CLASS 9, GIVEN ON 10/11/2010, FOR MATH 25

1. Integer mod n: modular arithmetic

Number theory asks questions about integers, such as when certain equations have solutions in integers. When studying these sorts of problems, it sometimes helps to replace all integers in a question with the remainders when divided by some fixed positive integer n. This leads to the study of *modular arithmetic* and the set $\mathbb{Z}/n\mathbb{Z}$, called the 'integers mod n', and the arithmetic operations of addition and multiplication which is defined on this set.

Let n be a fixed positive integer n. Let a, b be two integers. We say that a is *congruent* to b mod n if $n|(a-b)$, and sometimes write this as $a \equiv b \mod n$. One checks that congruence mod n satisfies the following properties:

Proposition 1. *Let a, b, c be integers. Then*

- $a \equiv a \mod n$, *for all a. (Reflexive property)*
- *If* $a \equiv b \mod n$, *then* $b \equiv a \mod n$. *(Symmetry property)*
- *If* $a \equiv b \mod n$ *and* $b \equiv c \mod n$, *then* $a \equiv c \mod n$. *(Transitive property)*

Proof. Reflexivity is obvious, since $a - a = 0$, and $n|0$. For symmetry, if $n|(a - b)$, then $n|(b-a)$, since $b-a = -(a-b)$. Finally, for the transitive property, if $n|(a-b)$ and $n|(b-c)$, then $(a - b) = nq, (b - c) = nq'$, for some integers q, q', and then $a - c = (a - b) - (b - c) = n(q-q')$. Since $q-q'$ is an integer, this means that $n|(a-c)$, or $a \equiv c \mod n$, as desired. □

Why do we care that these properties are satisfied? These three properties means that congruence mod n is what is known as an *equivalence relation*. If we look at an integer a, we can ask for the set of all integers which are congruent to $a \mod n$. This set is called the *congruence class* or *equivalence class* of $a \mod n$, and is written $[a]$ or sometimes $\overline{a}$. The number n is called the *modulus*. If we want to explicitly remind ourselves of the modulus n, we may write $[a]_n$. Alternative notations for the congruence class of $a \mod n$ also include $a \mod n$ or $a(n)$. Concretely,

$$[a] = \{a + qn | q \in \mathbb{Z}\} = \{\ldots, a - 2n, a - n, a, a + n, a + 2n, \ldots\}.$$

As a varies over integers, we get various congruence classes $[a]$. It is a general consequence of the fact that congruence is an equivalence relation that these congruence classes actually *partition* $\mathbb{Z}$. A partition of a set S is a collection of subsets S_i of S whose union is equal to S and which are pairwise disjoint (that is, any pair has empty intersection). Let's take the time to look at some examples.

Examples.

- Let $n = 1$. Then there is only one congruence class $\mod 1$, since given any two integers $a, b, 1|(a - b)$ always. So $[0] = [1] = [2] = [-4] = \mathbb{Z}$.
- Let $n = 2$. There are two congruence classes $\mod 2$, given by even and odd integers. Indeed, $a \equiv b \mod 2$ if and only if $2|(a - b)$ if and only if a, b have the same parity (ie, are either both odd or both even). So $[1] = [3] = [5] = [-27], [2] = [6] = [102] = [0]$.

- Let $n = 3$. There are three congruence classes $\mod 3$. These are given by numbers of the form $3k$, $3k+1$, and $3k+2$. For instance, $[0]$ consists of multiples of 3, while $[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$ consists of numbers of the form $3k+1$, while $[2]$ consists of numbers of the form $3k+2$.

These examples probably suggest that the number of congruence classes $\mod n$ is n. This is indeed the case, as the following proposition shows:

Proposition 2. *Let n be a fixed integer. Then $a \equiv b \mod n$ if and only if a, b have the same remainder after division by n. In particular, $[0]_n, [1]_n, \ldots, [n-1]_n$ are all the congruence classes of integers $\mod n$.*

Proof. If $a \equiv b \mod n$, then $n|(a-b)$. Suppose a, b have remainders r, r' and quotients q, q' after division by n. Then $a = qn + r, b = q'n + r'$, so $a - b = (q - q')n + (r - r')$. If $n|(a-b)$, then $n|(r-r')$, but since $0 \leq r, r' < n$, this is only possible if $r = r'$. Conversely, if $r = r'$, then $a - b = (q - q')n$, and clearly $n|(a-b)$.

We now check that $[0]_n, [1]_n, \ldots, [n-1]_n$ are all the congruence classes of integers $\mod n$. First, notice they are all different, since $[a] = [b]$ implies $n|(a-b)$, which is clearly impossible if a, b are distinct and chosen from $0, 1, \ldots, n-1$. These are all the congruence classes, since given any $[a]$, we have $[a] = [r]$, where r is the remainder upon division of a by n, and $0 \leq r < n$. □

This proposition tells us that the set of congruence classes $\mod n$ has exactly n elements and can be written as $[0], [1], \ldots, [n-1]$. We call this set the *integers* $\mod n$, and sometimes write this as $\mathbb{Z}/n\mathbb{Z}$, or sometimes $\mathbb{Z}_n$. We now want to show that we can add and multiply these congruence classes in the natural way.

Proposition 3. *Suppose that $a \equiv a' \mod n, b \equiv b' \mod n$. Then $a + b \equiv a' + b' \mod n$ and $ab \equiv a'b' \mod n$.*

Proof. If $a \equiv a' \mod n$, then $a = a' + q_1 n$ for some q_1, and similarly $b = b' + q_2 n$ for some q_2. Therefore $a + b = a' + b' + (q_1 + q_2)n$, which means $a + b \equiv a' + b' \mod n$. One can do something similar for multiplication; this is left as an exercise. □

The key point of this proposition is that it allows us to define addition and multiplication of residue classes in the natural way, and this definition makes sense. So we define addition of congruence classes $\mod n$ using the formula $[a] + [b] = [a + b]$, and multiplication via $[a][b] = [ab]$. We always add or multiply congruence classes to the same modulus n. We can also define subtraction as $[a] - [b] = [a - b]$, but we will need to wait a little while before defining division, because we need to worry about not 'dividing by 0'. We'll come back to this later.

The reason the previous proposition is necessary when defining addition or multiplication of equivalence classes this way is because the definition refers to the specific member a of the congruence class $[a]$, and we need to make sure that the definition is consistent regardless of which element of $[a]$ we choose to represent it. For instance, if we are looking at classes $\mod 4$, we know that $[1] + [2] = [3]$. Because $[1] = [9], [2] = [6]$, say, we would also like $[9] + [6] = [15] = [3]$, which is what the proposition above guarantees.

That this actually is an issue is made clear by the operation of exponentiation. For instance, consider the integers $\mod 3$. We have $4 \equiv 1 \mod 3$, but notice that $[2]^4 = [16] = [1]$, while $[2]^1 = [2]$. So we cannot define exponentiation of congruence classes, because this definition would not be *well-defined*.

A useful definition for the future is that of a *complete set of residues mod n*. A *residue* or *representative* of a congruence class is just a particular element of a congruence class. A complete set of residues mod n is a choice of residues (that is, integers) such that there is one residue from each of the n congruence classes mod n.

For instance, the complete set of residues consisting of least non-negative residues mod n is given by $0, 1, 2, \ldots, n-1$. This set will frequently appear in computations mod n, since these numbers are small and non-negative. Another set which will sometimes be of use is the complete set of least absolute residues, which consist of the residues from each congruence class which are smallest in absolute value. If n is odd, this set consists of $0, \pm 1, \ldots, \pm(n-1)/2$, and if n is even, $0, \pm 1, \ldots, \pm(n-2)/n, n/2$.

Examples.

- Find the remainder after division of 3^{16} by 11. Calculating 3^{16} by hand is really annoying, but calculating the least residue in the congruence class of $3^{16} \mod 11$ is not nearly as hard. We successively square 3, always taking the remainder mod 11 each time. For instance, $3^2 \equiv 9 \mod 11, 3^4 \equiv 9^2 \equiv 4 \mod 11, 3^8 \equiv 4^2 \equiv 5 \mod 11, 3^{16} \equiv 5^2 \equiv 3 \mod 11$. So the remainder after division of 3^{16} by 11 is 3. We could have also seen this by noticing that $3^4 \equiv 4 \mod 11$ implies that $3^5 \equiv 12 \equiv 1 \mod 11$, so that $3^{15} \equiv 1 \mod 11$, and then $3^{16} \equiv 3 \mod 11$.
- Show that the grade-school divisibility test by 3 and 9 is correct. (The test tells you that a number is divisible by 3 or 9 if and only if the sum of the digits is divisible by 3 or 9.) Suppose we are testing a number n, which has decimal digits $a_k a_{k-1} \ldots a_1 a_0$. This notation is really shorthand for the number $a_0 + 10^1 a_1 + \ldots + 10^k a_k$. This number is divisible by 3 if and only if it is $\equiv 0 \mod 3$. On the other hand, because $10 \equiv 1 \mod 3$, so that $10^i \equiv 1 \mod 3$, we have

  $$a_0 + 10^1 a_1 + \ldots + 10^k a_k \equiv a_0 + a_1 + \ldots + a_k \mod 3.$$

  Therefore, the original number is divisible by 3 if and only if the sum of its digits is divisible by 3, as desired. The exact same argument works with 3 replaced by 9, because $10 \equiv 1 \mod 9$ as well.
- Show that a number is divisible by 11 if and only if the alternating sum of its digits (where you alternate between adding and subtracting digits of the number) is divisible by 11. For instance, 1375 is divisible by 11 because the alternating sum of its digits is $1 - 3 + 7 - 5 = 0$, which is divisible by 11.

  This time we use the fact that $10 \equiv -1 \mod 11$. Therefore, $10^i \equiv 1 \mod 11$ if i is even, and $10^i \equiv -1 \mod 11$ if i is odd. Consider the number with decimal digits $a_k a_{k-1} \ldots a_1 a_0$. Then

  $$a_0 + 10^1 a_1 + \ldots + 10^k a_k \equiv a_0 - a_1 + a_2 - \ldots + (-10)^k a_k \mod 11,$$

  as desired.
- Show that the equation $x^2 - y^2 = 74$ has no solutions in integers. If this equation had a solutions in integers, it would also have solutions mod n for any integer n. Consider this equation mod 4. Because $74 \equiv 2 \mod 4$, this equation becomes $x^2 - y^2 \equiv 2 \mod 4$. However, $x^2 \equiv 0, 1 \mod 4$, as a case-by-case analysis shows, so $x^2 - y^2 \equiv 2 \mod 4$ is impossible, since $x^2 - y^2 \equiv -1, 0, 1 \mod 4$.

This last example illustrates a useful technique in number theory: it is possible to rule out the existence of integer solutions to polynomial equations sometimes by considering those equations mod n for suitably chosen n. This has the advantage of reducing a problem in which there are infinitely many cases to check to one in which there are only a finite number of cases. Of course, there is the problem that sometimes it is not possible to rule out integer solutions to polynomial equations in this way.