MOD NOTES

MATT GROTE

1. Definition

Formal definition Let a, b be integers and $n \in \mathbb{N}$. Then by $a \equiv b(mod\, n)$ we mean that $b - a = nk$ for some $k \in \mathbb{Z}$. This is read "a is equivalent to $b(mod\, n)$".

E.g.) $2 \equiv 5(mod\, 3)$ because $5 - 2 = 3(1)$.

Informal definition This is based around the idea of two numbers having the same remainder when divided by n.

E.g.) $8 \equiv 3(mod\, 5)$ because $8 - 3 = 5(1)$; but notice that $8 \div 5 = 1R3$.

2. Equivalence classes

Applying the definition, we see that $b - a = nk$ is the same as $b = nk + a$. Therefore every number equivalent to $a(mod\, n)$ will be some multiple of n plus a

E.g.) $2(mod\, 5)$ is equivalent to 2,7,12,17 but also -3,-8,-13, etc.

Since this is an equivalence relation, the set of all numbers equivalent to $a(mod\, n)$ form an equivalence class, which we denote $[a]$.

E.g.) Under $(mod\, 5)$, $[4] = \{m \in \mathbb{Z} : \exists k \in \mathbb{Z}, m = 5k + 4\} = \{..., -6, -1, 4, 9, 14, ...\}$

Notice that you must specify which $(mod\, n)$ you are talking about!

By convention, when describing an equivalence class we will always use the number a such that $0 \leq a < n$.

E.g.) In $(mod\, 5)$, $[7] = [2]$ but we use $[2]$.

3. Arithmetic

The set of distinct (not equal) equivalence classes $(mod\, n)$ is $[0], [1], ..., [n-1]$. With this understood, we adopt the convention of dropping [] and refer to $0, 1, ..., n - 1$.

Replacement In a practical sense, because of equivalence classes, whenever $a \equiv b(mod\, n)$ we can replace a with b in an equation using $(mod\, n)$.

E.g.) $7x \equiv 2x(mod\, 5)$. $3 + 11 \equiv 3 + 4(mod\, 7)$.

Addition, multiplication Addition and multiplication $(mod\, n)$ work just the same as normal addition and multiplication.

Inverses However, division does not exist $(mod\, n)$. Instead we have the idea of an inverse.

The inverse of $a(mod\, n)$, if it exists, is the unique number a^{-1} such that $aa^{-1} \equiv a^{-1}a \equiv 1(mod\, n)$.

The inverse of a exists if and only if a, n are coprime. This is because of a more complex theorem that shows us that $aa^{-1} - nk = 1$ if and only if a, n are coprime; but notice $aa^{-1} - nk = 1$ is the same as $aa^{-1} - 1 = nk$, which is the definition of $aa^{-1} \equiv 1(mod\, n)$.

Finding inverses There is no general quick way to find inverses at our disposal. We will have to find them by checking elements from each equivalence class. However several facts will speed things up:

–Just like how you can't divide by 0, there is never an inverse for $0(mod\, n)$.

–No matter n, 1 is always its own inverse.

–Notice that $(a^{-1})^{-1} = a$. Therefore inverses come in pairs.

–Since inverses are unique, once we find one inverse for an element there can't be any others.

E.g.) The inverses $(mod\, 7)$ are $1^{-1} = 1, 2^{-1} = 4, 3^{-1} = 5, 6^{-1} = 6$. Notice that a number can be its own inverse.

4. Solving equations

If x is unknown, then $ax \equiv b(mod\, n)$ has the solution $x \equiv a^{-1}b(mod\, n)$ if a is invertible. If a is not invertible, there is either no solution or no unique solution.

E.g.) $2x \equiv 4(mod\, 5)$. $2^{-1} = 3$ in $(mod\, 5)$, so $x \equiv 3 \cdot 4 \equiv 2(mod\, 5)$.

E.g.) $2x \equiv 0(mod\, 4)$. Here, 2^{-1} does not exist but $x = 2$ is a solution. However, so is $x = 0$; there are two solutions.

E.g.) $2x \equiv 3(mod\, 4)$ does not have any solutions.

Our focus will be on unique solutions.

Systems of equations A "system of equations" is fancy math talk for having multiple equations that we are hoping will share a solution. You have seen this before, for example, in finding the intersection of two lines:

E.g.) $y = x+2, y = -x-1$. Then $2y = 1$, $y = 1/2$; $1/2 = x+2$, $x = -3/2$. The solution is$(-3/2, 1/2)$.

Here we will solve systems of mod equations with one variable, x.

E.g.) Find x such that:

$$2x \equiv 5(mod\, 7)$$

$$3x \equiv 4(mod\, 5)$$

First notice that $2^{-1} = 4$ in $(mod\, 7)$ and $3^{-1} = 2$ in $(mod\, 5)$. Therefore, using the technique above, these equations can be rewritten as

$$x \equiv 6(mod\, 7)$$

$$x \equiv 3(mod\, 5)$$

There is a famous theorem called "the Chinese remainder theorem" that guarantees our ability to find a solution when we have a system of equation like this: the n's used for mod are coprime themselves. (You may assume this is true for this course.)

However this theorem does not tell us how to find the answer. This process is a bit arduous.

First we apply the definition of *mod*.

$$6 - x = 7k; x = 6 - 7k ...(1)$$

$$3 - x = 5q; x = 3 - 5q ...(2)$$

Where $k, q \in \mathbb{Z}$. We know that x must be the same in both equations, so we may make (1) and (2) equal:

$$6 - 7k = 3 - 5q; 7k - 5q = 3$$

The key here is this last equation, $7k - 5q = 3$. Our goal is to find integers for which this is true.

Solving equations with integers is a field of study in itself; for us, we will only use observation (plugging in values). On observation we find $k = 9, q = 12$ work.

Next we plug in k, q into (1), (2).

$$(1)...x = 6 - 7(9) = -57$$

$$(2)...x = 3 - 5(12) = -57$$

Since these values are the same, we know we haven't made a mistake so far. Finally we check our answers with the initial problem. $2(-57) = -104 \equiv 5 (mod\, 7)$, $3(-57) = -171 \equiv 4 (mod\, 5)$. So, $x = -57$ is a solution!

Notice! This x is <u>not</u> the same as equivalence classes from before. There are other answers: they are equivalent to $-57 \bmod 5 \cdot 7 = 35$. Why? The reasons are complicated, so we will have to leave this mysterious.

5. Applications

<u>Last digit</u> For a positive integer a, $a (mod\, 10)$ is the units place of a.

E.g.) $213 \equiv 3 (mod\, 10)$

Since we can replace any number in an equation by numbers in the same equivalence class, we can find the units digits of large numbers pretty easily.

E.g.) $13(17) \equiv 3(7) \equiv 21 \equiv 1 (mod\, 10)$.

E.g.) $17^8 \equiv 7^8 \equiv (7^2)^4 \equiv 9^4 \equiv (9^2)^2 \equiv 1^2 \equiv 1 (mod\, 10)$. The units digit is 1.

As someone noticed, this does not quite work for negative numbers. We can adapt to handle negative numbers, but we won't do this.

<u>Powers of i</u>

The unique powers of i are $1, i, -1$ and $-i$. These are i^0, i^1, i^2, i^3 respectively. Notice $i^4 = 1$, so that after these powers we begin repeating again.

Therefore i^k will depend only on what k is equivalent to $(mod\, n)$.

E.g.) $i^{22} = i^2 = -1$ because $22 \equiv 2 (mod\, 4)$.

We can also use what we know about mod arithmetic to answer different questions about i^k.

E.g.) If $k = 2x$ for some integer x, show that i^k is not a power of $-i$.

First notice that $-i = i^3$. From a previous example, we saw that $2x \equiv 3 (mod\, 4)$ has no solutions. Therefore there is no such number x and consequently no power i^k is equal to some power of $-i = i^3$.

Gears The usefulness of mod arithmetic is that it can model many situations. Often it is taught using the metaphor of a clock: suppose it is noon; 13 hours from now, the hour hand will be on 1, for instance.

Another such metaphor is gears.

E.g.) Two gears rely on the same crank. The first gear has 7 spokes, and the second has 5 spokes. One turn of the crank changes the first gear by 2 spokes, and changes the second gear by 3 spokes. Imagine that the gears are now set on spoke 0. How many turns of the crank are required so that the first gear is on its 5th spoke, and the second is on its 4th?

The difficulty here is setting up the equations. Let's take one at a time.

Let x be the number of cranks.

The first gear has 7 spokes, so it is represented by $(mod\, 7)$. We want to end on the 5th spoke, so we want $5(mod\, 7)$. Every crank moves two spokes, so $2x \equiv 5(mod\, 7)$.

The second gear has 5 spokes, so it is represented by $(mod\, 5)$. We want to end on the 4th spoke, so we want $4(mod\, 7)$. Every crank moves three spokes, so $3x \equiv 4(mod\, 5)$.

So, we are actually trying to solve:

$$2x \equiv 5(mod\, 7)$$
$$3x \equiv 4(mod\, 5)$$

This is the example given above, and we found that $x = -57$. Of course we cannot turn the crank a negative number of times, so we need a positive answer. As mentioned, this will be a positive number equivalent to $-57(mod\, 35)$; this is 13, so 13 cranks are needed.