Math Level 2 Handouts Week 07

Dylan Yu

Online Classes Season 3

October 17, 2020

Contents

§ 1 Modular Arithmetic

§ 1.1 Modular Congruences

Let us start with a problem involving congruences:

Example 1. We have a clock with six numbers on its face: $0, 1, 2, 3, 4$, and 5. The clock only hand moves clockwise from 0 to 1 to 2 to 3 to 4 to 5 and back again to 0.

1. What number is the hand pointing at after 12 ticks?
2. What number is the hand pointing at after 28 ticks?
3. What number is the hand pointing at after 42 ticks?
4. What number is the hand pointing at after 1337 ticks?

Solution. We start by listing the first 30 numbers in the list and the first 30 positive integers side by side:

1	2	3	4	5	0		1	2	3	4	5	6
1	2	3	4	5	*0*		7	8	9	10	11	*12*
1	2	3	4	5	0		13	14	15	16	17	18
1	2	3	4	5	0		19	20	21	22	23	24
1	2	3	*4*	5	0		25	26	27	*28*	29	30

We can see that the answers to parts 1 and 2 are $\boxed{0}$ and $\boxed{4}$, respectively. We can also notice that each number on the left grid is the remainder of each number on the right grid when divided by 6. Hence, we see that the answer to part 3 is the remainder when $42 \div 6$, which is $\boxed{0}$, and that the answer to part 4 is $1337 \div 6$, which is $\boxed{5}$. □

§ 1.2 Congruences

Definition 1 (Congruence). Two integers are said to be **equivalent** (or **congruent**) modulo a if their difference is a multiple of a.

We shorten "modulo" to "mod", and use the symbol $\equiv$ to denote congruence. For example,

$$12 \equiv 0 \pmod 6 \text{ and } 32 \equiv 16 \pmod 4.$$

For integers x and y, $y \equiv x \pmod a$ if and only if $m \mid x - y$. Hence, for an integer z, we have $x - y = za$. Isolating z gives us $z = \frac{x-y}{a}$. If z is an integer, then $y \equiv x \pmod a$.

Theorem 1 (Congruence Condition). for positive integers x and y, $x \equiv y \pmod a$ if and only if

$$x = z_1 a + w, \text{ and}$$
$$y = z_2 a + w,$$

where z_1, z_2, and w are integers, and $0 \leq w < a$.

§ 1.3 Operations in Modular Arithmetic

Theorem 2 (Modular Addition and Subtraction). Let a_1, a_2, b_1, and b_2 be integers such that

$$a_1 \equiv a_2 \pmod n$$

$$b_1 \equiv b_2 \pmod n.$$

We can add these, and get

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n}.$$

Theorem 3 (Modular Multiplication). Let a, b, c, and d be integers. If

$$a \equiv b \pmod{m}$$
$$c \equiv d \pmod{m},$$

then

$$ac \equiv bd \pmod{m}.$$

Theorem 4 (Modular Exponentiation). Let a and b be integers, and c be a natural number. If $a \equiv b \pmod{m}$, then

$$a^c \equiv b^c \pmod{m}.$$

There is no law of division in modular arithmetic. We can see this with the following example: we have the congruence

$$6 \equiv 16 \pmod{10},$$

which is true. Dividing by 2, we have

$$3 \equiv 8 \pmod{10},$$

which is clearly not true.

§ 1.4 Modular Inverses

Definition 2 (Modular Inverse). The **multiplicative inverse** of an integer $a \pmod{m}$ is the integer a^{-1} such that

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

Example 2. Find the inverses of all mod 12 residues that have inverses.

Solution. We write out the entire modulo 12 multiplication table:

$\times$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	$\boxed{1}$	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	$\boxed{1}$	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	$\boxed{1}$	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	$\boxed{1}$

From this, we see that all modulo 12 residues that have inverses are $1, 5, 7$, and 11, and that there exists no inverses for residues $2, 3, 4, 6, 8, 9$, and 10.
We can note that $1, 5, 7$, and 11 are relatively prime to 12, and $2, 3, 4, 6, 8, 9$, and 10 are not. □

Theorem 5 (Existence of Modular Inverse). a^{-1} modulo n exists only if $\gcd(a, n) = 1$.

From the exercise above, it is pretty hard to find modular inverses. So how can we speed up the process? Let's start with an example:

Example 3. Find the inverse of 3 modulo 7.

Solution. We list the first few integers that are congruent to 1 (mod 7). They are

$$8, 15, 22, 29, \ldots$$

The term 15 is of the form $3x$, where $x = 5$. Thus, the inverse of 3 modulo 7 is $\boxed{5}$. □

§ 1.5 Examples

Example 4. A quick refresher:

(a) What are the remainders when $3333 + 4444$ and $3333 \cdot 4444$ are divided by 5?

(b) What is the remainder when 7^{2015} is divided by 48?

Solution. The numbering corresponds to the numbering above:

(a) We have $3333 \equiv 3 \pmod 5$ and $4444 \equiv 4 \pmod 5$, so $3333+4444 \equiv 3+4 \equiv 7 \equiv \boxed{2} \pmod 5$. Similarly, $3333 \cdot 4444 \equiv 3 \cdot 4 \equiv 12 \equiv \boxed{2} \pmod 5$. In general, we can take any integer and replace it with an integer within the same residue class. We can do this multiple times within a problem.

(b) At first, it seems that even modular arithmetic can't prevent this problem from becoming messy. However, upon further inspection, we can see that $7^2 = 49$, which leaves a remainder of 1 when divided by 48! Hence, we can write

$$7^{2015} \equiv 7 \cdot (7^2)^{1007} \equiv 7 \cdot 1^{1007} \equiv \boxed{7} \pmod{48}.$$

□

Example 5. I am thinking of a number. All I can give to you is that if you triple my number, it leaves a remainder of 13 when divided by 17. Unfortunately, this is clearly not enough information to figure out my number. However, it is enough information to figure out what the remainder of my original number is when divided by 17. What is this remainder?

Solution. A one-line solution: $\frac{17+13}{3} = \boxed{10}$. □

Example 6. Find the remainder when 5^{15} is divided by 128.

Solution. Apply the rules from before:

$$(5^3)^5 \equiv (-3)^5 \equiv -243 \equiv \boxed{13} \pmod{128}.$$

□

Example 7. Find the remainder when 12^9 is divided by 1000.

Solution. Apply the rules from before:

$$12^9 \equiv (1728)^3 \equiv (-272)^3 \equiv 984 \cdot (-272) \equiv (-16) \cdot (-272) \equiv \boxed{352} \pmod{1000}.$$

□

Example 8 (Paraguay 2012). Define a list of numbers with the following properties:

- The first number of the list is a one-digit natural number.
- Each number (since the second) is obtained by adding 9 to the number before in the list.
- The number 2012 is in that list.

Find the first number of the list.

Solution. Notice that they all are of the same residue modulo 9. Thus,

$$2012 \equiv \boxed{5} \pmod 9.$$

□

Example 9 (AMC 8 2014). The 7-digit numbers $\underline{74A52B1}$ and $\underline{326AB4C}$ are each multiples of 3. What is the sum of all possible values of C?

Solution. Observe that

$$7+4+A+5+2+B+1 \equiv A+B+19 \equiv A+B+1 \pmod 3,$$

so $A+B \equiv 2 \pmod 3$. From the second number, we have

$$3+2+6+A+B+4+C \equiv A+B+C \equiv 0 \pmod 3,$$

so we must have $C \equiv 1 \pmod 3$. Thus, $C = 1, 4, 7$, so our answer is $1+4+7 = \boxed{12}$. □

Example 10 (Mock AMC 10). The integers a, b, c, and d are four distinct prime numbers. If $d = a^2b^2 - 49c^2$, then what is the minimum possible value of $a+b+c$?

Solution. Factor to get $d = (ab-7c)(ab+7c)$. Observe that d is prime, so we must have $ab-7c = 1$. By trial and error, we find that $(a,b,c,d) = (3,5,2,29)$ works, so our answer is $3+5+2 = \boxed{10}$. □

Example 11 (iTest 2007). Find the remainder when $1+2+\cdots+2007$ is divided by 1000.

Solution. A simple addition in modular arithmetic:

$$\frac{2007 \cdot 2008}{2} \equiv 2007 \cdot 1004 \equiv 7 \cdot 4 \equiv \boxed{28} \pmod{1000}.$$

□

Example 12 (Purple Comet HS 2013). There is a pile of eggs. Joan counted the eggs, but her count was off by 1 in the 1's place. Tom counted in the eggs, but his count was off by 1 in the 10's place. Raoul counted the eggs, but his count was off by 1 in the 100's place. Sasha, Jose, Peter, and Morris all counted the eggs and got the correct count. When these seven people added their counts together, the sum was 3162. How many eggs were in the pile?

Solution. We must have

$$3162 + 100a + 10b + c \equiv 0 \pmod 7,$$

where a, b, and c are each ± 1. Simplifying mod 7, we have $5 + 2a + 3b + c \equiv 0 \pmod 7$. Observe that $(a, b, c) = (-1, 1, 1)$ works, so our answer is

$$\frac{3162 - 100 + 10 + 1}{7} = \boxed{439.}$$

□

Example 13 (Mandelbrot 2008-09). Determine the smallest positive integer m such that $m^2 + 7m + 89$ is a multiple of 77.

Solution. We split it up mod 7 and mod 11.

Mod 7. $m^2 + 7m + 89 \equiv m^2 + 5 \equiv 0 \pmod 7$, so $m \equiv 3, 4 \pmod 7$.

Mod 11. $m^2 + 7m + 89 \equiv m^2 - 4mm + 1 \equiv (m-2)^2 - 3 \equiv 0 \pmod{11}$, so $m \equiv 7, 8 \pmod{11}$.

Now, we just combine these two equivalences in all four possible ways to find our minimum solution. It turns out that $m = \boxed{18}$ is the minimum. □

Remark 1. A common strategy is to split up the primes of the modulo, i.e.

$$p_1^{e_1}, p_2^{e_2}, p_3^{e_3}, \ldots,$$

where

$$N = \prod_{p \in \mathbb{P}} p^{e_i} = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot \ldots.$$

Example 14. Prove that every year, including any leap year, has at least one Friday 13th.

Solution. It is enough to prove that each year has a Sunday the 1st. Now, the first day of a month in each

year falls in one of the following days:

Month	Day of the Year	mod 7
January	1	1
February	32	4
March	60 or 61	4 or 5
April	91 or 92	0 or 1
May	121 or122	2 or 3
June	152 or 153	5 or 6
July	182 or183	0 or 1
August	213 or 214	3 or 4
September	244 or 245	6 or 0
October	274 or 275	1 or 2
November	305 or 306	4 or 5
December	335 or 336	6 or 0

(The above table means that, depending on whether the year is a leap year or not, that March 1st is the 50th or 51st day of the year, etc.) Now, each remainder class modulo 7 is represented in the third column, thus each year, whether leap or not, has at least one Sunday the 1st. □

§ 1.6 Problems

Problem 1. Is $54+42 \equiv 2+14 \pmod 8$? Is $69-45 \equiv 18-15 \pmod 3$?

Problem 2. Let a, b, and c be integers whose residues modulo 8 are 4, 5, and 7, respectively. Compute the residue of $a+b+c \pmod 8$.

Problem 3. Is $9 \cdot 43 \equiv 8 \cdot 98 \pmod{23}$?

Problem 4. Find the modulo 4 residue of 100!.

Problem 5. The residues of 3 positive integers modulo 8 are $1, 4$, and 7. Find the residue of their products modulo 8.

Problem 6. Is $24^{14} - 15^{14}$ divisible by 9?

Problem 7. Find residue r such that $5^{6001} \equiv r \pmod 7$.

Problem 8. Does 6 modulo 25 have an inverse? Why?

Problem 9. Find all possible residues modulo 20 that have inverses.

Problem 10. Find all solutions to $48x - 115 \equiv 291 \pmod{13}$.

Problem 11. Find all solutions to $56x + 43 \equiv 211 \pmod{96}$.

Problem 12. John bought n boxes of cookies containing 11 cookies each. On the way home from the store, John notice that if he ate just one cookie, the total number of cookies remaining would be a multiple of 23. What is the smallest possible value of n.

Problem 13. Solve for N in

$$4N \equiv 3 \pmod 7,$$

$$5N \equiv 7 \pmod 8.$$

Problem 14 (AIME I 2010). Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999\ 9\text{'s}}$ is divided by 1000.

Problem 15 (AMC 10 B 2010). Positive integers a, b, and c are randomly and independently selected with replacement from the set $\{1, 2, 3, \ldots, 2010\}$. What is the probability that $abc + ab + a$ is divisible by 3?

Problem 16 (AMC 12 A 2010). The number obtained from the last two nonzero digits of 90! is equal to n. What is n?

Problem 17 (AHSME 1995). Consider the triangular array of numbers with 0,1,2,3,... along the sides and interior numbers obtained by adding the two adjacent numbers in the previous row. Rows 1 through 6 are shown.

$$\begin{array}{ccccccccccc}
 & & & & & 0 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 2 & & 2 & & 2 & & & \\
 & & 3 & & 4 & & 4 & & 3 & & \\
 & 4 & & 7 & & 8 & & 7 & & 4 & \\
5 & & 11 & & 15 & & 15 & & 11 & & 5
\end{array}$$

Let $f(n)$ denote the sum of the numbers in row n. What is the remainder when $f(100)$ is divided by 100?

Problem 18 (AMC 8 1999). What is the remainder when 1999^{2000} is divided by 5?

Problem 19 (AMC 10 B 2009). What is the remainder when $3^0+3^1+3^2+\ldots+3^{2009}$ is divided by 8?