New Topics for Junior High Mathematics (2016-2017)

Modular Arithmetic [1]

Modular arithmetic consists of performing basic operations (adding, subtracting, multiplying, and exponents) all while staying within the set of possible remainders of a specific number. Notice that the possible remainders when dividing by 5 are 0, 1, 2, 3, and 4. As you run through the positive integers, this set of remainders repeat in that order:

Integer	...	12	13	14	15	16	17	18	19	20	21	...
Remainder when divided by 5	...	2	3	4	0	1	2	3	4	0	1	...

These remainders create *classes* which contain all of the numbers that have the same remainder. For example, the class of all integers that have a remainder of 2 when divided by 5 is denoted by $[2]_5$ or $[2]$ mod 5 and is equal to $\{2, 7, 12, 17, 22, \ldots\}$. There are also negative integers in this set as well.

Modular arithmetic is the system of performing operations on these classes. In particular, the following rules apply, with $[a]_n$ representing the class of remainders equal to a when divided by n:

- $[a]_n + [b]_n = [a + b]_n$
- $[a]_n - [b]_n = [a - b]_n$
- $[a]_n \cdot [b]_n = [a \cdot b]_n$
- $[a^m]_n = ([a]_n)^m$

The first rule says that you can add two classes together and you get the class that results from the remainder of the sum of any two elements from those classes. For example, let's work in mod 7 and simplify $[5]_7 + [4]_7$. To simplify this, we get $[5 + 4]_7 = [9]_7 = [2]_7$. Notice that we reduce 9 to 2 since both 9 and 2 are in the same class when dividing by 7 and 2 is the representative number from 0, 1, 2, ..., 6. So, in this sense, $5 + 4 \equiv 2 \pmod 7$, where the symbol $\equiv$ is used to show members of the same class in the modulus given on the right side. The symbol $\equiv$ can be read as "is equivalent to."

For another example, compute $[3]_8 \cdot [7]_8$. This would simplify to $[21]_8$. The remainder when $21 \div 8$ is 5, so $[21]_8 = [5]_8$. Here, $3 \cdot 7 \equiv 5 \pmod 8$.

Another example: find the remainder when 23^9 is divided by 7. It would take a long time to compute 23^9 and then an even longer time to divide that number by 7. However, if we use modular arithmetic, the problem is significantly shorter. The question asks for $[23^9]_7$. By the last rule above, we know that $[23^9]_7 = ([23]_7)^9$. In other words, find the remainder of $23 \div 7$ first, and then raise that remainder to the power. $[23]_7 = [2]_7$. So now we are dealing with $([2]_7)^9 = [2^9]_7 = [512]_7 = [1]_7$. So, $23^9 \div 7$ has a remainder of 1. Another short-cut that would help solve this problem is to notice that $[2^9]_7 = [(2^3)^3]_7 = [8^3]_7 = [1^3]_7 = [1]_7$.

> *Fermat's Little Theorem*
> If p is a prime number and a is any integer, then $a^p \equiv a \pmod p$.
> Further, if a is not divisible by p, then $a^{p-1} \equiv 1 \pmod p$.

[1] This document was prepared by Doug Ray for competition in years 2016 and 2017. If you have any questions about the material presented, please email `doug@academicmeet.com`.

Example: Find the remainder when 15^{12} is divided by 13.

Since 15 is not divisible by 13, 13 is prime, and $12 = 13 - 1$, we can use the second part of Fermat's Little Theorem to solve this problem. By this theorem, $15^{12} \equiv 1 \pmod{13}$.

Solving Modular Arithmetic Equations

Example If $4x + 3 \equiv 2 \pmod{7}$ and $0 \le x \le 6$, find x.

Here, we are working in mod 7. Start by solving the equation in the normal way. $4x+3 \equiv 2 \pmod{7} \implies 4x \equiv -1 \pmod{7}$. You can't divide 4 into -1 and get an integer, which is what these problems require. You need to find a number in the same class as $[-1]_7$ that is also a multiple of 4. Try adding 7 to -1 until you reach such a multiple: $-1 + 7 = 6$, $6 + 7 = 13$, $13 + 7 = 20$. Since 20 is a multiple of 4, we can divide $20 \div 4$ and get 5. So, 5 is the solution. In fact, $4(5) + 3 = 23 \equiv 2 \pmod{7}$.

Exploration Topic

For each number n, determine how many of the numbers from $1, 2, \ldots, n - 1$ there are that you can multiply by a number from $1, 2, \ldots, n - 1$ to get $1 \pmod{n}$.

For example, for $n = 8$, only the numbers 1, 3, 5, and 7 can be multiplied by other numbers to get 1. These numbers are called the *group of units*. The quantity of such numbers is symbolized by $\varphi(n)$ and is called the Euler's phi function. In this case, $\varphi(8) = 4$. φ is the Greek letter phi.

Research the various ways of computing $\varphi(n)$ and how to determine which numbers are in the group of units for various values of n.

Other topics: Chinese Remainder Theorem, quadratic residue

Sample Problems

Reduce each to the smallest positive representative of the class.

1. $[27]_5$
2. $[61]_3$
3. $[48]_{11}$
4. $[228]_{23}$
5. $[-7]_3$
6. $[-40]_9$

Find the remainder.

7. $347 \div 6$
8. $138 \div 3$
9. $(51 \times 46) \div 7$
10. $(61 \times 22) \div 12$
11. $3^9 \div 5$
12. $7^8 \div 9$
13. $17^{11} \div 11$

Solve.

14. If $5x + 4 \equiv 1 \pmod{11}$ and $0 \le x \le 10$, then find x.
15. If $7x - 13 \equiv 50 \pmod{17}$ and $0 \le x \le 16$, then find x.
16. Find $\varphi(10)$.
17. Find $\varphi(12)$.
18. Find $\varphi(98)$.
19. Find the smallest positive value of x such that $x \equiv 6 \pmod{7}$ and $x \equiv 4 \pmod{11}$.
20. Find the smallest positive value of x such that $x \equiv 2 \pmod{5}$ and $x \equiv 10 \pmod{13}$.