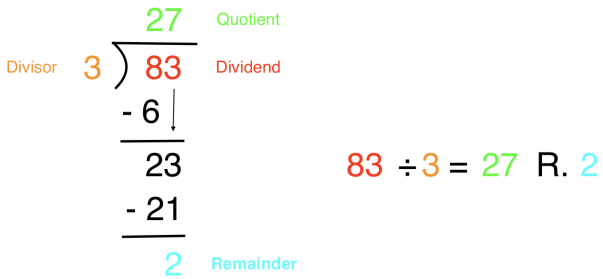
Grade 7/8 Math Circles

November 14/15/16/17, 2022

Modular Arithmetic

Divisibility

Integers are positive whole numbers, their negative counterparts, and 0.



The **remainder** is the value that is left after division, that is, the part of the dividend that cannot be equally divided by the divisor. The remainder of a division, in the case where the divisor is a positive integer n, is an integer betweeen 0 and $n-1$.

To find the remainder of a division $a \div b$, where a is an integer and b is a positive integer, find the largest multiple of b which is less than or equal to a and subtract this multiple from a.

Or, equivalently, just subtract or add b from or to a until the result is an integer between 0 and $b-1$.

Example 1

Since 35 is the largest multiple of 5 less than or equal to 36, the remainder of $36 \div 5$ is $36 - 35 = 1$.

Since -20 is the largest multiple of 4 less than or equal to -17, the remainder of $-17 \div 4$ is $-17 - (-20) = 3$.

Exercise 1

What are the remainders of the following divisions?

a) $8 \div 3$ b) $-10 \div 7$ c) $95 \div 8$ d) $-274 \div 10$

An integer a is **divisible** by another integer b if, for the division $a \div b$, the remainder is 0. That is, the result of the division is an integer. For example, 6 is divisible by 2 because $6 \div 2 = 3$.

Otherwise, if the remainder is not 0, we say that the integer a is **not divisible** by the integer b. For example, 83 is not divisible by 3 because $83 \div 3 = 27$ R. 2. So, the remainder is 2, not 0.

Motivation

In a year, there are four seasons: winter, spring, summer, and autumn. The four seasons exist in a cycle, meaning that there is no end and no beginning.

The current season is autumn. What season will it be 1 season from now? What about 4 seasons from now? What about 6 seasons from now? What about 9 seasons from now?

Notice how 1 season from now is the same as 9 seasons from now. They aren't equal because they will be two years apart, but they are the same season.

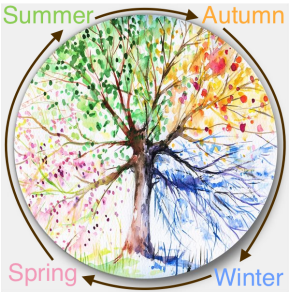


Figure 1: Retrieved from RONA.

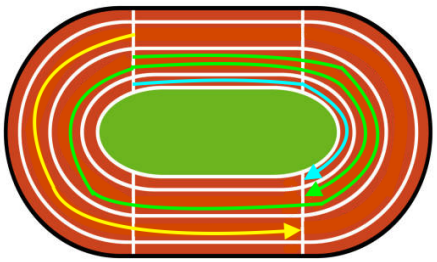


Figure 2: Retrieved from iStock.

Now, consider a 400 m track. I walk 200 m around the track, you walk 600 m, and we both start from the same position. We know that 200 m and 600 m are not the same, it would take a lot more effort to go 600 m as opposed to 200 m. However, these distances share something in common. Both of us will finish in the same position.

What distance could someone else walk, starting from the same starting position as us, to end in the same final position as us?

Stop and Think

What other examples are there of concepts that cycle?

Congruence

Let m be a fixed positive integer. For integers a and b, we say that a and b are **congruent modulo** m, written $a \equiv b \pmod{m}$, if a and b have the same remainder when divided by m. Otherwise, a and b are **not congruent** modulo m, written $a \not\equiv b \pmod{m}$.

The symbol $\equiv$ is referred to as **congruence** and m is called the **modulus**.

For example, since 6 and 0 both have remainder 0 when divided by 3, we write $6 \equiv 0 \pmod{3}$. And, since 83 and 2 both have remainder 2 when divided by 3, we write $83 \equiv 2 \pmod{3}$.

We use $\equiv$ instead of $=$ to emphasize that we are using a different kind of equality. Using $\equiv$ between two integers doesn't mean that the integers themselves are equal, it means their remainders when divided by the modulus are equal.

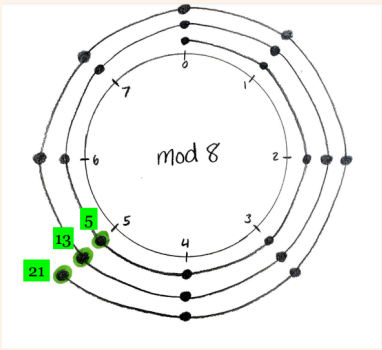
Note that the $\pmod{m}$ at the end of the congruence expression refers to the entire expression, not just to b. Imagine that it refers to the $\equiv$ symbol and is written as $\underset{(\text{mod } m)}{\equiv}$.

It is very important to remember that congruence is only defined for integers.

Example 2

We can visualize congruence by using circles. For example, with modulus 8, we label 8 portions of the circle as 0 through 7, since these are the possible remainders when dividing by 8. Let k be a positive integer. Starting at 0 and moving k steps in a clockwise direction, the number between 0 and 7 which we land on will be the remainder when k is divided by 8. That is, integer k which lands on that number will be congruent to that number modulo 8.

So, using the image to the right, we can see that 5, 13, and 21 all have remainder 5 when divided by 8. That is, 5, 13, and 21 are all congruent modulo 8 which is written as $5 \equiv 13 \equiv 21 \pmod{8}$.



Exercise 2

Fill in the blank with either $\equiv$ or $\not\equiv$.

a) $14 \_\_\_ 3 \pmod 8$ b) $6 \_\_\_ 9 \pmod 3$ c) $4 \_\_\_ 7 \pmod 4$ d) $5 \_\_\_ 1 \pmod 2$

Does the visual we used in Example 2 seem at all familiar? It should because analog clocks are set up in the same way.

The image to the right of an analog clock represents both the time 2 o'clock (in the morning) and 14 o'clock (2 o'clock in the afternoon).

Figure 3: Retrieved from Shutterstock.

Stop and Think

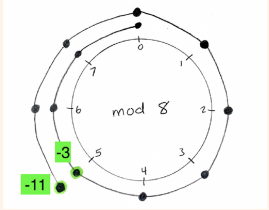
What modulus is used for analog clocks?

Analog clocks are our most intuitive understanding of modular arithmetic because many of us use the modular operations on time without even thinking of it.

Example 3

We can also visualize congruences with negative integers by using circles. This is the same method as Example 1 except that we are moving k steps in a counterclockwise direction.

So, using the image to the right, we can see that -3 and -11 both have remainders of 5 when divided by 8. That is, -3 and -11 are congruent modulo 8 which is written as $-3 \equiv -11 \pmod 8$.



And, since we found in Example 1 that 5, 13, and 21 all have remainder 5 when divided by 8, we have $-11 \equiv -3 \equiv 5 \equiv 13 \equiv 21 \pmod 8$.

Exercise 3

Fill in the blank with either $\equiv$ or $\not\equiv$.

a) $-4 \_\_\_ 3 \pmod 7$ b) $-2 \_\_\_ -7 \pmod 9$ c) $-1 \_\_\_ 15 \pmod 5$ d) $8 \_\_\_ -16 \pmod 3$

Properties of Congruence

Let m be a positive integer. Let a, b, and c be integers.

- $a \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.
- If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.
- $a \equiv 0 \pmod{m}$ exactly when a is divisible by m.
- If $a \equiv r \pmod{m}$ with $0 \leq r < m$, then r is the remainder when a is divided by m.

Example 4

- $5 \equiv 5 \pmod{7}$.
- $17 \equiv 3 \pmod{14}$ and $3 \equiv 17 \pmod{14}$.
- Since $98 \equiv 8 \pmod{3}$ and $2 \equiv 8 \pmod{3}$, we have $98 \equiv 8 \equiv 2 \pmod{3}$ or $98 \equiv 2 \pmod{3}$.
- $24 \equiv 0 \pmod{6}$ since 24 is divisible by 6.
- Since $48 \equiv 3 \pmod{5}$ and $0 \leq 3 < 5$, 3 is the remainder when 48 is divided by 5.

Exercise 4

Fill in the blank with either $\equiv$ or $\not\equiv$.

a) 4488 ___ $0 \pmod{17}$ since 4488 is divisible by 17.

b) 7 ___ $7 \pmod{9}$.

c) 564 ___ $5 \pmod{18}$ since 6 is the remainder when 564 is divided by 18.

d) $284 \equiv 5 \pmod{31}$ and 5 ___ $284 \pmod{31}$.

e) $-64 \equiv 118 \pmod{26}$ and $222 \equiv 118 \pmod{26}$, so -64 ___ $222 \pmod{26}$.

Applications

We've already seen that modular arithmetic is very useful when considering the four seasons, circular tracks, and analog clocks. But there are many other cycles to which we can apply the ideas of modular arithmetic.

- Days of the week (Mon, Tue, Wed, Thu, Fri, Sat, Sun)
- Months of the year (Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sept, Oct, Nov, Dec)
- Seconds in a minute (1, 2, ..., 59, 60)
- Minutes in an hour (1, 2, ..., 59, 60)
- Days in a month (28, 29, 30 or 31)
- Days in a year (365 or 366)
- Phases of the moon (New Moon, Waxing Crescent, First Quarter, Waxing Gibbous, Full Moon, Waning Gibbous, Third Quarter, Waning Crescent)
- Last digit of a number in the decimal number system (0, 1, .., 9)

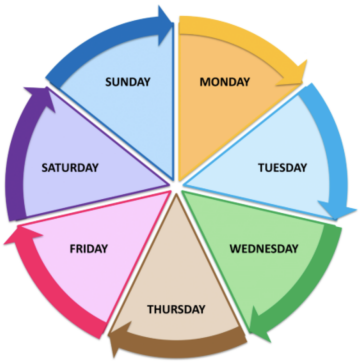


Figure 4: Retrieved from englishwsheets.

Figure 5: Retrieved from Printablee.

Figure 6: Retrieved from tes.

Modular Operations

Modular arithmetic is a system of arithmetic for integers where we start over once we reach a specified positive integer. That is, when we reach that positive integer, we count it as zero.

Modular arithmetic is just like normal arithmetic (operations on numbers: addition, subtraction, multiplication, exponentiation, etc.) but with congruences and is only defined for integers.

Note that modular division is possible, but it is a bit more complex and will not be covered in this lesson.

Modular Addition

With addition, we can can add an integer n to both sides of an equation and the equality holds: Since $a = b$, $a + n = b + n$. It turns out that we can extend this idea to congruences.

Modular Addition

Let m be a positive integer. Let a, b, c, and d be integers. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$. We can repeat this idea to add more pairs of congruent integers.

Example 5

Since $17 \equiv 4 \pmod{13}$ and $137 \equiv 7 \pmod{13}$, $17 + 137 \equiv 4 + 7 \equiv 11 \pmod{13}$.

We can verify this because we know that $17 + 137 = 154$. Since 154 has remainder 11 when divided by 13, we know that $154 \equiv 11 \pmod{13}$.

Exercise 5

Observe that $8 \equiv 25 \pmod{17}$, $19 \equiv 2 \pmod{17}$, and $0 \equiv 17 \pmod{17}$. Find an integer k, where $0 \leq k < 17$, which is congruent to the following sums **modulo 17** by using modular addition to simplify the calculations.

a) $25 + 19$ b) $19 + 17$ c) $25 + 19 + 17$ d) $19 + 19 + 17 + 25 + 19 + 19 + 19 + 17$

Additional Properties of Addition for Congruences

Let m be a positive integer. Let a, b, and c be integers.

- If $a + b = c$, then $a + b \equiv c \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a + k \equiv b + k \pmod{m}$ for any integer k
- If $a + b \equiv c \pmod{m}$, then $b + a \equiv c \pmod{m}$

The above properties can be very helpful to simplify expressions or integers using congruences. For example, $187 \equiv 180 + 7 \equiv 0 + 7 \equiv 7 \pmod{18}$ since $187 = 180 + 7$, $180 \equiv 0 \pmod{18}$, and $7 \equiv 7 \pmod{18}$.

Word Problem 1

Is $2093 + 4812 + 3838121$ divisible by 19?

Observe that

- $\begin{aligned} 2093 &\equiv 1900 + 190 + 3 && \pmod{19} \\ &\equiv 3 && \pmod{19} \end{aligned}$
- $\begin{aligned} 4812 &\equiv 1900 + 1900 + 1012 && \pmod{19} \\ &\equiv 1012 && \pmod{19} \\ &\equiv 200 + 200 + 200 + 200 + 200 + 12 && \pmod{19} \\ &\equiv 10 + 10 + 10 + 10 + 10 + 12 && \pmod{19} \\ &\equiv 62 && \pmod{19} \\ &\equiv 20 + 20 + 20 + 2 && \pmod{19} \\ &\equiv 1 + 1 + 1 + 2 && \pmod{19} \\ &\equiv 5 && \pmod{19} \end{aligned}$
- $\begin{aligned} 3838121 &\equiv 1900000 + 1900000 + 38121 && \pmod{19} \\ &\equiv 38121 && \pmod{19} \\ &\equiv 20000 + 18121 && \pmod{19} \\ &\equiv 1000 + 18121 && \pmod{19} \\ &\equiv 19121 && \pmod{19} \\ &\equiv 19000 + 121 && \pmod{19} \\ &\equiv 121 && \pmod{19} \\ &\equiv 20 + 20 + 20 + 20 + 20 + 20 + 1 && \pmod{19} \\ &\equiv 1 + 1 + 1 + 1 + 1 + 1 + 1 && \pmod{19} \\ &\equiv 7 && \pmod{19} \end{aligned}$

Using the above congruences and modular addition, we have

$$\begin{aligned} 2093 + 4812 + 3838121 &\equiv 3 + 5 + 7 && \pmod{19} \\ &\equiv 15 && \pmod{19} \end{aligned}$$

Since $0 \leq 15 < 19$, 15 is the remainder when $2093 + 4812 + 3838121$ is divided by 19. Since there is a nonzero remainder, $2093 + 4812 + 3838121$ is not divisible by 19.

Modular Subtraction

With subtraction, we can can subtract an integer n from both sides of an equation and the equality holds: Since $a = b$, $a - n = b - n$. It turns out that we can extend this idea to congruences.

Modular Subtraction

Let m be a positive integer. For all integers a, b, c, and d, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a - c \equiv b - d \pmod{m}$. We can repeat this idea to subtract more pairs of congruent integers.

Example 6

Since $17 \equiv 4 \pmod{13}$ and $137 \equiv 7 \pmod{13}$, $17 - 137 \equiv 4 - 7 \equiv -3 \equiv 10 \pmod{13}$.

We can verify this because we know that $17 - 137 = -120$. Since $-130 \equiv 0 \pmod{13}$, $-120 \equiv -130 + 10 \equiv 0 + 10 \equiv 10 \pmod{13}$.

Exercise 6

Observe that $-3 \equiv 6 \pmod{9}$, $11 \equiv 2 \pmod{9}$, and $9 \equiv 0 \pmod{9}$. Find an integer k, where $0 \leq k < 9$, which is congruent to the following differences **modulo 9** by using modular subtraction to simplify the calculations.

a) $11-9$ b) $9-11$ c) $(-3)-(-3)-9-11$ d) $11-9-9-11-9-9-(-3)-11$

Additional Properties of Subtraction for Congruences

Let m be a positive integer. Let a, b, and c be integers.

- If $a - b = c$, then $a - b \equiv c \pmod{m}$
- If $a \equiv b \pmod{m}$, then $a - k \equiv b - k \pmod{m}$ for any integer k

Word Problem 2

What is the last digit of $(38298 - 593 + 1283 - 9929 - 49348 + 239283 + 23825)$?

The last digit of an integer is just the remainder when divided by 10 because there are ten digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. So, we will be working with modulus 10. This means that for each integer we can ignore all except the last digit because the rest would be a multiple of 10 and so congruent to 0 modulo 10. For example, $38298 \equiv 38290 + 8 \equiv 0 + 8 \equiv 8 \pmod{10}$.

$$\begin{aligned} 38298 - 593 + 1283 - 9929 - 49348 + 239283 + 23825 &\equiv 8 - 3 + 3 - 9 - 8 + 3 + 5 \pmod{10} \\ &\equiv -1 \pmod{10} \\ &\equiv 9 \pmod{10} \end{aligned}$$

So, the last digit of $(38298 - 593 + 1283 - 9929 - 49348 + 239283 + 23825)$ is 9.

We could find the same answer by performing the addition and subtraction and then looking at the last digit, but this would require more work. There is also less of a risk of making an arithmetic error when working with the congruences.

Modular Multiplication

With multiplication, we can can multiply both sides of an equation by an integer n and the equality holds: Since $a = b$, $a \times n = b \times n$. It turns out that we can extend this idea to congruences.

Modular Multiplication

Let m be a positive integer. For all integers a, b, c, and d, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a \times c \equiv b \times d \pmod{m}$. We can repeat this idea to multiply by more pairs of congruent integers.

Example 7

Since $17 \equiv 4 \pmod{13}$ and $137 \equiv 7 \pmod{13}$, $17 \times 137 \equiv 4 \times 7 \equiv 28 \equiv 2 \pmod{13}$.

We can verify this because, using a calculator, we know that $17 \times 137 = 2329$. We have that

$$\begin{aligned}
2329 &\equiv 1000 + 1300 + 26 + 3 && \pmod{13} \\
&\equiv 1000 + 0 + 0 + 3 && \pmod{13} \\
&\equiv 1003 && \pmod{13} \\
&\equiv 990 + 13 && \pmod{13} \\
&\equiv 990 + 0 && \pmod{13} \\
&\equiv 990 && \pmod{13} \\
&\equiv 390 + 390 + 210 && \pmod{13} \\
&\equiv 0 + 0 + 210 && \pmod{13} \\
&\equiv 210 && \pmod{13} \\
&\equiv 130 + 80 && \pmod{13} \\
&\equiv 0 + 80 && \pmod{13} \\
&\equiv 80 && \pmod{13} \\
&\equiv 39 + 39 + 2 && \pmod{13} \\
&\equiv 0 + 0 + 2 && \pmod{13} \\
&\equiv 2 && \pmod{13}
\end{aligned}$$

Exercise 7

Observe that $15 \equiv 3 \pmod 4$, $21 \equiv 1 \pmod 4$, and $88 \equiv 0 \pmod 4$. Find an integer k, where $0 \leq k < 4$, which is congruent to the following products **modulo 4** by using modular multiplication to simplify the calculations.

a) 15×21 b) 21×15 c) $88 \times 21 \times 15$ d) $15 \times 15 \times 21 \times 15$

Additional Properties of Multiplication for Congruences

Let m be a positive integer. Let a, b, and c be integers.

- If $a \times b = c$, then $a \times b \equiv c \pmod m$
- If $a \equiv b \pmod m$, then $a \times k \equiv b \times k \pmod m$ for any integer k
- If $a \times b \equiv c \pmod m$, then $b \times a \equiv c \pmod m$

Word Problem 3

Gracee spends her summer volunteering at a public library. Her first day was on a Tuesday and she will volunteer every day for 52 days. What day of the week will be her last day volunteering?

Since there are seven days in a week, we have a modulus of 7. Note that $7 \times 7 \equiv 49 \equiv 0 \pmod 7$. So, $52 \equiv 49 + 3 \equiv 0 + 3 \equiv 3 \pmod 7$. This means that Gracee will have her last day three days after a Tuesday. So, her last day will be a Friday.

Word Problem 4

Bella is baking cookies for a school bake sale. One cookie sheet will contain 22 cookies and she wants to make bags which hold 3 cookies. If Bella bakes 14 full sheets of cookies, how many cookies will she have leftover?

The bags each hold 3 cookies, so we have a modulus of 3. The total number of cookies is 14×22. We have $14 \times 22 \equiv (12 + 2) \times (21 + 1) \equiv 2 \times 1 \equiv 2 \pmod 3$, so there will be 2 cookies left over.

Modular Exponentiation

We can also define modular exponentiation since exponentiation is just the repeated multiplication of a single number.

Modular Exponentiation

Let m be a positive integer. For all integers a and b, and positive integers k, if $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

Example 8

Since $15 \equiv 2 \pmod{13}$, $15^4 \equiv 2^4 \equiv 16 \equiv 3 \pmod{13}$.

Exercise 8

Observe that $23 \equiv 3 \pmod{10}$, $21 \equiv 1 \pmod{10}$, and $1430 \equiv 0 \pmod{10}$. Find an integer k, where $0 \leq k < 10$, which is congruent to the following powers **modulo 10** by using modular exponentiation to simplify the calculations.

a) 23^3 b) 21^8 c) 1430^{33429}

Additional Properties of Exponentiation for Congruences

Let m be a positive integer. Let a, b, and c be integers.

- If $a^b = c$, then $a^b \equiv c \pmod{m}$

Word Problem 5

What is the remainder when $(5999 + 66662^{12} - 1213^{29323}) \times 57^2$ is divided by 6?

Observe that

- $5999 \equiv 6000 - 1 \equiv -1 \pmod 6$
- $66662 \equiv 66660 + 2 \equiv 2 \pmod 6$
- $1213 \equiv 600 + 600 + 6 + 6 + 1 \equiv 1 \pmod 6$
- $57 \equiv 54 + 3 \equiv 3 \pmod 6$

$$\begin{aligned}
(5999 + 66662^{12} - 1213^{29323}) \times 57^2 &\equiv (-1 + 2^{12} - 1^{29323}) \times 3^2 && \pmod 6 \\
&\equiv (-1 + 2^{6\times 2} - 1) \times 9 && \pmod 6 \\
&\equiv ((2^6)^2 - 2) \times 3 && \pmod 6 \\
&\equiv (64^2 - 2) \times 3 && \pmod 6 \\
&\equiv (4^2 - 2) \times 3 && \pmod 6 \\
&\equiv (16 - 2) \times 3 && \pmod 6 \\
&\equiv 14 \times 3 && \pmod 6 \\
&\equiv 2 \times 3 && \pmod 6 \\
&\equiv 6 && \pmod 6 \\
&\equiv 0 && \pmod 6
\end{aligned}$$

So, the remainder when $(5999 + 66662^{12} - 1213^{29323}) \times 57^2$ is divided by 6 is 0.

We were able to find the remainder using simple calculations when applying congruence. However, if we had tried to evaluate the expression and then calculate the remainder, this would be very difficult. Trying to compute 1213^{29323} on most calculators will result in an overflow error.