Modular Arithmetic

Ieuan David Vinluan

July 2024

Introduction

Modular arithmetic is a system of arithmetic where numbers are limited within a certain range and loop around after exceeding this range.

Introduction

Modular arithmetic is a system of arithmetic where numbers are limited within a certain range and loop around after exceeding this range.

- Telling the time...

Introduction

Modular arithmetic is a system of arithmetic where numbers are limited within a certain range and loop around after exceeding this range.

- Telling the time...
- The days of the week...

Introduction

Modular arithmetic is a system of arithmetic where numbers are limited within a certain range and loop around after exceeding this range.

- Telling the time...
- The days of the week...
- Months of a year...

Introduction

Modular arithmetic is a system of arithmetic where numbers are limited within a certain range and loop around after exceeding this range.

- Telling the time...
- The days of the week...
- Months of a year...
- Essentially anything that loops in a set pattern

Introduction

We work with the remainders of integers after they have been divided by a certain number, which we call the modulus. The modulus defines the length of the loop.

Example

If it is now 3:30 PM, we say that after 40 minutes, it will be 4:10 PM, not 3:70 PM. In this case, the modulus is 60.

Introduction

These are the terms and notations that we will be using for the rest of this lesson.

- $a \bmod b$ denotes the remainder of a when divided by b
- $a \equiv b \pmod{c}$ means that $a \bmod c = b \bmod c$

Exercises

Evaluate the following.

Exercises

Evaluate the following.

- $5 \bmod 3 =$

Exercises

Evaluate the following.

- $5 \bmod 3 = 2$

Exercises

Evaluate the following.

- $5 \text{ mod } 3 = 2$
- $365 \text{ mod } 7 =$

Exercises

Evaluate the following.

- $5 \bmod 3 = 2$
- $365 \bmod 7 = 1$

Exercises

Evaluate the following.

- $5 \bmod 3 = 2$
- $365 \bmod 7 = 1$
- $-3 \bmod 9 =$

Exercises

Evaluate the following.

- $5 \bmod 3 = 2$
- $365 \bmod 7 = 1$
- $-3 \bmod 9 = 6$

Exercises

Evaluate the following.

- $5 \bmod 3 = 2$
- $365 \bmod 7 = 1$
- $-3 \bmod 9 = 6$
- $96 \bmod 24 =$

Exercises

Evaluate the following.

- $5 \bmod 3 = 2$
- $365 \bmod 7 = 1$
- $-3 \bmod 9 = 6$
- $96 \bmod 24 = 0$

Operations in Modular Arithmetic

Like in our usual arithmetic, we can add, subtract, multiply, and divide integers. After each operation, we then divide the result by the modulus and take the remainder. Note that we are always supposed to be working with integers.

Modular Addition and Subtraction

Evaluate the expression $23 + 35 \bmod 22$.

Modular Addition and Subtraction

Evaluate the expression $23 + 35 \bmod 22$.

Example

Evaluate $23 + 35$ first; $23 + 35 = 58$. Then, take the remainder when 58 is divided by 22; $58 = 2 \cdot 22 + 14$. Thus, $23 + 35 \equiv 14 \bmod 22$.

Modular Addition and Subtraction

Evaluate the expression $(23 - 30) \text{ mod } 24$.

Modular Addition and Subtraction

Evaluate the expression $(23 - 30)$ mod 24.

Example

Evaluate $23 - 30$ first; $23 - 30 = -7$. Then, take the remainder when -7 is divided by 24: $-7 = -1 \cdot 24 + 17$. Thus, $23 - 30 \equiv 17$ mod 24.

Useful Properties in Modular Addition/Subtraction

Here are some of the more important properties of modular addition that you will need in many CompProg problems. Note that subtracting an integer is equivalent to adding its additive inverse.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

Useful Properties in Modular Addition/Subtraction

Here are some of the more important properties of modular addition that you will need in many CompProg problems. Note that subtracting an integer is equivalent to adding its additive inverse.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

- $a + b \equiv m + n \pmod{x}$

Useful Properties in Modular Addition/Subtraction

Here are some of the more important properties of modular addition that you will need in many CompProg problems. Note that subtracting an integer is equivalent to adding its additive inverse.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

- $a + b \equiv m + n \pmod{x}$
- $a + k \equiv m + k \pmod{x}$, and $b + k \equiv n + k \pmod{x}$

Useful Properties in Modular Addition/Subtraction

Here are some of the more important properties of modular addition that you will need in many CompProg problems. Note that subtracting an integer is equivalent to adding its additive inverse.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

- $a + b \equiv m + n \pmod{x}$
- $a + k \equiv m + k \pmod{x}$, and $b + k \equiv n + k \pmod{x}$
- Let $a + b = y$. Then, $(a \bmod x) + (b \bmod x) \equiv y \pmod{x}$

Exercises

Using the properties mentioned, evaluate:
$(2007 + 2014 + 2021) \bmod 7$

Exercises

Using the properties mentioned, evaluate:
$(2007 + 2014 + 2021) \bmod 7$

Example

We can take the remainder of each addend when it is divided by 7:
$(2007 + 2014 + 2021) \equiv (5 + 5 + 5) \equiv 15 \equiv 1 \pmod 7$

Using the properties mentioned, evaluate:
$(1 + 2 + 3 + \ldots + 100)$ mod 3

Exercises

Using the properties mentioned, evaluate:
$(1 + 2 + 3 + \ldots + 100)$ mod 3

Example

We can, again, take the remainder of each addend when it is divided by 3, which simplifies the sum into:
$(1 + 2 + 0 + 1 + 2 + 0 + \ldots + 0 + 1) \equiv (3 + 3 + \ldots + 3 + 1) \equiv (0 + 0 + \ldots + 0 + 1) \equiv 1 \pmod 3$

Useful Properties in Multiplication

Now, we can move on to modular multiplication.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

Useful Properties in Multiplication

Now, we can move on to modular multiplication.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

- $ab \equiv mn \pmod{x}$

Useful Properties in Multiplication

Now, we can move on to modular multiplication.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

- $ab \equiv mn \pmod{x}$
- $ak \equiv mk \pmod{x}$, and $bk \equiv nk \pmod{x}$

Useful Properties in Multiplication

Now, we can move on to modular multiplication.

Given $a \equiv m \pmod{x}$, $b \equiv n \pmod{x}$, and an integer k:

- $ab \equiv mn \pmod{x}$
- $ak \equiv mk \pmod{x}$, and $bk \equiv nk \pmod{x}$
- Let $ab = y$. Then, $(a \bmod x) \cdot (b \bmod x) \equiv y \pmod{x}$

Exercises

Using the properties mentioned (for modular multiplication!), evaluate: $(1 + 2 + 3 + \ldots + 100)$ mod 3

Exercises

Using the properties mentioned (for modular multiplication!), evaluate: $(1+2+3+\ldots+100)$ mod 3

Example

Let the sum be S. From the formula for the sum of an arithmetic sequence: $S = 1+2+3+\ldots+100 = 50 \cdot 101$. Then, we can easily compute S mod 3: $S \equiv 50 \cdot 101 \equiv 2 \cdot 2 \equiv 1 \pmod{3}$

Evaluate: $10! \bmod 11$

Evaluate: $10!$ mod 11

Example

Using some grouping:

$$\begin{aligned}
10! &\equiv 10 \cdot 9 \cdot 8 \cdot \ldots \cdot 1 \\
&\equiv (-1) \cdot (-2) \cdot \ldots \cdot (-5) \cdot 5 \cdot 4 \cdot \ldots \cdot 1 \\
&\equiv -120 \cdot 120 \\
&\equiv -(-1) \cdot (-1) \\
&\equiv -1 \\
&\equiv 10 \pmod{11}
\end{aligned}$$

Exercises

Evaluate: $2^{20} \bmod 7$

Exercises

Evaluate: $2^{20} \bmod 7$

Example

Recall that $2^3 \equiv 1 \pmod 7$. Then:

$$\begin{aligned} 2^{20} &\equiv 2^3 \cdot 2^3 \cdot \ldots \cdot 2^3 \cdot 2^2 \\ &\equiv 1 \cdot 1 \cdot \ldots \cdot 1 \cdot 4 \\ &\equiv 4 \pmod 7 \end{aligned}$$

Modular Division

Division only works when the divisor and the modulus are relatively prime. That is, given an integer divisor k and an integer modulus x: $\text{gcd}(k, x) = 1$.

Modular Division

Division only works when the divisor and the modulus are relatively prime. That is, given an integer divisor k and an integer modulus x: $\text{gcd}(k, x) = 1$.

- For integers a and b, if $ka \equiv kb \pmod{x}$ AND k and x are relatively prime, then $a \equiv b \pmod{x}$

Homework :3

Refer to the Reboot Website. Just ask for help if you need it!