BASIC KNOWLEDGE for Modular Arithmetic

Definition of Congruence Modulo m

The integers a and b are congruent modulo m if and only if a – b is divisible by m. This congruence is written as:

$a \equiv b \mod m$

m is a positive integer greater than 1 and is called modulus.

When a and b are divided by m, the same remainder is obtained.
The sign "≡" indicates congruence.

Examples

(1). In the 12-hour clock system, 14 and 2 are congruence modulo 12:

$14 \equiv 2 \mod 12$.

We can add or subtract 12 in any side of the equation.

(2). In the 7-day week system, a modulo 7 system applies.

Today is Thursday. What day will it be 30 days from today?

$30 \equiv 2 \mod 7$.

That is, 30 days from today will be Saturday.

Theorem 1

The following expression is unique:

$$a = qb + r$$
$$\frac{a}{b} = q + \frac{r}{b}$$

where a and b are integers,

b > 0, q is the quotient, and r is the remainder with $0 \le r < b$

If $\frac{a}{b} = q$ and we have $a = qb$, we say that a is divisible by b, or b|a $\Rightarrow$ we can also say b divides a.

Theorem 2

If $a \equiv b \quad \text{mod } lcm(m_1, m_2, m_3, \ldots m_k)$,

then $a \equiv b \quad \text{mod } (m_i) \quad i = 1, 2, 3, 4 \ldots, k$.

Theorem 3

If $\begin{matrix} a \equiv b & \text{mod } m \\ a \equiv b & \text{mod } n \end{matrix}$

then $a \equiv b \quad \text{mod } lcm(m, n)$

Theorem 4

If $\begin{matrix} a \equiv b & \text{mod } m \\ a \equiv b & \text{mod } n \end{matrix}$, and m and n are relatively prime,

then $a \equiv b \quad \text{mod } (m \times n)$

Theorem 5

If $a \equiv b \quad \text{mod } m$

and n|m,

then $a \equiv b \quad \text{mod } n$.

Theorem 6

If $a \equiv b \quad \text{mod } m$,

then $a^k \equiv b^k \quad \text{mod } m$

where k is a natural number.

Theorem 7

If
$$a \equiv b \mod m$$
$$c \equiv d \mod m$$

then
$$a \pm c \equiv b \pm d \mod m$$
$$a \times c \equiv b \times d \mod m$$

In general we cannot divide in modular arithmetic, but we do have the following cancellation rules:

If $ac \equiv bc \mod m$, and gcd (c, m) = 1, then $a \equiv b \mod m$

If $ac \equiv bc \mod m$, and gcd (c, m) = d > 1, then $a \equiv b \mod \frac{\text{m}}{\text{d}}$

Theorem 8

If a positive integer d | (a, b, m), then

$$ax \equiv b \mod \text{m, and}$$
$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$$

have the same solution.

Theorem 9

If
$$a_1 \equiv b_1 \mod m$$
$$a_2 \equiv b_2 \mod m$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$a_k \equiv b_k \mod m$$

then $a_1 \times a_2 \times \ldots . \times a_k \equiv b_1 \times b_2 \times \ldots . \times b_k \mod m$

PROBLEMS

Problem 1. A number N divides each of 17 and 30 with the same remainder in each case. What is the largest value of N?

Problem 2. A number N divides 17 with the remainder of R and divides 30 with the remainder 2R. What is the largest value of N?

Problem 3. If a certain number is divided by 2, 3, 4, or 5, the remainder is 1 in each case. What is the least number that satisfies these conditions?

Problem 4. If a certain number is divided by 2, 3, 4, or 5, the respective remainders are 1, 2, 3, and 4. What is the least number that satisfies these conditions?

Problem 5. The notation $a \equiv b \pmod{n}$ means $(a - b)$ is a multiple of n where n is a positive integer greater than one. Find the sum of all possible values of n such that both of the following are true: $171 \equiv 80 \pmod{n}$ and $468 \equiv 13 \pmod{n}$. (1995 Mathcounts State Team)

Problem 6. When n is divided by 2016, the remainder is 42. What is the remainder when n is divided by 24?

Problem 7. When a positive integer m is divided by 7, the remainder is 2; when a positive integer n is divided by 7, the remainder is 6. What is the remainder when $m \times n$ is divided by 7?

Problem 8. When two different numbers are divided by 7, remainders of 2 and 3, respectively, are left. What is the greatest possible three-digit product of these two numbers? (1998 Mathcounts Handbook Warm Up 12).

Problem 9. An integer has a remainder of 2 when divided by 6 and a remainder of 3 when divided by 7. Find the sum of all such integers from 1 to 1000.

Problem 10. When a two-digit number is multiplied by 5, the result is a three-digit number. When the digit 7 is written after the resulting three-digit number, the new four-digit number is 1281 greater than the original two-digit number. What is the original number? (1998-1999 Mathcounts National Target)

Problem 11. a and b are positive integers. When a is divided by 7, the remainder is 2. When b is divided by 7, the remainder is 1. What is the remainder when $a^2 + b$ is divided by 7?

Problem 12. When the three integers 618, 343, and 277 are divided by a positive integer, d, where d > 1, the remainders are the same. What is the smallest possible value of d? (Mathcounts 1993 National Sprint)

Problem 13. 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? (2003 Mathcounts State Sprint #26)

Problem 14. When Rachel divides her favorite number by 7, she gets a remainder of 5. What will the remainder be if she multiplies her favorite number by 5 and then divides by 7? (1999 Mathcounts National)

Problem 15. A digit can be placed in each of the boxes for the hundreds and units digits to form the least possible five-digit number divisible by 36. What is the ratio of the smaller digit to the larger digit? Express your answer as a common fraction. (1999 Mathcounts Nationals Sprint)

21□ 7 □

Problem 16. What is the greatest three-digit number that is one more than a multiple of 7 and three more than a multiple of 5?

Problem 17. When a positive integer is divided by 7, the remainder is 4. When the same integer is divided by 9, the remainder is 3. What is the smallest possible value of this integer? (2008 Mathcounts State Sprint #20)

Problem 18. The members of a band are arranged in a rectangular formation. When they are arranged in 8 rows, there are 2 positions unoccupied in the formation. When they are arranged in 9 rows, there are 3 positions unoccupied. How many members are in the band if the membership is between 100 and 200? (2009 Mathcounts Chapter #26)

Problem 19. The odd positive integers 1,3,5,7, ,….. are arranged in five columns continuing with the pattern as shown. Counting from the left, what column in which 1985 will appear? (1985 AMC 12)

	1	**3**	**5**	**7**
15	**13**	**11**	**9**	
	17	**19**	**21**	**23**
31	**29**	**27**	**25**	
	33	**35**	**37**	**39**
47	**45**	**43**	**41**	
	49	**51**	**53**	**55**
..	..	..	..	
	..	..	..	..

Problem 20. In year N, the 300th day of the year is a Tuesday. In year N +1, the 200th day is also a Tuesday. On what day of the week did the 100th day of year N - 1 occur? (2000 AMC 10 #25)

Problem 21. Katrina and Abbie start a game with one pile of 40 pennies. They take turns. On each turn, a player must take 1, 2, 3, 4 or 5 pennies from the pile. The player who takes the last penny from the pile of 40 pennies wins the game. If Abbie plays first, what number of pennies must she take from the pile on her first turn in order to guarantee that she can win the game? (2004 Mathcounts Team #7)

SOLUTIONS

Problem 1. Solution: **13**

From Theorem 7, we have

$17 \equiv r \pmod N$ (1)
$30 \equiv r \pmod N$. (2)

(2) – (1) $\Rightarrow$ $13 \equiv 0 \pmod N$

The largest value of N is 13.

Problem 2. Solution: **4**

$17 \equiv r \pmod N$ (1)
$30 \equiv 2r \pmod N$. (2)

Based on Theorem 7, we have:

$(1)\times 2 - (1)$:

$4 \equiv 0 \pmod N$

The largest value of N is 4.

Problem 3. Solution: **61**

Let the number be a,

$a \equiv 1 \mod 2$
$a \equiv 1 \mod 3$
$a \equiv 1 \mod 4$
$a \equiv 1 \mod 5$

Based on Theorem 4, we know that

$a \equiv 1 \mod [\text{lcm}(2,3,4,5)]$ or $a \equiv 1 \pmod{60}$

The least number will be 60 + 1 = 61.

Problem 4. Solution: **59**

$$\begin{cases} a \equiv 1 & \bmod 2 \\ a \equiv 2 & \bmod 3 \\ a \equiv 3 & \bmod 4 \\ a \equiv 4 & \bmod 5 \end{cases} \Rightarrow \begin{cases} a+1 \equiv 1+1 = 2 & \bmod 2 \\ a+1 \equiv 2+1 = 3 & \bmod 3 \\ a+1 \equiv 3+1 = 4 & \bmod 4 \\ a+1 \equiv 4+1 = 5 & \bmod 5 \end{cases} \Rightarrow$$

$$\begin{cases} a+1 \equiv 0 & \bmod 2 \\ a+1 \equiv 0 & \bmod 3 \\ a+1 \equiv 0 & \bmod 4 \\ a+1 \equiv 0 & \bmod 5 \end{cases}$$

Based on Theorem 4, we know that

$a+1 \equiv 0 \quad \bmod \operatorname{lcm}(2,3,4,5)$ or

$a+1 \equiv 0 \quad \bmod 60$

The least number will be 60 - 1 = 59.

Problem 5: Solution: **111**

171 – 80 ≡ 0 (mod n) and 468 - 13 ≡ 0 (mod n) $\Rightarrow$ 91 ≡ 0 (mod n) and 455 ≡ 0 (mod n)

$\Rightarrow$ 7×13 ≡ 0 (mod n) and 5×7×13 ≡ 0 (mod n).

The sum of all possible values of n such that both of the equations are true is: 7 + 13 + 91 =111.

Problem 6. Solution**: 18**

Based on Theorem 6 we know: $n \equiv 42 \pmod{2016}$

Since 2016 = 84×24, 24|2016

$n \equiv 42 \pmod{24} \quad \Rightarrow \quad n \equiv 18 \pmod{24}$.

The remainder is then 18.

Problem 7. Solution: **5**

$$a \equiv 2 \pmod 7$$
$$b \equiv 6 \pmod 7.$$

Based on Theorem 7, we have: $a \times b \equiv 12 \mod 7$ or $a \times b \equiv 5 \mod 7$.

The remainder is 5.

Problem 8. Solution: **993**

$$a \equiv 2 \mod 7$$
$$b \equiv 3 \mod 7$$

Based on Theorem 7, we have $a \times b \equiv 6 \pmod 7 \Rightarrow a \times b + 1 \equiv 0 \pmod 7$

The greatest 3-digit number will be 999: 999 = 142 × 7 +5 or $999 - 5 = 142 \times 5$

So $999 - 5 \equiv 0 \pmod 7$ or $994 \equiv 0 \pmod 7$

Since $a \times b + 1 \equiv 0 \pmod 7$, $a \times b + 1 = 994$
$a \times b = 994 - 1 = 993$ is the desired solution.

Problem 9. Solution: **11500**

The numbers, when 4 is added, will be divisible by 6 and 7. They form an arithmetic sequence with the common difference of 42. The smallest of these numbers is 42 - 4 = 38, so $a_1 = 38$. From $38 + 42(n-1) \le 1000$, we get $n \le 23$. So s = 23(76+22×42)/2 = 11500.

Problem 10. Solution: **26**

Let the two-digit number be 10a + b. We have

5(10a+b) = 100c +10d+e or

10a+ b = 1000c+100d+10e+7-1281

Solve this system equation, and we get

49(10a+b)= 1274, so

10a+b= 26.

Problem 11. Solution: **5**

We have: $\begin{cases} a \equiv 2 & \mod 7 \\ b \equiv 1 & \mod 7 \end{cases}$

Based on Theorem 7, we have: $\begin{cases} a^2 \equiv 4 & \mod 7 \\ b \equiv 1 & \mod 7 \end{cases}$ or $a^2 + b \equiv 4 + 1 = 5 \mod 7$

The remainder is then 5.

Problem 12. Solution 1: **11**

Let the remainder be r. We can write the following algebraic forms:

618 = dt + r (1)

343 = dw + r (2)

277 = dz+ r (3)

Where t, w, and z are positive integers.

(1) –(2) $\Rightarrow$ 275 = d(t-w)

(2) – (3) $\Rightarrow$ 66 = d(w-z)

(1) – (3) $\Rightarrow$ 341 = d(t-z)

Add all three equations together, we have 2dt = 682 or dt = 341 = 11 × 31. The smallest value for d is 11.

Solution 2. We have:

618 $\equiv$ r (mod d) (1)

343 $\equiv$ r (mod d) (2)

277 $\equiv$ r (mod d) (3)

Based on Theorem 7, we can say:

(2) – (3): 66 $\equiv$ 0 (mod d) (4)

(4) tells us that d should be divisible by 2, 3, or 11. Among these three numbers, both 2 and 3 divides 618. Only 11 gives the same remainder when divides 618, 343, and 277, so the smallest d is 11.

Problem 13. Solution: **3**

Official solution:

n^2 gives a remainder of 4 when divided by 5 and n^3 gives a remainder of 2 when divided by 5.
If n^2 gives a remainder of 4 when divided by 5, the number must have a square which ends in either 4 or 9.

Then, if n^3 gives a remainder of 2 when divided by 5, the number must also have a cube which ends in either 2 or 7.

Case I: Numbers that, when squared, end in 4, must end in 2 or 8. 2^3 = 8 so a number ending in 2, when cubed would end in 8. So n cannot end in 2. 8^3 = 512 so the number could end in 8.

Case II: Numbers that, when squared, end in 9, must end in 3 or 7. 7^3 = 343 so a number ending in 7, when cubed would end in 3. So n cannot end in 7. 3^3 = 27 so the number could end in 3.
When any number ending in 8 or 3 is divided by 5, the remainder will be 3.

My solution:

We have:

$$n^2 \equiv 4 \mod 5 \qquad (1)$$
$$n^3 \equiv 2 \mod 5 \qquad (2)$$

From (2), we have:

$n(n^2) \equiv 2 \mod 5 \quad \Rightarrow \quad 4n \equiv 2 \mod 5 \Rightarrow \quad 4n \equiv 12 \mod 5$

$n \equiv 3 \mod 5$

Problem 14. Solution: **4**

Let the unknown number be x, then

$x \equiv 5 \mod 7$

Based on Theorem 7, we have: $5x \equiv 5\times5 \equiv 4 \mod 7$.

So the remainder will be 4.

Problem 15. Solution: $\frac{1}{3}$

The number needs to be divisible by both 4 and 9. Therefore, the number formed by the last two digits must be divisible by 4 (it must then be 2 or 6) and the sum of the digit must be divisible by 9.
From this information, we then can write:

$2 + 1 + x + 7 + 2 \equiv 0 \mod 9 \quad \Rightarrow \quad 3 + x \equiv 0 \mod 9 \quad \Rightarrow \quad x = 6$

$2 + 1 + x + 7 + 6 \equiv 0 \mod 9 \quad \Rightarrow \quad x + 7 \equiv 0 \mod 9 \quad \Rightarrow \quad x = 2$

The ratio is $\frac{2}{6} = \frac{1}{3}$

Problem 16. Solution: **988**

Let the number be n. We can write

$$\begin{matrix} n \equiv 1 \mod 7 \\ n \equiv 3 \mod 5 \\ n \equiv 8 \mod 35 \end{matrix} \Rightarrow \begin{matrix} n \equiv 8 \mod 7 \\ n \equiv 8 \mod 5 \end{matrix} \Rightarrow$$

So $n = 35\times k+8$

where $k \equiv \left\lfloor \frac{999}{35} \right\rfloor = 28$

$n \equiv 35\times 28+8 = 988$

Problem 17. Solution: **39**

Official solution:

When a positive integer is divided by 7, the remainder is 4. When the same integer is divided by 9, the remainder is 3. We are asked to find the smallest possible value of this integer.

Let x be the number. Let y be the value when x is divided by 7 and let z be the value when x is divided by 9. Then,

$$\frac{x}{7} = y + 4$$

$$\frac{x}{9} = z + 3$$

$x = 7y + 28$

$x = 9z + 27$

$7y + 28 = 9z + 27$

$7y + 1 = 9z$

So when is $7y + 1$ a multiple of 9? Or what multiple of 9, when subtracted by 1 is a multiple of 7?
Let's just look at a few numbers: 9, 18, 27, 36, 45, 54, 63, 72, 81, 90, 99

Subtract 1 and we get: 8, 17, 26, 35, 44, 53, 62, 71, 80, 89, 98.

Are any of these multiples of 7? Yes. 35 = 7 × 5

Then y = 5 and z = 4

$$\frac{x}{7} = 5R4$$

$x = 7 \times 5 + 4 = 35 + 4 = 49$

Is this right?

39/7 = 5R4

39/9 = 4R

39 Ans.

My solution:

$n \equiv 9a + 3 = 7b + 4$

$9a + 3 = 7b + 4$

$9a = 7b + 1$

$9a = 7b + 1 \pmod 7$

$2a = 1 \pmod 7$

$2a = 8 \pmod 7$

$a = 4 \pmod 7$

The smallest value for a is 4, so the smallest value of n can be calculated as follows:

$n \equiv 9a + 3 = 9 \times 4 + 3 = 39$

Problem 18. Solution: **150**

Official solution:

If the members of a band are arranged in 8 rows, there are 2 positions unoccupied in the formation. If they are arranged in 9 rows, there are 3 positions unoccupied. We are asked to find how many members are in the band if the membership is between 100 and 200.

The fact that using 8 rows leaves 2 positions unfilled says that the number of members in the band is 2 less than a multiple of 8. That makes this an even number. We also know that the number of members is 3 less than a multiple of 9. Let's just enumerate even numbers that are 3 less than multiples of 9 between 100 and 200 and are even.

117 – 3, 135 – 3, 153 – 3, 171 – 3, 189 – 3 or 114, 132, 150, 168, 186

Now the numbers that are two less than a multiple of 8:

102, 110, 118, 126, 134, 142, 150, 158, 166, 174, 182, 190, 198

150 is in both lists. Does it satisfy the requirements?

$$\frac{150}{8} = 18R6 \quad (8 - 6 = 2)$$
$$\frac{150}{9} = 16R6 \quad (9 - 6 = 3)$$

Yes it does. 150 Ans.

My solution:

Let the number of students be n.

$$\begin{matrix} n \equiv -2 & \mod 8 \\ n \equiv -3 & \mod 9 \end{matrix} \Rightarrow \begin{matrix} n \equiv 6 & \mod 8 \\ n \equiv 6 & \mod 9 \end{matrix} \Rightarrow$$
$$n \equiv 6 \quad \mod 72$$

Because n is between 100 and 200, n = 2×72+6 = 150

Problem 19. Solution: **Second.**

Observe the pattern repeats every 8 integers (mod 8). So 1985 is the 993 terms and 993≡ 1 (mod 8). Thus 1985 will appear in the same column as the number 1 appears. That is the second column.

Problem 20. Solution: **Thursday**

Official Solution:

Note that, if a Tuesday is d days after a Tuesday, then d is a multiple of 7. Next, we need to consider whether any of the years N - 1, N, N + 1 is a leap year. If N is not a leap year, the 200th day of year N + 1 is 365 - 300 + 200 = 265 days after a Tuesday, and thus is a Monday, since 265 if 6 larger than a multiple of 7. Thus, year N is a leap year and the 200th day of year N + 1 is another Tuesday (as given), being 266 days after a Tuesday. It follows that year N - 1 is not a leap year. Therefore, the 100th day of year N - 1 precedes the given Tuesday in year N by 365 – 100 + 300 = 565 days, and therefore is a Thursday, since $565 = 7 \times 80 + 5$ is 5 larger than a multiple of 7.

Note that there is a typo in the official solution: "if" should be "is"

<u>My solution:</u>

We need to know two things before we start:

(1) There is one leap year every 4 years; and

(2) For regular years Monday in year N will be Tuesday in N + 1 year. (Because $365 \equiv 1 \bmod 7$).

In year N:

$300 \equiv 6$ (Tuesday) mod 7

Remainder	0	1	2	3	4	5	6
Day	W	Th	F	Sat	Sun	Mon	Tue

Then we have in year N:

$200 \equiv 4$ (Sunday) mod 7

$100 \equiv 2$ (Friday) mod 7

In the N + 1 year, the 200^{th} day should be:

$200 \equiv 4$ (Sunday + one day = Monday) mod 7

But we know that in year N +1, the 200th day is a Tuesday. Therefore, it advanced one more day than usual, so year N is a leap year. We can conclude that N – 1 year is not a leap year.

So for N – 1 year:

100 $\equiv 2$ (Friday – one day) mod 7.

The day must be Thursday.

Problem 21. Solution: **4**

If Abbie is able to leave 6 pennies for Katrina's last turn, no matter what Katrina does, Abbie can always win the game. We know that $40 \equiv 4$ mod 6. Abbie only needs to take 4 pennies from the pile on her first turn in order to guarantee that she can win the game. After her first turn, Abbie only needs to take whatever number that adds up to 6 with Karina's number. For example, if Katrina takes 1, Abbie will take 5; if Katrina takes 4, Abbie will take 2.

General case: We have n, the number of pennies, and $n \equiv b$ mod 6. If $b \neq 0$, the person who takes the pennies first has the winning strategy (first takes b pennies then taking whatever number of pennies that adds up to 6 with the opponent's number). If $b = 0$, the person who takes the pennies second has the winning strategy.