NASSAU COUNTY INTERSCHOLASTIC MATHEMATICS LEAGUE
ALL-STAR PROGRAM

$\forall^*$

Practice #6: Number Theory, Part II: Modular Arithmetic

Some warm-up problems:

1. Compute the last digit of 3^{2009}.

2. Given $a_n + a_{n+1} + a_{n+2} = 7$ for all positive integer values of n. If $a_3 = 5$ and $a_5 = 8$, compute a_{1998}. [NYSML 1998 I1]

3. Compute the value of $\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)^{2009}$.

In the last practice on number theory, we explored the idea of divisibility, that is, given an integer m, another integer n is divisible by m if there exists an integer k such that $n = mk$.

So, given an integer m, there exists a set of numbers ■ which are divisible by m. For example, $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$. By this method, we have partitioned the integers into sets of those that are "divisible by 3" and "not divisible by 3". The question arises as to whether or not there is a logical way to classify those integers that are not divisible by 3. Modular systems provide a method for doing this.

If we start by considering divisibility by 2, we can look at the two sets $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ and $\mathbb{Z} - 2\mathbb{Z} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}$. These two sets, of course, go by other names ("even" and "odd"), and modular arithmetic doesn't do anything to subdivide the odd integers any farther (we could split them into those numbers 1 greater than a multiple of 4 and 1 less than a multiple of 4, but we'll look at that in the context of multiples of 4 instead.)

However, when we compare $3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$ and $\mathbb{Z} - 3\mathbb{Z} = \{\ldots, -5, -4, -2, -1, 1, 2, 4, 5, \ldots\}$ we immediately notice that, on an informal level, that there are 2 elements of the latter set for each element of the former. This suggests that we might separate the set of integers not divisible by 3 into two groups: those one greater than a multiple of 3 ($\{\ldots, -5, -2, 1, 4, 7, \ldots\}$, referred to in a Mandlebrot competition as "odd-up") and those one less than a multiple of 3 ($\{\ldots, -4, -1, 2, 5, 8, \ldots\}$, which Mandlebrot called "odd-down"). Alternatively, the latter set can be described as "integers two greater than a multiple of 3". This suggests a partitioning of the integers into 3 **equivalence classes**:

$$3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\} = 3\mathbb{Z} + \{0\}$$
$$3\mathbb{Z} + \{1\} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$$
$$3\mathbb{Z} + \{2\} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$$

(The sum of two sets is formed by adding every element of the first to every element of the second.)

Under this system, which we will call the integers **modulo** 3 $(\mathbb{Z}/3\mathbb{Z})$, two numbers are considered **equivalent modulo** 3 if they fall in the same set of the three listed above. This is to say that two numbers are equivalent with respect to a given **modulus** m if they have the same remainder when divided by m. This definition of equivalence, however, can be somewhat inconvenient when dealing with negative integers (for example, is it obvious to you that when -43 is divided by 12, the remainder is 5?), so we should find another way of defining equivalence.

Notice that for each of the sets modulo 3, consecutive elements differ by 3. Elements which are non-consecutive are simply separated by elements that are all 3 apart, and so we conclude that the difference between any two elements of any of the equivalence classes is always a multiple of 3. This leads us to the following definition:

$a \equiv b \pmod{m}$ if and only if $a - b = mk$ for some integer k.

4. Prove that equivalence modulo m is an **equivalence relation**. That is, prove that it satisfies the following three properties (sometimes called the RST properties of equivalence):

a. **Reflexive** property: $a \equiv a \pmod{m}$ for all integers a.

b. **Symmetric** property: if $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$ for all integers a, b.

c. **Transitive** property: if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$ for all a, b, c.

Now, given our original set [redacted], we formed the other two **cosets** by adding the integers 1 and 2 to the original set. However, note that $3\mathbb{Z}+\{4\} = \{\ldots -2, 1, 4, 7, \ldots\} = 3\mathbb{Z}+\{1\}$. As a matter of fact, if we add *any* element of the set $3\mathbb{Z}+\{1\}$ to the set [redacted], we get the set $3\mathbb{Z}+\{1\}$. This suggests the rather interesting fact that if we add the sets [redacted] and $3\mathbb{Z}+\{1\}$, we get the set $3\mathbb{Z}+\{1\}$. In addition, if we add any element of $3\mathbb{Z}+\{1\}$ to any other element of $3\mathbb{Z}+\{1\}$, we get an element of $3\mathbb{Z}+\{2\}$. We rapidly find that the three cosets listed above form a group under addition, with the following addition table:

+	$3\mathbb{Z}+\{0\}$	$3\mathbb{Z}+\{1\}$	$3\mathbb{Z}+\{2\}$
$3\mathbb{Z}+\{0\}$	$3\mathbb{Z}+\{0\}$	$3\mathbb{Z}+\{1\}$	$3\mathbb{Z}+\{2\}$
$3\mathbb{Z}+\{1\}$	$3\mathbb{Z}+\{1\}$	$3\mathbb{Z}+\{2\}$	$3\mathbb{Z}+\{0\}$
$3\mathbb{Z}+\{2\}$	$3\mathbb{Z}+\{2\}$	$3\mathbb{Z}+\{0\}$	$3\mathbb{Z}+\{1\}$

Of course, there does seem to be an awful lot of superfluous writing here. The only part that differs from cell to cell in the table above is the remainder for each set. As such, we can allow each set to be represented by the single number in braces, that is, in the case of a modular system, we will

allow the *number* n to stand for the *set* $m\mathbb{Z}+\{n\}$. With this definition in mind, the modulo 3 addition table becomes:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

But hang on a minute here! We didn't actually <u>prove</u> that if you pick any element from, say, set 1 and any element from, say, set 2, the sum will always be from set 0. So let's do that formally:

<u>Theorem</u>: If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c \equiv b + d \pmod{m}$.

<u>Proof</u>: If $a \equiv b \pmod{m}$, then $a - b = mk$ for some integer k. Similarly, $c - d = mj$ for some integer j. Then, by addition, we see that

$$a - b + c - d = mk + mj$$
$$a + c - (b + d) = m(k + j)$$

which, by definition of equivalence, implies that

$$a + c \equiv b + d \pmod{m}.$$

This theorem suggests that if all we care about is the remainder when a given sum is divided by a given modulus, we can replace the addends with any other equivalent value, modulo m, and the result will be equivalent, modulo m.

5. Compute 8675309 + 314159 (mod 100).

What is even more interesting is that the theorem above also holds for multiplication:

6. Prove that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $ac \equiv bd \pmod{m}$. [Hint: show that $a \equiv b$ implies that $a = mk + b$.]

7. Compute (8675309) * (314159) (mod 8).

It can be shown (though not here) that the integers modulo m also satisfy the distributive property, and so the integers, modulo m, form a **ring**, which is a set of elements, along with two operations we call addition and multiplication, that satisfy the following 10 properties:

Properties of a Ring

1& 2: The set is commutative under addition and multiplication.

3&4: The set is associative under addition and multiplication.

5&6: The set contains both an additive identity (0) and a multiplicative identity (1).

7&8: The set is closed under both addition and multiplication, that is, if you add or multiply any two elements of the set, the result is also an element of the set.

9: The set contains an additive inverse (negative) for every element of the set.

10: The distributive property of multiplication over addition holds.

The only thing stopping the integers modulo m from being a full-fledged **field** (like the rational, real, or complex numbers) is the fact that there is an 11th property that does not hold: not every nonzero element of the integers (modulo m) has a multiplicative inverse. However, for the integers (modulo 3), we find that every nonzero element does have a multiplicative inverse:

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

As we can see above, 1 and 2 are both their own multiplicative inverses.

11. Construct a multiplication table for the integers modulo 4 and confirm that not every modular system is a field. Which nonzero element(s) do not have multiplicative inverses?

So, under what conditions are the integers, modulo m, a field? Well, if a number n has a multiplicative inverse, modulo m, then

$$an \equiv 1 \pmod{m}$$
$$an - 1 = km$$
$$an + (-k)m = 1$$

However, as we learned in the previous lesson on number theory, the smallest positive integer that can be expressed as a linear combination of m and n is gcd(m, n), and so the equation $an + (-k)m = 1$ will have a solution in integers if and only if m and n are relatively prime. If the modulus (m) is a prime number, however, then every number 1, 2, 3, …., (m-1) will be relatively prime to m, and so, every nonzero element will have a multiplicative inverse. On the other hand, if the modulus is not a prime, then some nonzero element will be a factor of m, and so not every element will have a multiplicative inverse.

Therefore, we reach the following conclusion:

The set of integers (modulo m) is a field if and only if m is a prime number.

12. Find the multiplicative inverse of 6, modulo 13. (It has to have one!)

13. Use your answer to 12 to solve the equivalence $6x \equiv 10 \pmod{13}$.

14. Solve $4x + 3 \equiv 6 \pmod{7}$.

15. Solve $4x + 3 \equiv 6 \pmod{10}$.

Of course, question15 is a trick question. Any number congruent to 6 (mod 10) will end with the digit 6 (or 4, if negative) and the number 4x + 3 is clearly odd. The fact that we cannot solve this equivalence uniquely is due to the fact that 4 and 10 are not relatively prime. However, such equivalences do not always have no solution. Consider $4x \equiv 6 \pmod{10}$. By trial-and-error, we quickly find that $x \equiv 4$ is a solution, but it is not the only one. When you are solving an equivalence where the coefficient and the modulus are not relatively prime, you can solve by dividing by the gcd, but you have to divide the modulus as well!

$$4x \equiv 6 \pmod{10}$$
$$2x \equiv 3 \pmod{5} \equiv 8 \pmod{5}$$
$$x \equiv 4 \pmod{5}$$

Since both 4 and 9 are in a mod-10 system and both are congruent to 4, modulo 5, the solution to this equivalence is $x \equiv \{4, 9\} \pmod{10}$.

16. Solve $6x + 9 \equiv 12 \pmod{15}$

Divisibility Tests

One other area that uses modular arithmetic is the area of divisibility. For example, it is a well-known fact that any number which is divisible by 2 ends in a 2, 4, 6, 8, or 0, but now we have an efficient way of proving this fact:

$$x \equiv 0 \pmod{2}$$
$$5x \equiv 0 \pmod{10}$$
$$x \equiv \{0, 2, 4, 6, 8\}$$

Other divisibility tests can be considered using modular arithmetic as well. For example, consider divisibility by 4. Let $d_n d_{n-1} \ldots d_1 d_0$ be a number where the d's represent the digits of the number. Thus:

$$d_n d_{n-1} \ldots d_1 d_0 = d_n 10^n + d_{n-1} 10^{n-1} + \ldots + 100 d_2 + 10 d_1 + d_0$$

Now, let's consider that expression modulo 4. Since 100, 1000, etc. are all divisible by 4:

$$\begin{aligned}
&d_n 10^n + d_{n-1} 10^{n-1} + \ldots + 100 d_2 + 10 d_1 + d_0 \\
&\equiv d_n 0^n + d_{n-1} 0^{n-1} + \ldots + 0 d_2 + 10 d_1 + d_0 \pmod 4 \\
&\equiv 10 d_1 + d_0 \pmod 4
\end{aligned}$$

Thus any number is equivalent to its final two digits, modulo 4, and so not only can you tell divisibility by 4 by looking at the last 2 digits, but you can tell the mod-4 value of a number which is *not* divisible by 4 in the same manner.

17. Prove a similar divisibility test for 8 in the same manner, and derive a rule for checking divisibility by 2^n.

Another famous divisibility test involves divisibility by 9. Since $10 \equiv 1 \pmod 9$, we find

$$\begin{aligned}
&d_n 10^n + d_{n-1} 10^{n-1} + \ldots + 10^2 d_2 + 10 d_1 + d_0 \\
&\equiv d_n 1^n + d_{n-1} 1^{n-1} + \ldots + 1^2 d_2 + 1 d_1 + d_0 \pmod 9 \\
&\equiv d_n + d_{n-1} + \ldots + d_1 + d_0 \pmod 9
\end{aligned}$$

Thus any number is equivalent to the sum of its digits, mod 9. Indeed, the same test can be used for mod-3, since 10 is also equivalent to 1, modulo 3.

18. $20! = 2432902008 1X 6640000$. Compute the missing digit X.

Last one: since $10 \equiv -1 \pmod{11}$, we can apply the same methodology:

$$\begin{aligned}
&d_0 + d_1 10^1 + d_2 10^2 + \ldots + d_n 10^n \\
&\equiv d_0 + d_1 (-1)^1 + d_2 (-1)^2 + \ldots + d_n (-1)^n \pmod{11} \\
&\equiv d_0 - d_1 + d_2 - d_3 + \ldots \pm d_n \pmod{11}
\end{aligned}$$

So we can find the value of any number, modulo 11, by alternately adding and subtracting the digits, starting from the right end.

Practice Problems:

1. [NYSML 2005 I3] Compute the smallest positive integer n that is a multiple of 9, uses each of the digits 0, 2, and 5 at least once, and uses no other digits.

2. [NYSML 2000 I3] In standard form, 5^3 is written as 125. Given $S = \{7^1, 7^2, 7^3, ..., 7^{1998}\}$. How many members of S have a units digit of 3 when written in standard form?

3. Compute the last digit of $7^{7^{2009}}$.

4. [NYSML 1998 I5] The ten digit integer 1998A1998B is divisible by 99. If neither A nor B is 0, compute the ordered pair (A, B).

5. [NYSML 2008 I8] Compute the number of $n \in \{1, 2, 3, ..., 2008\}$ for which $x^2 - y^2 = n$ has a solution with x and y integers.