MATH 115, SUMMER 2012
LECTURE 4
THURSDAY, JUNE 21ST

JAMES MCIVOR

Today we enter Chapter 2, which is the heart of this subject. Before starting, recall that last time we saw the integers have unique factorization into primes. To make sure you don't take this for granted, consider the following example.

Example 0.1. (Number system **without** unique factorization)
Let R be the set of all numbers of the form $a + b\sqrt{-5}$. It's a subset of $\mathbb{C}$. In this number system, we can add and multiply and subtract, which makes it a **ring** (more on rings later). It contains $\mathbb{Z}$. There is also a notion of primes in this ring. The usual integers 2 and 3 are prime, but there are other primes too. The number 6 has two factorizations:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

so the "Fundamental Theorem of Arithmetic" *fails* for this number system!

1. Congruences - What are They?

Congruence is a relationship between two integers - it's like equality, but a little looser. Before defining congruence, let's consider an informal example. Say we're studying an integer - we've called it x, but we don't know exactly what it is (maybe it's a potential solution to some equation or something like that). If we find out that $x = 5$, then there is no more to say - there is one and only one value for x. But sometimes equations can have more than one solution, and we would still like to know about them, even though in this case we can't pin them down exactly (since there are many possibilities). This is where congruence comes in handy. In such a situation, we might find, for instance, that

$$x \equiv 5 \mod 7,$$

which we read in English as "x is congruent to 5 modulo 7". This means that x can be any one of the numbers

$$5, 12, 19, 26, 33, 40, \ldots,$$

or even in the negative range: $-2, -9, -16, \ldots$. In other words, x is "almost" equal to 5, but ambiguous up to multiples of 7.

This ambiguity may seem annoying, but it's already familiar from high school: If you have to solve the equation

$$\cos x = \sqrt{2}/2,$$

you will say "$x = \pi/4$ or $x = 7\pi/4$, and actually $\pi/4$ or $7\pi/4$ plus any multiple of 2π will work, too." So you've found two basic solutions, but there are a bunch of

others obtained by adding or subtracting copies of 2π. Thus what you've found is that

$$x \equiv \pi/4 \mod 2\pi \text{ or } x \equiv 7\pi/4 \mod 2\pi$$

Definition 1. If a and b are two integers, and m is a positive integer[1], when we say a **is congruent to** b **modulo** m, written $a \equiv b \mod m$, we mean that $a = b + km$ for some integer k.

An equivalent way to state this is that a and b are congruent modulo m if m divides their difference, i.e., $m|b-a$. I prefer the above definition because intuitively, "if we ignore the multiples of m, then $a = b$". So some would say "congruent mod m" means "equal up to multiples of m."

Let's see some examples of this notion in familiar settings.

Examples 1.1.
(1) Even-ness and odd-ness (referred to as **parity**) can be expressed with congruences: an integer n is even iff it is congruent to 0 modulo 2. For n is even iff 2 divides n iff 2 divides n-0 iff $n \equiv 0 \mod 2$. Similarly, the odd integers are exactly those which are congruent to 1 mod 2.
(2) As you know, we write integers in base 10 notation, so the different digits correspond to different powers of ten. Intuitively, working mod 10 means ignoring all the multiples of 10, so if we take a number, say 38854727, we see that it is congruent to 7 modulo 10, since $38854727 = 7 + 3885472 \cdot 10$. Similarly, when working modulo 100, we may just omit the digits in the hundreds place and beyond: since $38854727 = 27 + 388547 \cdot 100$, we have $38854727 \equiv 27 \mod 100$.

2. Properties

Let's now see some properties of congruences. You should pay attention to which properties they have in common with equality, and also which properties of equality *don't hold* for congruence.

In the following, a, b, c, d are arbitrary integers, m a positive integer.

(1) (Symmetry) If $a \equiv b \mod m$, then $b \equiv a \mod m$.
(2) (Transitivity) If $a \equiv b \mod m$ and $b \equiv c \mod m$, then $a \equiv c \mod m$.
(3) (Reflexivity) $a \equiv a \mod m$.
(4) (Subtraction Rule) If $a \equiv b \mod m$, then $a - b \equiv 0 \mod m$.
(5) (Addition Rule) If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$.
(6) (Multiplication Rule) If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.
(7) (Reduction of Modulus Rule) If $a \equiv b \mod m$ and $d|m$, $d > 1$, then $a \equiv b \mod d$.
(8) (Scalar Multiplication Rule) If $a \equiv b \mod m$ and $c > 0$, then $ac \equiv bc \mod mc$.

[1]Technically, we could allow m to be negative as well, but we don't gain anything extra from doing so.

(9) (Polynomial Substitution Rule) If $a \equiv b \mod m$ and $f(x)$ is a polynomial with integer coefficients, then $f(a) \equiv f(b) \mod m$

The first three properties can be summarized by saying that "congruence modulo m is an **equivalence relation**". The fourth was an observation we made above. The names of the remaining properties I just made up, but hopefully they help you remember them. Notice in (8) that the modulus m ALSO gets multiplied by c! It's also true that $ac \equiv bc \mod m$ but the statement in 8 is stronger. Let's prove (6) and (8) to give you an idea of how to work with congruences:

Proof. (of (6)) If $a \equiv b \mod m$ and $c \equiv d \mod m$, then by the definition we have

$$a = b + km \text{ and } c = d + lm$$

for some integers k and l. What we want to show is that $ac - bd$ is a multiple of m. So let's write it out and replace a and c using the above equations:

$$ac - bd = (b + km)(d + lm) - bd = dkm + blm + klm^2 = (dk + bl + klm)m,$$

which shows that $ac - bd$ is a multiple of m, hence $ac \equiv bd \mod m$. □

Proof. (of (8)) Let $a \equiv b \mod m$ and $c > 0$; to show $ac \equiv bc \mod mc$, we have to show that $ac - bc$ is a multiple of mc. But we know that $a - b = km$ for some k, so multiplying this equation through by c does it. Notice that it even works for c negative - the only reason we say $c > 0$ in the statement is that in our definition of congruence we took the modulus m to always be positive. □

Since congruence is a way of talking about divisibility, it is natural to ask how it relates to the gcd. This is related to a very important point: *the main reason congruence is different from equality is that you cannot always cancel something from both sides*!

For example, when dealing with equalities, if we know that

$$5x = 5y,$$

then it follows that $x = y$. We can cancel any nonzero number from an equality and obtain another valid equality. This is not true for congruence! For example,

$$5 \cdot 2 \equiv 5 \cdot 4 \mod 10,$$

but

$$2 \not\equiv 4 \mod 10.$$

But *sometimes* it works... For example

$$3 \cdot 4 \equiv 3 \cdot 14 \mod 10$$

and here we *can* cancel the three and get

$$4 \equiv 14 \mod 10,$$

which is true. So why can we cancel the 5 and not the 3? The reason is that 5 shares a common factor with the modulus 10, which can sometimes cause a problem. What we can say about cancelling terms from a congruence is the following:

Theorem 1. *If $ax \equiv ay \mod m$ and $(a, m) = 1$, then we can cancel the a and get $x \equiv y \mod m$. More generally, $ax \equiv ay$ if and only if $x \equiv y \mod (m/(a, m))$.*

Informal version: If a is relatively prime to the modulus, we may divide both sides by a. If not, we have to divide the modulus m by the gcd of a and m in order to cancel the a.

Let's see how this latter statement fixes our problem with 5s above. From the congruence $5 \cdot 2 \equiv 5 \cdot 4 \mod 10$, we *cannot* conclude that $2 \not\equiv 4 \mod 10$, but we get a valid congruence if we divide the modulus by the gcd of 5 and 10, namely 5, giving $2 \equiv 4 \mod 2$, which *is* true.

Proof - see textbook.

Another useful and easy fact is the following:

Lemma 1. *If two integers a and b are congruent mod m, then $(a, m) = (b, m)$.*

You should be able to prove this yourself, using the definition of congruence and properties of the gcd. If you get stuck it's in the book.

3. Residue Systems

You should think of the integers as the number line - just a bunch of dots lined up, one for each integer. You should think of congruence modulo m as "collapsing" the number line: we treat all the numbers congruent to zero as one point, all those congruent to one as another point, all those congruent to two as another, and so on, all the way up to $m-1$. For when we get to m, it's not there - we already collapsed it into the same point as 0, since $0 \equiv m \mod m$.

$$\begin{array}{cccccccccccc} \ldots & \bullet & \circ & \bullet & \bullet & \circ & \bullet & \bullet & \circ & \bullet & \ldots \\ \ldots & -3 & -2 & -1 & 0 & 1 & 2 & 3 & 4 & 5 & \ldots \end{array}$$

In the diagram above, all the hollow circles are congruent to 1 mod 3 - we identify them all. The collapsed number line mod 3 looks simply like this:

$$\begin{array}{ccc} \bullet & \bullet & \bullet \\ 0 & 1 & 2 \end{array}$$

This is one reason why congruence is great: it reduces the study of integers (an infinite set) to the study of a finite set. Of course, we lose some information when we do so, namely, when working modulo 3 we can't tell 5 apart from 8 or from -4, etc., since they all get collapsed together.

Let's try to make this "collapsing" a bit more rigorous. We mentioned above, under "Properties," that congruence modulo m is an **equivalence relation** on the set $\mathbb{Z}$ of integers. This means it divides up the integers into disjoint subsets, whose union is all of $\mathbb{Z}$. These subsets are called **congruence classes**, or **residue classes** modulo m. For example, working mod 3 as above, there are three congruence classes:

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

Clearly these three are disjoint subsets whose union is all[2] of $\mathbb{Z}$. Now rather than write them out like this every time, it is convenient to just work with a **representative** of each congruence class. Usually we would just use 0,1,2, but in fact we may choose one from each class arbitrarily. The set obtained by picking exactly

[2]If S is any set, a collection of disjoint subsets S whose union is S is called a **partition** of S.

one representative for each congruence class is called a **complete residue system** modulo 3. The same goes for other moduli besides 3. So $\{0, 1, 2\}$ is a complete residue system, and so are $\{8, -6, 10\}$ and $\{n, n+1, n+2\}$, where n could be any integer. Notice that once we have a complete residue system, ifwe take any arbitrary integer, it will be congruent to exactly one of the representatives in the system, because every integer falls into exactly one congruence class.