{54x}{27} \equiv \frac{27}{27}\left(mod\ \frac{7}{\gcd(7,27)}\right) \Rightarrow 2x \equiv 1\left(mod\ \frac{7}{1}\right) \Rightarrow 2x \equiv 1(mod\ 7) \Rightarrow x \equiv 4(mod\ 7) \Rightarrow\ x \in \{-3,4,11,18, \dots\}$$

But have we found all values that will satisfy the congruence in the range:

$$1 \leq x < mod\ 7$$

2.150: Finding all solutions of a congruence

If

- $\gcd(a,b,c) = 1$, there will be only one solution x of $a \equiv b(mod\ c)$ in the range $1 \leq x < c$
- $\gcd(a,b,c) > 1$, then there will be multiple solutions.

Example 2.151

Solve for all positive values of x less than 10 that satisfy $6x \equiv 8(mod\ 10)$.

Brute Force Solution

x	$6x$	$6x(mod\ 10)$
1	6	6
2	12	2
3	18	8
4	24	4
5	30	0
6	36	6
7	42	2
8	48	8
9	54	4

There are two values of x that satisfy that the congruence, and which also lie in the range $1 \leq x < 10$.
This creates a problem since we do not want to try all values. The next method shows how to avoid this situation.

Division Based Solution

$$HCF(6,8,10) = 2 > 1$$

To not miss out on solutions, first reduce the congruence, by dividing both sides of the congruence by 2 and dividing 10 by $\gcd(2,10) = 2$:

$$\frac{6x}{2} \equiv \frac{8}{2}\left(mod\ \frac{10}{\gcd(2,10)}\right) \Rightarrow 3x \equiv 4(mod\ 5) \Rightarrow x \equiv 3(mod\ 5)$$

The solution above can be converted in terms of $mod\ 10$. We find that there are two values $mod\ 10$ that satisfy the congruence.

$$\underbrace{x \equiv 3(mod\ 10), x \equiv 8(mod\ 10)}_{Answer}$$

We got the same answer as using the table, but we did more systematically.

Example 2.152

Solve for all values of x: $4x \equiv 4\ (mod\ 12)$. State your answer as a congruence in the smallest possible mod, and also in terms of $mod\ 12$

Divide both sides by 4, and divide 12 by $\gcd(4,12) = 4$

$$\frac{4x}{4} \equiv \frac{4}{4}\left(mod \frac{12}{\gcd(4,12)}\right) \Rightarrow x \equiv 1(mod\ 3) \Rightarrow x \in \{\dots, -2,1,4,7,10 \dots .\}$$

While there is only one congruence class $mod\ 3$ which satisfies the congruence, there are four congruence classes $mod\ 12$, which satisfy the congruence.

$$x \equiv \{1,4,7,10\}(mod\ 12) \Rightarrow x \in \{\dots, -2,1,4,7,10 \dots .\}$$

Example 2.153: mod 11

Solve $-901x + 781 \equiv 234\ (mod\ 11)$

Since the test of divisibility by 11 is complicated to apply, collect like terms (variables on the RHS, and numbers on the LHS).

$$\underbrace{547}_{=781-234} \equiv 901x$$

Apply the test of divisibility of 11, remembering to start with the rightmost digit:

$$\underbrace{8}_{\substack{547(mod\ 11)\\ =5+7-4=8}} \equiv \underbrace{10x}_{\substack{901x(mod\ 11)\\ =1+9-0=10x}} \Rightarrow \underbrace{4 \equiv 5x}_{\text{Divide by 2 both sides}} \Rightarrow x = 3(mod\ 11)$$

Example 2.154

The manager of an agricultural trading firm tells the owner that he bought crates of mangoes, each with twelve mangoes. Six mangoes were spoilt, and thrown away. Then the mangoes were repacked in boxes of eight, and four mangoes are left over. The owner says there is a problem. Why?

$$Total\ Mangoes = \underbrace{12}_{\substack{Mangoes\\ per\ crate}} \times \underbrace{c}_{No.of\ Crates} = 12c \Rightarrow Unspoilt\ Mangoes = \underbrace{12c}_{\substack{Total\\ Mangoes}} - \underbrace{6}_{\substack{Mangoes\\ Spoilt}}$$

Now the mangoes were repacked in boxes of eight, and four mangoes were left over.

$$\therefore 12c - 6 \equiv 4\left(\underbrace{mod\ 8}_{\substack{\text{Packed in boxes}\\ \text{of eight}}}\right) \Rightarrow \underbrace{12c \equiv 2(mod\ 8)}_{\text{Subtract 2 from both sides}}$$

Divide the congruence by 2:

$$\frac{12c}{2} \equiv \frac{2}{2}\left(mod \frac{8}{\gcd(2,8)}\right) \Rightarrow \underbrace{6c}_{\text{LHS is even}} \equiv \underbrace{1}_{\text{RHS is odd}} (mod\ 4) \Rightarrow \textbf{\textit{No Solutions}}$$

Since no values of c satisfy the congruence, it is not possible to have a number of crates ordered which would meet the conditions given in the report.

Example 2.155

Solve $3x \equiv 2(mod\ 7)$

We want to divide both sides by 3. We cannot divide 2 by 3, so we add multiples of 7 to the right-hand side, till we get a number that is divisible by 3.

$$\underbrace{3x \equiv 9(mod\ 7)}_{\text{Add 7 to both sides}} \Rightarrow \underbrace{x \equiv 3\ (mod\ 7)}_{\substack{\text{Divide by 3 both sides}\\ \gcd(3,7)=1}}$$

B. Multiplicative Inverses

Definition: $xn = 1(mod\ m) \Rightarrow x, n$ are inverses of each other (mod m)

Notation: The modular inverse of x is written as x^{-1}

Application: $ax \equiv b(mod\ m) \Leftrightarrow x \equiv ba^{-1}(mod\ m)$

Existence of Modular Inverse

$$\boldsymbol{x^{-1}(\mathbf{mod}\ m)\ \text{exists}\ if\ and\ only\ if\ \text{HCF}(x,m)=1}$$

Existence of Modular Inverse for mod p (where p is prime)

Therefore, modular inverses exists for all numbers

$$x, \qquad 0 < x < p(mod\ p)$$

Guaranteed Modular Inverses

$$\underbrace{(m-1)^2 \equiv m^2 - 2m + 1 \equiv 1(\text{mod}\ m)}_{m-1 \text{ is its own inverse mod } m}$$

$$\underbrace{1 \times 1 \equiv 1(\text{mod}\ m)}_{1 \text{ is its own inverse mod } m}$$

$$\underbrace{m \equiv 0(\text{mod}\ m)}_{\text{Zero does not have a modular inverse for any mod}} \quad \Rightarrow x = \underbrace{\{\phi\}}_{\text{Null Set}}$$

Uniqueness of modular inverse

$$\because \boldsymbol{a^{-1}(mod\ m) = x}$$

The set of all modular inverses a($\boldsymbol{mod\ m}$) can be written as

$$\ldots \equiv x - 2m \equiv x - m \equiv a^{-1}(mod\ m) \equiv x \equiv x + m \equiv x + 2m \equiv \cdots$$

C. Multiplicative Inverses: Rational Numbers

This section is on rational numbers, not mod arithmetic. We will introduce the concept of multiplicative inverse in rational numbers, and then use the same concept in mod arithmetic in the next section.

Division is more difficult in modular arithmetic as compared to real numbers. There are a few issues:

- **Problem I:** Fractions and Decimals are not a part of modular arithmetic systems. This means that we cannot always divide one number by another - the way we do with rational numbers.
- **Problem II:** Even if a number is divisible, we must be careful, due to the property of linear congruences.

D. Multiplicative Inverses

Solving Problem I

To get around problem I, we introduce the concept of inverses. Inverses play the same role in rational numbers that division does. But since modular arithmetic does not always have division, they help us get division done in modular arithmetic.

However, we will also learn that division is not always possible in modular arithmetic.

We first introduce multiplicative inverses in the familiar context of rational numbers. Then, we show they can be used in modular arithmetic.

E. Multiplicative Inverses – Rational Numbers

Background

$$2x = 1 \Rightarrow x = \frac{\mathbf{1}}{\mathbf{2}} \Rightarrow \frac{1}{2} \text{ is the multiplicative inverse of } 2$$

$$\frac{3}{4}x = 1 \Rightarrow x = \frac{\mathbf{4}}{\mathbf{3}} \Rightarrow \frac{4}{3} \text{ is the multiplicate inverse of} \frac{3}{4}$$

In each case, multiplying the number by x results in getting 1.

Definition

For a number x, the number n is a multiplicative inverse if

$$\underbrace{xn = 1 \Rightarrow x = \frac{1}{n} \Rightarrow n = \frac{1}{x}}_{\text{Multiplicative Inverses are reciprocals of each other}}$$

Existence of Multiplicative Inverse

$$0x = 1 \Rightarrow x = \underbrace{\{\phi\}}_{\text{Null Set}} \Rightarrow \underbrace{\text{No Solutions}}_{\text{Multiplicative Inverse of Zero does not exist}}$$

Invertibility

If a number has a multiplicative inverse, it is said to be invertible. Not all numbers are invertible, as seen in the property below.

Example 2.156

What is the multiplicative inverse of the following (in regular arithmetic, not mod arithmetic)? Show that a number multiplied by its multiplicative inverse is one for all of the below numbers.

$$\left\{5, 7, \frac{1}{3}, \frac{3}{5}\right\}$$

To find the multiplicative inverse, we just take the reciprocal

$$\left\{\frac{1}{5}, \frac{1}{7}, 3, \frac{5}{3}\right\}$$

$$\left\{5 \times \frac{1}{5} = 1, 7 \times \frac{1}{7} = \frac{1,1}{3} \times 3 = 1, \frac{3}{5} \times \frac{5}{3} = 1\right\}$$

F. Multiplicative Inverses: Modular Arithmetic

Background

The concept of inverses can be extended to modular arithmetic, though it does not work in the same way. Finding the inverse is not as simple as finding the reciprocal.

Definition

$$xn = 1(mod\ m) \Rightarrow x, n \text{ are inverses of each other (mod } m)$$

$$Example: \underbrace{7x}_{x=7} \equiv 49 \equiv 1(\text{mod } 8) \Rightarrow 7\ is\ its\ own\ multiplicative\ inverse\ (mod\ 8)$$

Notation

The modular inverse of x is written as x^{-1}

$$\therefore x \cdot x^{-1} = 1$$

We do not write the modular inverse as $\frac{1}{x}$, because $\frac{1}{x}$ does not have meaning in modular arithmetic.

We will call the *multiplicative inverse in modular arithmetic* as the modular inverse.

Example 2.157: Set of Modular Inverses

We can find a complete set of modular inverses for a number. This will also illustrate the concept of modular inverses.

Find modular inverses of all numbers *mod* 7.

Method I

$$1x \equiv 1(mod\ 7) \Rightarrow x = 1 + \underbrace{7y}_{y \in Z}$$

We won't write this everytime

The next one let us find two modular inverses in one go. We find the inverse of 2, and in the process find the inverse of 4:

$$\underbrace{2x \equiv 1}_{x \neq \frac{1}{2}} \quad (mod\ 7) \Rightarrow Try\ x = \{1,2,3 \dots\} \Rightarrow 2x = \{2,4,6,8\} \Rightarrow 8 \equiv 1(mod\ 7) \Rightarrow x = 4$$

Fractions not allowed

Now that we found one value of x, we can find more values of x that belong to the same congruence class:

$$x = \{\dots -10, -3, 4, 11, 18 \dots\} = 4 + \underbrace{7y}_{y \in Z} \Rightarrow \underbrace{(4,2) \text{ are mod inverses } mod\ 7}_{\text{No need to find 4 separately}}$$

Same for this one. We get:

$$3x \equiv 1(mod\ 7) \Rightarrow x = 5 \Rightarrow (3,5) \text{ are mod inverses } mod\ 7$$

6 is its own inverse mod 7. This is a property, as we will see next:

$$6x \equiv 1(mod\ 7) \Rightarrow x = 6 \Rightarrow 6\ is\ its\ own\ inverse\ mod\ 7$$

Method II

Tabulate values of products $mod\ 7$						
	1	2	3	4	5	6
1	**1**	2	3	4	5	6
2	2	4	6	**1**	3	5
3	3	6	2	5	**1**	4
4	4	**1**	5	2	6	3
5	5	3	**1**	6	4	2
6	6	5	4	3	5	**1**

Answer

$$\underbrace{1^{-1} = 1, \quad 2^{-1} = 4, \quad 3^{-1} = 5, \quad 4^{-1} = 2, \quad 5^{-1} = 3, \quad 6^{-1} = 6}_{mod\ 7}$$

Properties:

- Every column (and every row) in the table has exactly one mod inverse.
  - ✓ This is true in general. All values $x^{-1}(mod\ y)$ belong to the same congruence class.
- The mod inverses of 1 to 6 are also 1 to 6, in a different order.
  - ✓ This property holds not just for $mod\ 7$, but for all primes).

G. Finding Modular Inverses: Trial and Error

We used the trial and error method to find modular inverses so far. This will work for small/easy numbers. Below are some examples of using the trial and error method.

Example 2.158: Modular Inverses Basics

Find the modular inverses of $\{3\ (mod\ 4), 13(mod\ 17), 1\ (mod\ 17)\}$

$3 \times 3 \equiv 9 \equiv 1\ (mod\ 4) \Rightarrow \underbrace{3^{-1} = 3\ (mod\ 4)}_{Remember: 3^{-1}\ is\ modular\ inverse\ of\ 3}$

$13 \times 4 \equiv 52 \equiv 1(mod\ 17) \Rightarrow 13^{-1} = 4(mod\ 17)$

$1 \times 1 \equiv 1\ (mod\ 17) \Rightarrow 1^{-1} = 1(mod\ 17)$

H. Finding Modular Inverses: Using the Decimal System

You can use tricks related to the decimal system to find modular inverses.

$$10 \equiv 1(mod\ 9), 100 \equiv 1(mod\ 9), 10^n \equiv (10)^n \equiv 1^n \equiv 1(mod\ 9)$$

So, if we are able to create a power of ten, it will be useful in calculating modular inverses.
Powers of ten can only be created for numbers which have only 2 and 5 in their prime factorization.

Example 2.159: Modular Inverses: Using or creating a nine

Evaluate:

A. $5^{-1}\ (mod\ 9)$
B. $4^{-1}\ (mod\ 13)$

Nine in the last digit (get a zero):
The last digit of the mod that we want is 9. Hence, a zero in the last digit of the number is congruent to one:

$$5 \times 2 \equiv 10 \equiv 1(\ mod\ 9) \Rightarrow 5^{-1} = 2(mod\ 9)$$

Creating a nine in the last digit:
We don't have a nine in the last digit, but we can get a nine in the last digit by multiplying 13 by three. Also, we can get zero in the last digit by multiplying by 10:

$$4 \times 10 \equiv 40 \equiv 1(\ mod\ 13) \Rightarrow 4^{-1} = 10(mod\ 13)$$

Example 2.160: Modular Inverses: Factors of 10^n

Find the modular inverses of:

A. $8\ mod\ 999$
B. $1250\ mod\ 9999$

Using Factors of 10^n
$999 + 1 = 1{,}000$, and $8 \times 125 = 1{,}000$:

$$8 \times 125 \equiv 1{,}000 \equiv 1(\ mod\ 999) \Rightarrow 8^{-1} = 125(mod\ 999)$$

$9999 + 1 = 10{,}000$, and $8 \times 125 = 1{,}000$:

$$1250 \times 8 \equiv 10{,}000 \equiv 1(\ mod\ 9999) \Rightarrow 1250^{-1} = 8(mod\ 999)$$

I. Existence of Modular Inverses

It is not necessary that modular inverses always exist, as the next example shows.

Example 2.161: Checking for existence of Modular Inverses

Do the following modular inverses exist?

A. $6\ mod\ 8$
B. $5\ mod\ 11$
C. $3\ mod\ 9$

(Only check $1 \leq x < m$, where m is the mod being taken. Why?)

We find $-1(mod\ 11)$, and use the fact that $(-1)^2 = 1$ to find the modular inverse:

$$5 \times 2 \equiv 10 \equiv -1(mod\ 11) \Rightarrow 10 \times 10 \equiv 5 \times 20 \equiv 1\ (mod\ 11)\ \Rightarrow 5^{-1} \equiv 20 \equiv 9\ (mod\ 11)$$

The other two modular inverses do not exist, as can be confirmed by checking all values from 1 to 7 (for mod 8), and 1 to 8 (for mod 9).

J. Guaranteed Modular Inverses

Certain properties of modular inverses help to speed up calculations. You might have observed some of these properties in the example above. We now formalise them:

$$\underbrace{(m-1)^2 \equiv m^2 - 2m + 1 \equiv 1(\text{mod}\ m)}_{\textbf{m−1 is its own inverse mod } m}$$

$$\underbrace{1 \times 1 \equiv 1(\text{mod}\ m)}_{\textbf{1 is its own inverse mod } m}$$

$$\underbrace{m \equiv 0(\text{mod}\ m)}_{\textbf{Zero does not have a modular inverse for any mod}} \quad \Rightarrow x = \underbrace{\{\phi\}}_{\textbf{Null Set}}$$

Example 2.162

Find the following modular inverses using the properties (if they exist):

A. $5(mod\ 6)$

B. $1(mod\ 72)$
C. $36(mod\ 37)$
D. $46(mod\ 23)$

$$5^{-1} \equiv 5(mod\ 6)$$
$$1^{-1} \equiv 1(mod\ 72)$$
$$36^{-1} \equiv 36(mod\ 37)$$
$$\underbrace{46 \equiv 0(mod\ 23)}_{\textbf{No Modular Inverse}}$$

Challenge 2.163

Let $A = \sum_{x=1}^{10}[x^{-1}(mod\ (x+1))], B = \sum_{x=1}^{20} 1^{-1}(mod\ (x+2))$

Write the above as a series.

$$A = 1^{-1}(mod\ 2) + 2^{-1}(mod\ 3) + \cdots + 10^{-1}(mod\ 11)$$

$$B = 1^{-1}(mod\ 3) + 1^{-1}(mod\ 4) + \cdots + 1^{-1}(mod\ 22)$$

Example 2.164

Evaluate the value of AB, using A and B from the previous question.

$$A = 1^{-1}(mod\ 2) + 2^{-1}(mod\ 3) + \cdots + 10^{-1}(mod\ 11) = \underbrace{1 + 2 + \cdots + 10}_{\textbf{(m−1) is its own inverse mod m}} = 55$$

$$B = 1^{-1}(mod\ 3) + 1^{-1}(mod\ 4) + \cdots + 1^{-1}(mod\ 22) = \underbrace{1 + 1 + \cdots + 1}_{\textbf{1 is its own inverse mod m}} = 20$$

$$AB = 55 \times 20 = 1100$$

K. Application: Solving Linear Congruences

Modular Inverses are useful in solving linear congruences because they play the role of division. Finding modular inverses is both an art and a science, and it requires familiarity with numbers.

$$ax \equiv b(mod\ m) \Leftrightarrow x \equiv ba^{-1}(mod\ m)$$

Example 2.165: Modular Inverses to solve linear congruences

Solve the linear congruence below using modular inverses:

$$7x \equiv 3\ (mod\ 5)$$

Solving

Simplify the left-hand side of the congruence by re-writing $7x$ as $2x$. We can do this since $5x \equiv 0\ (mod\ 5)$

$$\underbrace{2x \equiv 3\ (mod\ 5)}_{\textbf{5x≡0 (mod 5)}}$$

Since we cannot divide by 2, we multiply by $2^{-1}\ (mod\ 5) = 3$

$$2x \equiv 3\ (mod\ 5) \Rightarrow 2^{-1}2x \equiv 3 \times 2^{-1}\ (mod\ 5) \Rightarrow \underbrace{3 \times 2x \equiv 3 \times 3\ (mod\ 5)}_{\textbf{∵2^{-1}≡3 (mod 5)}} \Rightarrow 6x \equiv 9\ (mod\ 5) \Rightarrow x \equiv 4\ (mod\ 5)$$

Checking the Answer

Substitute in the original congruence:

$$7x \equiv 3\ (mod\ 5) \Rightarrow 7 \times 4 \equiv 3\ (mod\ 5) \Rightarrow 28 \equiv 3\ (mod\ 5) \Rightarrow \mathbf{3 \equiv 3\ (mod\ 5)}$$

We can also check only the left-hand side of the congruence

$$LHS \equiv 7x \equiv 7 \times 4 \equiv 28 \equiv 3 \equiv RHS(mod\ 5) \Rightarrow \textbf{Verified}$$

L. Existence of Inverse

Introduction

We did a few examples where we found the modular inverse (and some where it did not exist).

Let's look at one more example where there is no modular inverse:

$$\underbrace{2x \equiv 1 (\text{mod } 4)}_{\gcd(2,4)=2} \Rightarrow \underbrace{2 \cdot 1 \equiv 2, \quad 2 \cdot 2 \equiv 0, \quad 2 \cdot 3 \equiv 2}_{mod\ 4} \Rightarrow x = \underbrace{\{\phi\}}_{Null\ Set}$$

We could exhaust the values of x easily since m had a small value. But this may not always be the case. Let's look at the general conditions for the existence of a modular inverse.

2.166: Existence of Modular Inverse

$$\boldsymbol{x^{-1} (\text{mod } m) \text{ exists } if \text{ and only } if \text{ HCF}(x, m) = 1}$$

2.167: Existence of Modular Inverse for mod p (where p is prime)

$0 \equiv p$ does not have a modular inverse $mod\ p$. The numbers left to check are the numbers between 0 and p:

$$0 < x < p$$

But, all numbers between 0 and p are co-prime to p.
Therefore, all modular inverse exists for all numbers

$$x, \quad 0 < x < p (mod\ p)$$

Example 2.168: Checking for existence of Inverse

If a number is not prime, we cannot confirm, without examination whether a number has a modular inverse. But, for all numbers, we will still be able to find the modular inverse of 1 and $1 - p$.

$$1 \times 1 \equiv 1 \bmod x \Rightarrow 1^{-1} = 1 \bmod x \Rightarrow 1^{-1} \bmod x \text{ always exists}$$
$$HCF(x - 1, x) = 1 \Rightarrow (x - 1) \bmod x \text{ always exists}$$

Example 2.169: Checking for existence of Inverse

Check whether the inverses in the following set exist? $\{5^{-1} (\text{mod } 7), 2^{-1} (\text{ mod } 8), 4^{-1} (\text{mod } 9)\}$

$$\underbrace{5^{-1} \bmod 7\ exists}_{\because \gcd(5,7)=1}, \underbrace{2^{-1} \bmod 8\ does\ not\ exist}_{\because \gcd(2,8)=2}, \underbrace{4^{-1} \bmod 9\ exists}_{\because \gcd(4,9)=1}$$

In 4^{-1} (mod 9), neither 4 nor 9 are prime, but the numbers are co-prime and hence the modular inverse exists.

Example 2.170: Finding the set of numbers for modular inverse exists

For which natural numbers x less than 8 does there exist x^{-1} mod 8?
We check $HCF(x, 8)$ for numbers in the set {1,2,3,4,5,6,7}:

$$\left\{\underbrace{1}_{1}, \underbrace{2}_{2}, \underbrace{3}_{1}, \underbrace{4}_{4}, \underbrace{5}_{1}, \underbrace{6}_{2}, \underbrace{7}_{1}\right\} \Rightarrow x^{-1} \bmod 8 \text{ exists for } \{1,3,5,7\}$$

Example 2.171: Finding the number of modular inverses

For how many natural numbers x less than 36 does there exist x^{-1} mod 36?

$$x = \{1,2,3, \dots, 35\}$$

Method I: Enumeration

$$36 = 2^2 \times 3^2 \Rightarrow HCF(x, 36) = 1 \Leftrightarrow x \text{ does not have 2 or 3 as a prime factor}$$
$$x = \{1,5,7,11,13,17,19,23,25,29,31,35\} \Rightarrow 12\ Numbers$$

Method II:

$$36 = 2^2 \times 3^2$$

We want numbers which are co-prime to 36.
∴ We want numbers which do not have 2, or 3 as factors.
Use complementary counting:

- Count numbers which have 2 or 3 as a factor
- Subtract the count from the numbers less than 36:

Let:
A be the set of multiples of 2, which are ≤ 36
B be the set of multiples of 3, which are ≤ 36
$A \cap B$ is the set of multiples of 6, which are ≤ 36

$$(A \cup B) = n(A) + n(B) - n(A \cap B)$$

$$Numbers\ with\ Factor\ of\ 2\ or\ 3: \underbrace{18}_{Multiples\ of\ 2} + \underbrace{12}_{Multiples\ of\ 3} - \underbrace{6}_{Multiples\ of\ 6} = 24$$

$$Numbers\ Co-prime\ to\ \{2,3\} = 36 - 24 = 12$$

2.172: Uniqueness of modular inverse

$$\because \boldsymbol{a^{-1}(mod\ m) = x}$$

The set of all modular inverses a$(\boldsymbol{mod\ m})$ can be written as

$$\ldots \equiv \boldsymbol{x - 2m \equiv x - m \equiv a^{-1}(mod\ m) \equiv x \equiv x + m \equiv x + 2m \equiv \cdots}$$

$$3^{-1}(mod\ 5) = 2$$

From the above, we can see that 2 is a modular inverse of $3(mod\ 5)$. Is this the only number that is a modular inverse? No, as we see from the table below.

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$x(mod\ 5)$	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
$3x$	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45
$3x(mod\ 5)$	3	1	4	2	0	3	1	4	2	0	3	1	4	2	0

The numbers

$$\{2, 7, 12\}$$

Are the modular inverses of $3(mod\ 5)$. Each of these numbers is itself

$$2(mod\ 5)$$

This is not a coincidence. Once we have found a modular inverse, all modular inverses belong to the same congruence class

$$\ldots \equiv -8 \equiv -3 \equiv\ 3^{-1}(mod\ 5) \equiv 2 \equiv 7 \equiv 12 \equiv \cdots$$

2.173: Complete set of congruence classes for primes

If a number p is prime, then

- all numbers $1 \leq x < p$ will have modular inverses

These modular inverses will belong to unique congruence classes.
Therefore, the modular inverses of all the congruence classes must the same congruence classes rearranged:

$$\{1^{-1}, 2^{-1}, 3^{-1}, \ldots (1-p)^{-1}\}(mod\ p) = \{1,2,3, \ldots, 1-p\}(mod\ p)$$

M. Back-Calculations

Given $x^{-1}(mod\ m) = y$, where we know the value of x and y, we can be concerned with finding:

- the number of values of m

- the set of values of m
- a specific value of m that meets certain conditions

Example 2.174: Find the set of values of m

7 is its own inverse mod m. Find the possible value(s) of m.

$$7^{-1}(mod\ m) = 7 \Rightarrow \underbrace{49}_{=7\times7} \equiv 1(mod\ m) \Rightarrow \underbrace{48 \equiv 0(mod\ m)}_{Subtract\ 1\ from\ both\ sides} \Rightarrow m = \{2,3,4,6,8,12,16,24,24,48\}$$

Example 2.175 : Find set of values while meeting conditions

The inverse of 5 $(mod\ m)$ is 3. 5 and 3 represent distinct congruence classes $(mod\ m)$. Find the sum of the possible values of m.

S1: $5^{-1}(mod\ m) = 3 \Rightarrow \underbrace{15}_{=5\times3} \equiv 1(mod\ m) \Rightarrow \underbrace{14 \equiv 0(mod\ m)}_{Subtract\ 1\ from\ both\ sides}$

$\therefore$ 14 must be a multiple of $m \Rightarrow 14 = xm \Rightarrow \underbrace{m = \{2,7,14\} \Rightarrow 7 + 14 = 21}_{5\equiv3\equiv1(mod\ 2)\Rightarrow Same\ congruence\ class\ \therefore(mod\ 2)\ is\ not\ valid}$

Example 2.176

25 is its own inverse mod m, but 5 is not its own inverse mod m. Find the value(s) of m.

$$25^{-1}(mod\ m) = 25 \Rightarrow \underbrace{625}_{=25\times25} \equiv 1(mod\ m) \Rightarrow 624 \equiv 0(mod\ m) \Rightarrow m \mid 624$$

$$5^{-1}(mod\ m) \neq 5 \Rightarrow \underbrace{25}_{=5\times5} \not\equiv 1(mod\ m) \Rightarrow 24 \not\equiv 0(mod\ m) \Rightarrow m \nmid 24$$

$$624 = 24 \times \underbrace{26}_{2\times13} \Rightarrow m = \{24\times2, 24\times13, 24\times26\} = \{48,312,624\}$$

N. Distributive Property over Multiplication

We can distribute modular inverses over multiplication. That is:

$$(xy)^{-1} = x^{-1}y^{-1}$$

We can illustrate this with:

$$6^{-1} \equiv 2^{-1} \times 3^{-1} \equiv 4 \times 5 \equiv 4 \times (-2) \equiv -8 \equiv -1 \equiv 6(mod\ 7)$$

$$3^{-1} + 5^{-1} \equiv \frac{1}{3} + \frac{1}{5} \equiv \frac{8}{15} \equiv \frac{1}{1} \equiv 1(mod\ 7)$$

$$3a \equiv 1(mod\ 7), 5a \equiv 1(mod\ 7) \Rightarrow 15a \equiv$$

O. Recovering Real Number Properties

We cannot divide in mod arithmetic. However, certain properties that we are used to can be *recovered* in mod arithmetic. We look at some of these properties.

P. Inverse of a sum of inverses

Q. Telescoping Series

177 Examples