Modular Arithmetic

Dylan Yu

March 26, 2021

Contents

1 Modular Congruences

Let us start with a problem involving congruences:

Example 1.1

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 $\underline{0}$ and $\underline{4}$, 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 0, and that the answer to part 4 is $1337 \div 6$, which is 5. □

1.1 Congruences

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

$$x = z_1a + w, \text{ and}$$
$$y = z_2a + w,$$

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

Example 1.4
How many positive integers less than 12 are relatively prime to 12?

Solution. We know that $1, 5, 7$, and 11 are relatively prime to 12, so the answer is 4. □

2 Operations in Modular Arithmetic

2.1 Basic Operations

- (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

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

- (Multiplication) Let a, b, c, and d be integers. If

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

  then

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

- (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.

2.2 Modular Inverses

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 2.2

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

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

×	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. □

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

Example 2.3
Find the inverse of 3 modulo 7.

Solution. We list the first few integers that are congruent to $1 \pmod 7$. 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 $\boxed{5}$. □

This method seems rather tedious for larger moduli and inverses - we need a systematic way to find inverses.

3 Units Digit

Example 3.1
Find the units digit of 2^{2020}.

Solution. The pattern is $2, 4, 8, 6, 2, 4, 8, 6, \ldots$. This means that it repeats every 4. Notice that $4, 8, 12, 16, \ldots$ all end in 6, and 2020 is also inside this sequence, so it must also end in $\boxed{6}$. □

Notice that **mod 10** gives us the **units digit**. This will be very important in the next problem!

Example 3.2
Karen is a teenager and the square of her age is equal to the number on her street address. If her age and the number on her street address have the same units digit, but do not add up to a multiple of 10, how old is Karen?

Solution. Let the age of Karen be k. This means that k^2 is her street address. This has the same units digit as k, so in mod 10,

$$k^2 \equiv k \pmod{10},$$

so if we test the possibilities, we get that $k \equiv 5, 6 \pmod{10}$ both work. However, if k ends in 5, so does k^2, so when we add them together, we will get a multiple of 10, which is not what we want! This means Karen's age ends in 6, and since she is a teenager, she has to be $\boxed{16}$. □

4 Examples

Example 4.1
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 4.2
What are the last two digits of the integer 17^{198}?

Solution. Note that $17^2 \equiv 289 \equiv -11 \pmod{100}$. Thus, the problem is simplified to computing $(-11)^{99} \equiv -11^{99} \pmod{100}$. Now note that by the Binomial Theorem

$$11^{99} = (10+1)^{99} = 10^{99} + \cdots + \binom{99}{2} 10^2 + \binom{99}{1} 10^1 + 1.$$

When this expansion is reduced modulo 100, all but the last two terms will go away since they are all divisible by 100, so $11^{99} \equiv \binom{99}{1} \cdot 10 + 1 \equiv 91 \pmod{100}$. As a result, $17^{198} \equiv -91 \equiv \boxed{09} \pmod{100}$. □

> *Remark 4.3.* There are some instances where modular division works. Don't count on it all the time, however.

Example 4.4
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 4.5 (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 4.6 (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 4.7 (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 4.8 (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 4.9. 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

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