Math 126 Number Theory

Prof. D. Joyce, Clark University

15 Feb 2006

Due Today. From page 47, exercises 3–8, 10.

Due Friday. From page 54: 1–5, 8, 10; and from page 63: 1, 4–6, 8, 9, 13, 19–21.

First test. Wednesday, Feb. 22.

For next time. Finish reading through section 3.3.

Last meeting. Congruence modulo n and polynomials.

Today. We define $\mathbf{Z}/n\mathbf{Z}$, also denoted $\mathbf{Z}_n$, as the set of residues modulo n and note that it's a ring in general, and a field when n is a prime. We'll note that some elements of $\mathbf{Z}_n$ do have square roots, and some don't. And we begin the study of linear congruences.

The natural numbers, the integers, the rational numbers, the real numbers, and the complex numbers. There are standard notations for these various kinds of numbers.

A *natural number* is a positive integer, although sometimes it's more convenient to include 0. The set of all natural numbers is usually denoted $\mathbf{N}$. We saw how $\mathbf{N}$ can be defined axiomatically using the Dedekind/Peano axioms. The operations of addition and multiplication are defined on $\mathbf{N}$, but subtraction and division are only partially defined operations, since $a - b$ is only defined if $a > b$, and a/b is only defined when $b|a$.

The *integers*, denoted $\mathbf{Z}$ includes the natural numbers as well as zero and negative integers. The operations of addition, subtraction, and multiplication are defined on $\mathbf{Z}$, but division is still only a partial operation.

Any set equipped with the three operations of addition, subtraction, and multiplication that satisfy certain axioms is called a *ring*. The axioms are the statements that the three operations act as you expect they should. Such axioms require that addition and multiplication be commutative and associative, that multiplication distributes over addition, that 0 acts as a neutral element for addition and 1 acts as a neutral element for multiplication, and that negation is inverse to addition. We won't dwell on these axioms.

Since $\mathbf{Z}$ has these three operations and they have the usual properties, that makes $\mathbf{Z}$ into a ring. But since subtraction is not defined for all pairs of natural numbers, $\mathbf{N}$ is not a ring. Another ring we've seen is the set of polynomials. Since you can add, subtract, and multiply polynomials, and those three operations have the usual properties for polynomials, therefore the set of all polynomials is a ring.

A rational number is the quotient of two integers a/b where the denominator is not 0. The set of all rational numbers is denoted $\mathbf{Q}$. Besides the three operations of addition, subtraction, and multiplication, $\mathbf{Q}$ also has the fourth operation of division which is a partial operation since division by 0 is not defined, but that's the only exception.

Any set with the four operations of addition, subtraction, multiplication, and division (where division is defined except division by 0) which satisfies certain axioms, namely the axioms for rings and one more that says division is inverse to multiplication, is called a *field*. The rational numbers $\mathbf{Q}$ is a field. Note that every field is automatically a ring.

There are two other fields we'll look use. One

is the field of real numbers $\mathbf{R}$. A real number is any number including all positive numbers, 0, and negative. Not just the rational numbers are real, but so are irrational numbers.

Finally, we'll have use for the complex numbers $\mathbf{C}$. A complex number is a number of the form $a+ib$ where a and b are real numbers and $i^2 = -1$. We'll review complex numbers before we use them.

The integers modulo n. If we think of two integers a and b as being the same if $a \equiv b \pmod{n}$, then there are only n integers modulo n. One way of doing that is to represent integers modulo n by a complete residue system, and, as usual, we'll take that complete residue system to be the integers from 0 through $n-1$. Thus, we'll say, for instance, that 5 plus 3 equals 1 modulo 7, by which we mean $5+3 \equiv 1 \pmod{7}$. Thus, we can turn congruence modulo n, which is an equivalence relation on $\mathbf{Z}$ into equality on an n-element set. That n-element set is denoted $\mathbf{Z}/n\mathbf{Z}$, read $\mathbf{Z}$ mod $n\mathbf{Z}$, or more simply as $\mathbf{Z}_n$, read $\mathbf{Z}$ sub n. We can take the elements of $\mathbf{Z}_n$ to be the integers from 0 through $n-1$, where we understand that addition, subtraction, and multiplication are done modulo n.

Since we have those three operations, $\mathbf{Z}_n$ is a ring.

Last time we proved the theorem which said that if $(a,n) = 1$, then cancellation by a works modulo n. More precisely, if $(a,n) = 1$ and $ab \equiv ac \pmod{n}$, then $b \equiv c \pmod{n}$. Now if n happens to be a prime p, then $(a,p) = 1$ means the same thing as $a \not\equiv 0 \pmod{p}$. Thus, cancellation except by 0 works modulo a prime p.

When we looked at the multiplication table modulo $p = 7$ last time, we saw that every one of the 7 elements in $\mathbf{Z}_7$ occurred exactly once in each row and column, except the 0 row and 0 column which were all 0s. That every element c occurs in a row a means that there is exactly one b such that $ab = c$. In other words, $c/a = b$. Thus, $\mathbf{Z}_7$ has an operation of division that's inverse to multiplication, so $\mathbf{Z}_7$ is a field. Likewise, $\mathbf{Z}_p$ will be a field for any prime p.

What we've just done is solve the linear congruence

$$ax \equiv b \bmod 7$$

which leads into our next major topic. Before we go to the linear case, let's look at a quadratic congruence first.

Squares modulo n. In the multiplication table modulo 7, if you look down the diagonal, you're looking at squares. Thus, modulo 7,

a	0	1	2	3	4	5	6
a^2	0	1	4	2	2	4	1

First, what pattern do you see? And why is it there?

Second, note that some numbers are squares and some are not. For instance, 3 is not a square modulo 7. Thus, the quadratic congruence $x^2 \equiv 3 \bmod 7$ has no solution. But some quadratic congruences have two solutions, such as $x^2 \equiv 2 \bmod 7$, the solutions being $x = \pm 3$, and one, namely $x^2 \equiv 0 \bmod 7$ has one solution.

The question of what numbers are squares modulo n is one that's well studied. One that is a square is called a *quadratic residue*. Unfortunately, we won't have time in this course to study the theory of quadratic residues.

Linear congruences. The easiest sort of congruence equation to solve is a linear congruence, one of the form

$$ax \equiv b \pmod{n}.$$

It's easy because we've really already solved it. Suppose we have a solution x. Since $ax \equiv b \pmod{n}$, therefore $n|ax-b$, so there is some number y such that $ny = ax - b$, in other words,

$$ax - ny = b.$$

That's just a linear equation in two unknowns, and we know how to find all it's solutions. Namely, let $d = (a,n)$. If $d \not| b$, then there are no solutions. Otherwise the Euclidean algorithm gives us one solution, and then we can find the rest.

Let's record this as a theorem, and supply the details in a proof.

Theorem. The congruence

$$ax \equiv b \pmod{n}$$

has a solution if and only if $d|b$ where $d = (a, n)$. When $d|b$, then the solution is unique modulo n/d. Thus, if $(a, n) = 1$, the congruence $ax \equiv b \pmod{n}$ always has a unique solution.

Proof: As mentioned just above, the congruence $ax \equiv b \pmod{n}$ has a solution if and only if the equation $ax - ny = b$ has a solution. More precisely, if (x, y) is a solution to the equation, then x is a solution to the congruence. (Thus, a solution to the congruence is part of a solution to the equation.) The equation has a solution if and only if $d|b$, therefore the congruence has a solution if and only if $d|b$.

Let's suppose now that $d|b$. We've seen that every solution to the equation $ax - ny = b$ is of the form

$$x = x_0 + t(n/d), \quad y = y_0 + t(n/d)$$

where (x_0, y_0) is a particular solution (which we can find with the help of the Euclidean algorithm), and t is any integer. Therefore, every solution to the congruence $ax \equiv b \pmod{n}$ is of the form

$$x = x_0 + t(n/d).$$

But

$$x_0 + t(n/d) \equiv x_0 \pmod{n/d},$$

so the congruence has a unique solution modulo n/d. Q.E.D.