Modular Arithmetic and the Caesar Cipher

Yan Huang

Objectives

- Divisibility
- Prime and Composite Numbers
- Fundamental Theorem of Arithmetic
- `ceiling, floor, /, mod`
- Caesar cipher

Divisibility

- The set of ingtegers $\mathbb{Z} = \{\dots,\ -2,\ -1, 0, 1, 2,\ \dots\}$.

Def:

- "a divides b" if $az = b$ for some $z \in \mathbb{Z}$.

5 divides 10

because $5 \times 2 = 10$, and $2 \in \mathbb{Z}$

- We write $a|b$ to denote a divides b. We say a is a *divisor* of b and b is a *multiple* of a.

Divisibility

For all $a, b, c \in \mathbb{Z}$

$$a|a, \quad 1|a, \quad a|\,0.$$

$$a|a \iff a \cdot 1 = a, \; 1 \in \mathbb{Z}$$

$$1|a \iff 1 \cdot a = a, \; a \in \mathbb{Z}$$

$$a|0 \iff a \cdot 0 = 0, \; 0 \in \mathbb{Z}$$

Divisibility

"There exists"

For all $a, b, c \in \mathbb{Z}$

$$0|a \text{ if and only if } a = 0.$$

$0|a \iff \exists z$ such that $0 \cdot z = a$

$0 \cdot z = 0$ so, $0 \cdot z = a$ iff $a = 0$

Divisibility

For all $a, b, c \in \mathbb{Z}$

$$a|b \Leftrightarrow -a|b \Leftrightarrow a|-b.$$

$a|b \Leftrightarrow \exists k \in \mathbb{Z},\ ak = b.$

$-a \cdot k = a \cdot (-k) = b$

$\Rightarrow -a \mid b$ because $k \in \mathbb{Z}$.

Divisibility

For all $a, b, c \in \mathbb{Z}$

$$a|b \text{ and } a|c \Rightarrow a|(b+c).$$

$a|b \Leftrightarrow b = ka,\ k \in \mathbb{Z}$

$a|c \Leftrightarrow c = na,\ n \in \mathbb{Z}$

$\Rightarrow a(k+n) = ak + an = b + c,\ (k+n) \in \mathbb{Z}$

$\Rightarrow a|(b+c)$

$\blacksquare$

Divisibility

For all $a, b, c \in \mathbb{Z}$

$$a|b \text{ and } b|c \Rightarrow a|c.$$

Proof: $a|b \iff \exists\, k_1 \in \mathbb{Z}$ s.t. $a \cdot k_1 = b$

$b|c \iff \exists\, k_2 \in \mathbb{Z}$ s.t. $b \cdot k_2 = c$

$\Rightarrow a \cdot k_1 \cdot k_2 = c \qquad k_1 k_2 \in \mathbb{Z}$

$\Rightarrow a|c$

$\blacksquare$ ← QED

Divisibility

For all $a, b \in \mathbb{Z}$

$$a|b \text{ and } b|a \Leftrightarrow a = \pm b.$$

Proof: $a|b \Leftrightarrow b = ka, \ k \in \mathbb{Z}.$

$b|a \Leftrightarrow a = mb, \ m \in \mathbb{Z}.$

$a = mb = m \cdot (ka) = m \cdot k \cdot a$

$\Rightarrow mk = 1 \Rightarrow m = k = 1$ or $m = k = -1 \Rightarrow a = \pm b$

Primality

n is a ***prime*** if $n > 1$ and has no other positive divisor besides 1 and n.

n is a ***composite*** if $n > 1$ and is not a prime.

Primes:

2, 3, 5, 7, 11

Composite:

4, 6, 9,

The List of Primes

Fundamental theorem of arithmetic

Every non-zero integer n can be written as

$$n = \pm p_1^{e_1} \dots p_r^{e_r}.$$

where $p_1 < p_2 < \cdots < p_r$ are distinct primes and $e_1, \dots, e_r$ are non-negative integers. Moreover, the expression is unique.

$15 = 3 \times 5$ $\quad$ $23 = 23$ $\quad$ $12 = 2^2 \times 3$

$22 = 2 \times 11$ $\quad$ $4 = 2^2$

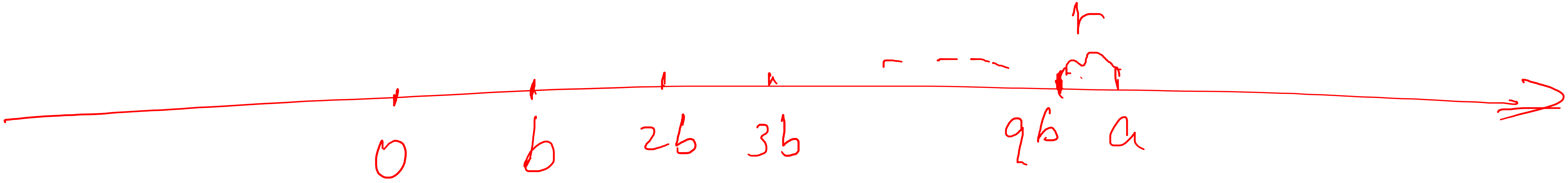
Division with Remainder

Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that

$$a = qb + r \text{ and } 0 \leq r < b.$$

e.g.

$a = 43$. $b = 5$. $43 = 5 \times 8 + 3$. $q = 8$. $r = 3$.



Floors

The **floor** function, denoted by $\lfloor \cdot \rfloor$, is a function from real numbers $\mathbb{R}$ to $\mathbb{Z}$. For every $x \in \mathbb{R}$, $\lfloor x \rfloor$ is the greatest integer $m \leq x$.

$\lfloor x \rfloor$ is uniquely defined for every x.

$\lfloor 5 \rfloor = 5$ $\quad$ $\lfloor 5.1 \rfloor = 5$ $\quad$ $\lfloor 4.999 \rfloor = 4$

Ceilings

The **ceiling** function, denoted by $\lceil \cdot \rceil$, is a function from real numbers $\mathbb{R}$ to $\mathbb{Z}$. For every $x \in \mathbb{R}$, $\lceil x \rceil$ is the smallest integer $m \geq x$.

$\lceil x \rceil$ is uniquely defined for every x.

$\lceil 5 \rceil = 5$ $\quad \lceil 5.1 \rceil = 6$ $\quad \lceil 4.9 \rceil = 5$

$\lceil -5 \rceil = -5$ $\quad \lceil -5.1 \rceil = -5$ $\quad \lceil -4.99 \rceil = -4$

The **mod** operator

Let $a, b \in \mathbb{Z}$ with $b > 0$, $a = qb + r$ and $0 \leq r < b$. We define

$$a \bmod b := r$$

$5 \bmod 3 = 2$ because $5 = 1 \times 3 + 2$

$105 \bmod 50 = 5$ because $105 = 2 \times 50 + 5$

The **mod** operator (Generalized Definition)

Let $a, b \in \mathbb{Z}$, we define

$$a \bmod b \coloneqq a - b\lfloor a/b \rfloor$$

$$-5 \bmod 2 = -5 - 2 \cdot \lfloor -5/2 \rfloor = -5 - 2(-3) = 1$$

$$5 \bmod (-2) = 5 - (-2) \lfloor 5/(-2) \rfloor = 5 + 2(-3) = -1$$

$$(-5) \bmod (-2) = (-5) - (-2) \lfloor (-5)/(-2) \rfloor = -5 + 2 \times 2 = -1$$

Day in a Week

September 1, 2016 is Thursday. What day is Oct 1, 2016?

$30 \bmod 7 = 2$

Oct 1, 2016 is 2 "+" Thursday = Saturday.

Messages Encoding & Decoding

- Per character:

```
encodeC :: Char -> Int
encodeC =

decodeC :: Int -> Char
decodeC =
```

Messages Encoding & Decoding

- Per character:

```
encodeC :: Char -> Int
encodeC 'A' = 0
encodeC 'B' = 1
...
encodeC 'Z' = 25
```

```
decodeC :: Int -> Char
decodeC 0 = 'A'
decodeC 1 = 'B'
...
decodeC 25 = 'Z'
```

Very tedious and unscalable.
Do you have better ideas?

Messages Encoding & Decoding

- Dealing with multi-character messages

```
encode :: [Char] -> [Int]
encode m = map encodeC m
```

```
encode :: [Char] -> [Int]
encode = map encodeC
```

Point-free form

Caesar Cipher (Shift Cipher)

Input *character* The encryption ***key***

Encryption: $C = (M + k) \bmod 26$

Decryption: $M = (C - k) \bmod 26$

Implementing Caesar Cipher

```
caesarC :: Int -> Int -> Int
caesarC k c = (c + k) mod 26

caesar :: Int -> [Int] -> [Int]
caesar = map . caesarC
```

Implementing Caesar Cipher

```
caesarDC :: Int -> Int -> Int
caesarDC k c = (c - k) mod 26

caesar :: Int -> [Int] -> [Int]
caesar = map . caesarDC
```