Sections 4.1   Number Theory

Comp 232
Instructor: Robert Mearns

What is Number Theory ?

1. Number theory is the part of mathematics devoted to the study of the integers and their properties.
2. Key ideas in number theory include divisibility, modular arithmetic, prime integers, greatest common divisors and least common multiples.
3. Representations of integers, including binary and hexadecimal representations, are part of number theory. This will be used to represent different number types in computer memory
4. We will look at several computer applications of Number Theory.

Section 4.1

Divisibility
Modular Arithmetic

Section 4.2

Computer representation of Integers

Section 4.3

Prime numbers
Greatest Common Divisors

1. Terms and Definitions

Term	Definition	Example
Divisor Dividend Quotient Remainder	Division Algorithm d is the divisor | a is the dividend | q is the quotient | r is the remainder Iff $\forall a,d\ \exists q,r,\ a,d,q,r \in \mathbf{Z},\ d > 0,\ 0 \leq r < d$, a/d = q + remainder r Note: Remainder r is Positive or 0 and less than d Notation: q = a div d r = a mod d	$\frac{11}{4}$ = 2 + remainder 3 Hence: 4 is the divisor 11 is the dividend 2 is the quotient 3 is the remainder
Divides Factor Multiple	d divides a | d is a factor of a | a is a multiple of d Iff $\forall a,d\ \exists q,\ a,d,q \in \mathbf{Z},\ d \overset{>}{\neq} 0$, a/d = q or a =dq Note: Remainder r is 0 Notation: d|a is read as "d divides a" d|a means a/b	Ex 1 $\frac{12}{4} = 3$ or $12 = 4 \times 3$ Hence: 4 divides 12: 4|12 4 is a factor of 12 12 is a multiple of a Ex 2 $\frac{11}{4}$ = 2 + remainder 3 4 11 because the remainder $\neq$ 0

Terms and Definitions (continued)

Term	**Definition**	**Example**
Congruent Modulo	a is congruent to r , modulo m Iff $\forall$a,r,m, a,r $\in$ **Z,** m $\in$ $\mathbf{Z}^+$, m | (a-r) Notation: a ≡ r mod m is read as "a is congruent to r modulo m" Note: a≡r mod m → m | (a-r) → a-r = mq, q∈Z → a = mq + r → Congruence value r (where r>0) is the remainder where a is divided by m Hence: r = a mod m	Examples: m | (a-b) ⟶ a ≡ b mod m 3 | (3-0) ⟶ 3 ≡ 0 mod 3 3 | (4-1) ⟶ 4 ≡ 1 mod 3 3 | (5-2) ⟶ 5 ≡ 2 mod 3 3 | (6-0) ⟶ 6 ≡ 0 mod 3 Note that the congruence values b are really the remainders when divide the given numbers a by 3: $\frac{5}{3}$ = 1 + remainder 2 Hence 5 ≡ 2 mod 3

Ex 1: Does 7 divide 833 ? $\frac{833}{7}$ = 119 + remainder 0. Hence 7 divides 811

Write:

7 | 833 = 7 | (833-0)

833 ≡ 0 mod 7 or 0 = 833 mod 7 because 0 is the remainder when 833 is divided by 7

Ex 2: Does $7 \mid 377$? (Use the calculator to get) $\frac{377}{7} = 53.\underline{857142}\,\underline{857142}\ldots\ldots.$

- Decimal part = 0.85… is not the remainder but $0.85\ldots \rightarrow \text{remainder} \neq 0$
- Remainder $\neq 0 \rightarrow 7$ 377
- How do we calculate remainder: $377 - (53 \times 7) = 377\text{-}371 = 6$, hence remainder = 6
- Write: $377/7 = 53 + \text{remainder } 6$ OR $377 \equiv 6 \bmod 7$ OR $6 = 377 \bmod 7$

Ex 3: $50 \equiv ?\ \bmod 6$

Step1 $\frac{50}{6} = 8.33..$

Step 2 $50 - 6 \times 8 = 2 \rightarrow \text{rem} = 2 \rightarrow 50 \equiv 2 \bmod 6$ OR $2 = 50 \bmod 6$

Ex 4: $492 \equiv ?\ \bmod 15$

Step1 $\frac{492}{15} = 32.8$

Step 2 $492 - 15 \times 32 = 12 \rightarrow \text{rem} = 12 \rightarrow 492 \equiv 12 \bmod 15$ OR $12 = 492 \bmod 15$

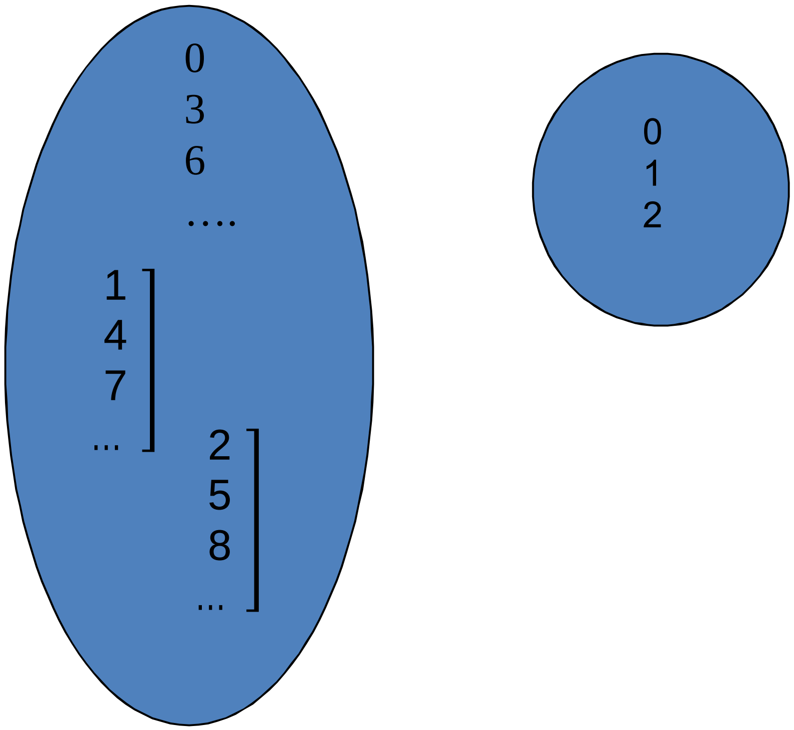
Ex 5: $492 \equiv ?\ \bmod 6$

Step1 $\frac{492}{6} = 82$

Step 2 The rem $= 0 \rightarrow 492 \equiv 0 \bmod 6$ OR $0 = 492 \bmod 6$

2. The Mod m Relation is a Function

Ex 1: Consider mod 3 Relation with Domain as $\mathbf{Z}^+$



$\frac{0}{3} \to \text{Rem} = 0 \to 0 = 0 \bmod 3$

$\frac{3}{3} \to \text{Rem} = 0 \to 0 = 3 \bmod 3$

$\frac{6}{3} \to \text{Rem} = 0 \to 0 = 6 \bmod 3$

………..

$\frac{1}{3} \to \text{Rem} = 1$

$\frac{4}{3} \to \text{Rem} = 1$

$\frac{7}{3} \to \text{Rem} = 1$

………… Hence: 1,4,7,... all map to 1

Similarily 2, 5, 8 …. divided by 3 $\to$ Rem = 2

Hence: 2,5,8,... all map to 2

The Mod 3 function is many to 1

There are an infinite number of values that map from $\mathbf{Z}^+$ to each value in the Range {0,1,2}

If the Codomain = {0,1,2} the Mod 3 function is Onto this Codomain

Note: The Mod m function maps every element in the Domain $\mathbf{Z}^+$ (positive Integers) to a unique value in the set {0,1,2,3,..., m-1}

Ex 2: Consider negative Integers in the Domain of Mod m function.

Note: $\frac{b}{a}$ = q + remainder r,

The remainder r is positive or 0 by definition and $0 \leqslant r < a$

(i) -44 ≡ ? mod 3:

Step1 $\frac{-44}{3}$ = - 14.66

$\frac{-44}{3}$ = - 14 - 0.66 (- 0.66 is not the remainder but it $\rightarrow$ the remainder $\neq$ 0)

$\frac{-44}{3}$ = - 14 - 1 + 1 - 0.66 = -15 + 0.34 (subtract / add 1 is done to ensure excess > 0)

Step 2 -44 - (-15 × 3) = -44 + 45 = 1 $\rightarrow$ rem = 1 $\rightarrow$ 1 = -44 mod 3

(ii) -82 ≡ ? mod 3

Step1 $\frac{-82}{3}$ = - 27.33

$\frac{-82}{3}$ = - 27 - 0.33 = -27 - 1 + 1 - 0.33 = -28 + 0.67

Step 2 -82 - (−28 X 3) = −82 + 84 = 2 → the remainder = 2 → 2 = −82 mod 3

(iii) In a similar way $\frac{-90}{3}$ $\rightarrow$ rem = 0 $\rightarrow$ 0 = -90 mod 3

Conclusion: The Congruence function mod 3 maps Negative Integers onto the Codomain {0,1,2}

Hence the Congruence function mod 3 maps all Z onto the Codomain {0,1,2}

3. Theorems concerning Division and Modular arithmetic

Note the three equivalent statements: $r = a \bmod m \leftrightarrow m \mid a - r \leftrightarrow a \equiv r \bmod m$

Ex 1: Theorem: For all a, b $\in$ **Z**, ($a \equiv b \mod m$) iff ($a \bmod m = b \bmod m$)

Part 1 (if): If ($a \bmod m = b \bmod m$) then ($a \equiv b \bmod m$)

Proof (Direct)

1.	Let $a \bmod m = r_1$	
2.	$\rightarrow$	Def of mod m
3.	$\rightarrow$	Def Division
4.	$\rightarrow$	Algebra, get r_1 on LHS
5.	Similarily if $b \bmod m = r_2$	
6.	$\rightarrow r_2 = b - q_2 m$, $q_2 \in \mathbf{Z}$	Def Mod, Div, Algebra
7.	Since $r_1 = r_2$	Given
8.	$\rightarrow$	Substitute
9.	$\rightarrow$	Algebra, leave a-b on LHS
10.	$\rightarrow m \mid (a-b)$	Def of Div
	$\rightarrow a \equiv b \bmod m$	Def of mod m

QED

Part 2 (only if): If $(a \equiv b \bmod m)$ then $(a \bmod m = b \bmod m)$

Proof (Contradiction)

1.	Either $(a \bmod m = b \bmod m)$ or $(a \bmod m \neq b \bmod m)$	list all possible conclusions
2.	Assume $a \bmod m \neq b \bmod m$	Assume not wanted conclusion
3.	let $a \bmod m = r_1$	
4.	m |	Def mod
5.		Def of Div
6.		Algebra, n_1 on LHS
7.	Similarily if $b \bmod m = r_2$	
8.		Def mod, Div, Algebra
9.		Assumption line 2
10.		Substitute
11.		Algebra, a-b on LHS
12.		Algebra, Factor
13.	m | a - b is false	Def of Div
14.	$\rightarrow a \equiv b \bmod m$ is false	Def mod
15.	Contradiction	Given $a \equiv b \bmod m$
	$\rightarrow a \bmod m = b \bmod m$	Only remaining possibility in line 1

QED

Ex 2: Theorem: $\forall a,b,c,m \in \mathbf{Z}$, $m \geq 2$, $c > 0$, if $a \equiv b \bmod m$ then and $ac \equiv bc \bmod mc$

Proof (Direct)

1.	$a \equiv b \bmod m$	Given
2.	$m \mid (a-b)$	Def of mod
3.	$a - b = qm,\ q \in Z$	Def division
4.	$(a - b)c = qmc$	Multiply by c
5.	$ac - bc = q(mc)$	Distributive, associative
6.	$mc \mid (ac - bc)$	Def of division
7.	$ac \equiv bc \bmod mc$	Def. of mod

QED

Ex 3: Consider the proposition: If $k \mid m n$ then $k \mid m$ or $k \mid n$.
Is the proposition true or false. Prove your conjecture.

Ex 4: When an Integer n is divided by 7 the remainder is 5.
What is the remainder when 9n is divided by 7 ?

Ex 5: State the value(s) of r if $r = n^2 \bmod 8$, $n \in \mathbf{Z}^+$, n is odd

Ex 6: Prove that $r \equiv 7 \bmod 13$ iff $4r \equiv 2 \bmod 13$