Modular Arithmetic I

Neil Shah

primeri.org

This handout will be the first in a multi-part series on Modular Arithmetic. Together, this series should cover almost all of the theory required to solve AMC and AIME number theory problems.

§1 Divisibility

Before we dive into the topic of modular arithmetic, let's have a quick discussion on the subject of divisibility.

Definition 1.1. A number b is divisible by another number a if $\frac{b}{a}$ is an integer.

This is a pretty simple idea, but let's just go over some examples to drive the point home.

Example 1.2

Given the pair of numbers (a, b), determine if b is divisible by a.

(a) $(3, 7)$

(b) $(4, 28)$

(c) $(7, 35)$

It's easy to see that the first pair is **not** divisible while the other two are.

Fact 1.3. If both b and c are divisible by a, both $b - c$ and $b + c$ are divisible by a.

For example, 2 divides both 18 and 10. So, 2 also divides both $10 + 18 = 28$ and $18 - 10 = 8$.

Fact 1.4. If b is divisible by a and c is divisible by b, c is divisible by a.

For example, 4 is divisible by 2 and 8 is divisible by 4. It is then true that 8 is divisible by 2.

Definition 1.5 (GCD)**.** The greatest common divisor (GCD) of two numbers x and y is the largest number a such that both x and y are divisible by a. This is written as:

$$\gcd(x, y) = a$$

Definition 1.6. Two numbers x and y are deemed *relatively prime* if $\gcd(x, y) = 1$. This means that they share no common divisors other than 1.

An example of the above is the two numbers 4 and 9. The divisors of 4 are $1, 2, 4$ whereas the divisors of 9 are $1, 3, 9$. The greatest common divisor of the two numbers is 1, so the two numbers are relatively prime.

§2 Modular Arithmetic

Now that we have a better understanding of how divisibility works, let's learn the basics of modular arithmetic:

§2.1 Some Definitions

Definition 2.1. Two numbers x and y are **congruent** modulo n if they have an equal remainder when divided by n. This is written as:

$$x \equiv y \pmod{n}$$

Here's an example:

$$17 \equiv 10 \pmod{7}$$

This is true because the remainder when 17 is divided by 7 is 3. The same is true for 10.

Definition 2.2. A *residue* modulo n is the remainder (between 0 and $n-1$) when a number is divided by n.

Definition 2.3. A *residue class* is the set of numbers that share a specific residue.

For example, the remainder when 13 is divided by 9 is 4, which is between 0 and 12. So, the residue of 13 mod 9 is 4 and it belongs to the residue class $4 \pmod{9}$.

§2.2 Four Operations in Modular Arithmetic

Fact 2.4 (Addition and Subtraction)**.** If $x \equiv a \pmod{n}$ and $y \equiv b \pmod{n}$, it follows that $x + y \equiv a + b \pmod{n}$.

Note that one of more important results from this is that you can add multiples of n to either side of the congruence without having to worry about whether or not the statement is true. This follows because all multiples of n are congruent to 0 mod n.

Fact 2.5 (Multiplication)**.** If $x \equiv a \pmod{n}$ and $y \equiv b \pmod{n}$, it follows that $xy \equiv ab \pmod{n}$.

Fact 2.6 (Exponents)**.** If $x \equiv a \pmod{n}$, $x^k \equiv a^k \pmod{n}$.

Note that the above is a repeated application of Fact 2.5 (multiplication).

The last thing we have to cover regarding the four operations in Modular Arithmetic is division within congruences. Note that modular arithmetic itself has to do with the idea of performing operations on remainders, and as expected, there is some unexpected behavior when trying to divide within congruences. For example, we know that $10 \equiv 4 \pmod{6}$. However, dividing both sides of the congruence by 2 yields $5 \equiv 2 \pmod{6}$. This is an obviously false statement. However, there is still a correct way to divide in congruences, as seen in Fact 2.7:

Fact 2.7 (Dividing in Congruences)**.** If we have the congruence $ax \equiv bx \pmod{n}$, then it is true that:

$$a \equiv b \pmod{\frac{n}{\gcd(x, n)}}$$

Going back to the congruence $10 \equiv 4 \pmod 6$ that we just mentioned, let's check if Fact 2.7 holds true. We have:

$$5 \cdot 2 \equiv 2 \cdot 2 \pmod 6$$

$$5 \equiv 2 \pmod{\frac{6}{\gcd(2,6)}}$$

$$5 \equiv 2 \pmod 3$$

The above statement is true. It might be hard to remember that you can't just regularly divide in congruences like you would in a normal equation. Here are some opportunities to practice this so that you can get the idea down:

Exercise 2.8. Divide in each of the following congruences **if possible** using Fact 2.7:

1. $14 \equiv 2 \pmod 4$
2. $27 \equiv 2 \pmod 5$
3. $16 \equiv 4 \pmod 6$

§3 Fermat, Euler and Wilson

§3.1 Fermat's Theorem

Theorem 3.1 (Fermat)
For all primes p and numbers n such that n is not divisible by p:

$$n^{p-1} \equiv 1 \pmod p$$

The statement does not look complicated, but don't be fooled. This is one of the most important tricks at our disposal when solving AMC and AIME number theory problems. We'll go over some examples of how to use Fermat's Theorem when solving problems in the Examples section.

For now, let's move on to Euler's Theorem. Note that Fermat's Theorem is just a specific case of Euler's Theorem when dealing with primes.

§3.2 Euler's Theorem

The concept behind Euler's Theorem has to do with the definition we gave for the idea of relatively prime pairs of numbers in Definition 1.6. Recall that two numbers are relatively prime if their greatest common divisor is equal to 1.

Definition 3.2 (Euler's Totient Function)**.** Let $\phi(n)$ refer to the total number of positive integers less than or equal to n that are relatively prime with n.

Fact 3.3. If $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots p_m^{a_m}$ where the numbers p_k are the prime divisors of n:

$$\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_m})$$

Fact 3.3 is a rather important fact when it comes to applying Euler's Theorem. We'll prove this fact later in the series on Modular Arithmetic after we develop some further ideas.

Now that we've defined the Euler's Totient Function, here is Euler's Theorem itself:

Theorem 3.4 (Euler)
For all pairs of numbers x, n such that x and n are relatively prime, we have:

$$x^{\phi(n)} \equiv 1 \pmod{n}$$

When dealing with standard problems on the topic of modular arithmetic, this might be the most powerful tool in our arsenal. Now, let's move on to the last idea that we will cover in this handout.

§3.3 Wilson's Theorem

This idea is not as common as the other two theorems we covered in this handout. However, when it appears, you can use it to absolutely **DESTROY** problems.

Theorem 3.5 (Wilson)
For any prime p:

$$(p-1)! \equiv -1 \pmod{p}$$

Note that in this case the exclamation point refers to the factorial sign, where $n!$ is the product of all of the positive integers from 1 to n. Also, be careful when using Wilson's Theorem because it only works for a prime modulus.

Now that we've gone over the main tools that we use when solving standard number theory problems on the AMC and the AIME, let's go through some walkthroughs before the problem set.

§4 Examples

For each of these examples, multiple steps in the solution will be provided without giving the exact solution. The reason for this is so that the reader has the opportunity to gain valuable experience using these techniques without simply reading solutions.

Example 4.1 (1989 AIME 9)
One of Euler's conjectures was disproved in then 1960s by three American mathematicians when they showed there was a positive integer n such that

$$133^5 + 110^5 + 84^5 + 27^5 = n^5.$$

Find the value of n.

This problem can be quickly solved using an application of Fermat's Theorem along with some thinking. Follow along with the steps to try and solve the problem

1. What happens if you take the whole equation modulo 5? What is the result you obtain?
2. Try the same thing for (mod 3). What do you get?
3. Combine the results from parts 1 and 2 to figure out what form n must be in.
4. Think about what the logical bounds for n are. Using these bounds and form for n you got in part 3, get a final answer.

Once everything is said and done, you should've obtained a final answer of $\boxed{144}$.

Example 4.2 (2008 AMC12A 15)
Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

As before, follow along with the steps to try and find the correct answer. This question is just an application of the basic operations in modular arithmetic:

1. By which modulus should you take a number in order to obtain its unit digit? Let this be mod x.
2. Take k^2 mod x.
3. Take 2^k mod x. Here's a hint: repetition.
4. Add up the values from parts 2 and 3 to get your final answer.

If you solved the problem correctly, you should've obtained the answer $\boxed{6}$.

Example 4.3
What is the remainder when 97! is divided by 101?

Same process as before:

1. Using Wilson's Theorem, what can you say about the prime 101?
2. Using what you have in part 1, set up a congruence and isolate the parts that you need to get rid of.
3. Notice that $100 \equiv -1 \pmod{101}$. Try to see if you can use something like this to isolate only the parts that you need.
4. At this point, you should have a congruence of the form $a \cdot 97! \equiv 1 \pmod{101}$. You want to find a value x between 0 and 100 such that $ax \equiv 1 \pmod{101}$. For the value of a that you have, find a value that works. This should be your answer.

The correct answer to this problem will be $\boxed{17}$.

§5 Exercises

Now that we've gone over some examples, here are some examples using the methods we've learned in this handout. Note that these exercises are not ordered from easiest to hardest, and instead are intentionally ordered randomly so that people do not simply cherry pick and only try the easier problems. Also, sources will be given for each problem so that you can easily find the solution either by searching Google or AoPS (the Art of Problem Solving).

Exercise 5.1 (2017 AIME I 2)**.** When each of 702, 787, and 855 is divided by the positive integer m, the remainder is always the positive integer r. When each of 412, 722, and 815 is divided by the positive integer n, the remainder is always the positive integer $s \neq r$. Fine $m + n + r + s$.

Exercise 5.2 (1975 IMO 4)**.** When 4444^{4444} is written in decimal notation, the sum of its digits is A. Let B be the sum of the digits of A. Find the sum of the digits of B. (A and B are written in decimal notation.)

Exercise 5.3 (2004 AIME I 8)**.** Define a regular n-pointed star to be the union of n line segments $P_1P_2, P_2P_3, \ldots, P_nP_1$ such that

- the points $P_1, P_2, \ldots, P_n$ are coplanar and no three of them are collinear,
- each of the n line segments intersects at least one of the other line segments at a point other than an endpoint,
- all of the angles at $P_1, P_2, \ldots, P_n$ are congruent,
- all of the n line segments $P_2P_3, \ldots, P_nP_1$ are congruent, and
- the path $P_1P_2, P_2P_3, \ldots, P_nP_1$ turns counterclockwise at an angle of less than 180 degrees at each vertex.

There are no regular 3-pointed, 4-pointed, or 6-pointed stars. All regular 5-pointed stars are similar, but there are two non-similar regular 7-pointed stars. How many non-similar regular 1000-pointed stars are there?

Exercise 5.4 (2005 AIME II 4)**.** Find the number of positive integers that are divisors of at least one of $10^{10}, 15^7, 18^{11}$.

Exercise 5.5 (2019 AIME I 14)**.** Find the least odd prime factor of $2019^8 + 1$.

Exercise 5.6 (2018 AMC10B 16)**.** Let $a_1, a_2, \ldots, a_{2018}$ be a strictly increasing sequence of positive integers such that

$$a_1 + a_2 + \cdots + a_{2018} = 2018^{2018}.$$

What is the remainder when $a_1^3 + a_2^3 + \cdots + a_{2018}^3$ is divided by 6?

Exercise 5.7 (2019 AMC10A 25)**.** For how many integers n between 1 and 50, inclusive, is

$$\frac{(n^2-1)!}{(n!)^n}$$

an integer? (Recall that $0! = 1$.)

Exercise 5.8 (2019 BMT Discrete 5)**.** Let $2^{1110} \equiv n \pmod{1111}$ with $0 \leq n \leq 1111$. Compute n.

Exercise 5.9 (2004 HMMT Algebra 9)**.** A sequence of positive integers is defined by $a_0 = 1$ and $a_{n+1} = a_n^2 + 1$ for each $n \geq 0$. Find $\gcd(a_{999}, a_{2004})$.

Exercise 5.10 (2007 HMMT Guts 27)**.** Find the number of 7-tuples $(n_1, \ldots, n_7)$ of integers such that

$$\sum_{i=1}^{7} n_i^6 = 96957.$$

Exercise 5.11 (2007 PuMAC NT A9)**.** How many pairs of integers a and b are there such that a and b are between 1 and 42 and $a^9 = b^7 \mod 43$?

Exercise 5.12 (2007 PuMAC NT A1)**.** Find the last three digits of

$$2008^{2007^{\cdot^{\cdot^{\cdot^{2^1}}}}}.$$

Exercise 5.13 (2018 CMIMC NT6)**.** Let $\phi(n)$ denote the number of positive integers less than or equal to n that are coprime to n. Find the sum of all $1 < n < 100$ such that $\phi(n) \mid n$.

Exercise 5.14 (2002 SMT Advanced Topics 5)**.** 17 penguins are on an ice floe trying to divide up a booty of red herring amongst them. They find when they divide the fish up evenly, 13 are left over. Fighting for these extra fish causes 2 penguins to fall off the floe. When they redivide up the fish among the remaining 15 penguins, they end up with 7 left over. More fighting ensues and 2 more penguins fall off. Finally, the fish divide evenly for the remaining penguins. What is the smallest possible positive number of red herrings?