Math 217
Winter 2015
Monday, January 12

Most of what we did in class today, plus a little bit more, is covered in Section 1.6 of the textbook. In these notes, I will expand a little on the terminology associated with congruence, and prove the fact the textbook simply refers to as "known," that

> $gcd(b, c)$, the greatest common divisor of the positive integers b and c, can be represented in the form $bx - cy$.

First, some notation and terminology:

$$a \equiv b \mod c$$

is read "a is congruent to b modulo c," or "a is congruent to b mod c." We use this notation only if c is positive.

The number c is called the *modulus*[1] and the relation $(a \equiv b \mod c)$ is called *congruence with respect to* the modulus c.

Two ways to think about the relation of congruence with respect to c:

1. $a \equiv b \mod c$ means that a and b have the same remainder if you divide them by c;
2. $a \equiv b \mod c$ means that the difference $a - b$ is a multiple of c; that is, we can write $(a - b) = cx$.

The second way may be less misleading if a or b is negative. The second way is also useful in proofs, since it's phrased as an equation that we can work with.

Some examples:

$$5 \equiv 9 \mod 4$$

$$-1 \equiv 3 \mod 4$$

In general, for any integers a, b, and d,

$$4a + d \equiv 4b + d \mod 4.$$

The *congruence class* modulo c of a number a consists of all the numbers that are congruent to a modulo c;

$$[a] = \{x \mid x \equiv a \mod c\}.$$

For example, the congruence class [1] modulo 4 consists of all numbers of the form $4y + 1$. Two numbers have the same congruence class iff they are congruent.

We have c-many congruence classes, one for each remainder. So, mod 4, our four congruence classes are

$$[0], [1], [2], [3],$$

[1] The plural of modulus is *moduli*.

and every integer is in exactly one congruence class:

$$-1 \in [3];\ 5 \in [1];\ 9 \in [1].$$

In this case, we have chosen the numbers 0, 1, 2 and 3 as *representatives* of the congruence classes. We chose, for each congruence class, the smallest natural number in that class.

A different choice that is sometimes useful is to choose, for each congruence class, the number with smallest absolute value (taking the positive one if there are two to choose from). In other words, instead of choosing representatives from the interval $[0, c)$, we choose representatives from the interval

$$\left(-\frac{c}{2}, \frac{c}{2}\right].$$

For $c = 4$, our representatives are -1, 0, 1, and 2:

$$[0] = [0], [1] = [1], [2] = [2], [3] = [-1], .$$

A little more notation: Two positive numbers x and y are called *relatively prime* or *coprime* if they have no prime factors in common; in other words, if their greatest common divisor is 1:

$$gcd(x, y) = 1.$$

It is useful to think of this in terms of prime factorization: If we write a and b as products of primes, their greatest common divisor is the product of the primes that occur as factors of both a and b. For example,

$$24 = 2 \cdot 2 \cdot 2 \cdot 3\ ;\ 36 = 2 \cdot 2 \cdot 3 \cdot 3;$$

$$24 = (2 \cdot 2 \cdot 3) \cdot 2\ ;\ 36 = (2 \cdot 2 \cdot 3) \cdot 3;$$

$$gcd(24, 36) = 2 \cdot 2 \cdot 3 = 12.$$

If $gcd(a, b) = c$, we can write $a = cx$ and $b = cy$. The prime factors of x are the "leftover" prime factors of a that did not occur in the prime factorization of b, and similarly for y, so x and y have no prime factors in common. That is, $gcd(x, y) = 1$. For example,

$$24 = (2 \cdot 2 \cdot 3) \cdot 2 = gcd(24, 36) \cdot 2\ ;\ 36 = (2 \cdot 2 \cdot 3) \cdot 3 = gcd(24, 36) \cdot 3$$

and $gcd(2, 3) = 1$.

The textbook proves that the greatest common divisor and least common multiple functions are Diophantine using the following proposition:

Proposition: If $gcd(a, b) = c$ then we can write c in the form $c = ax - by$ for some natural numbers x and y.

Proof: First we prove the proposition in the special case $gcd(a, b) = 1$.

In this case, consider the list of numbers

$$0, a, 2a, 3a, \ldots, (b-1)a.$$

We will show that no two of these numbers are congruent mod b.

To do this, suppose that $i \cdot a$ and $j \cdot a$ are two numbers on the list (so $0 \leq i < b$ and $0 \leq j < b$) that are congruent ($i \cdot a \equiv j \cdot a \mod b$). We will show that they are actually the same number, by showing $i = j$.

To do this, since ($i \cdot a \equiv j \cdot a \mod b$), their difference ($i \cdot a - j \cdot a$) is a multiple of b, so we can write

$$(i-j) \cdot a = bz.$$

The prime factors of b must appear as prime factors of $(i-j) \cdot a$; but since a and b have no prime factors in common, they must all appear as prime factors of $(i-j)$, That is, $(i-j)$ is a multiple of b. Since both i and j are less than b, we have $|i-j| < b$, so the only way $(i-j)$ could be a multiple of b is if $(i-j) = 0$. Therefore, $i = j$, which is what we needed to prove.

Now we have shown that no two of

$$0, a, 2a, 3a, \ldots, (b-1)a,$$

are congruent mod b. Since there are b-many of these numbers, there must be one from each congruence class; in particular, one of them must be congruent to 1 modulo b. That is, for some x with $0 \leq x < b$, we have

$$ax \equiv 1 \mod b;$$

so we can write

$$ax - 1 = by;$$

or

$$1 = ax - by;$$

$$gcd(a, b) = ax - by.$$

This proves the proposition for the case $gcd(a, b) = 1$.

Now suppose $gcd(a, b) = c$. As noted above, we can write

$$a = c\overline{a} \ ; \ b = c\overline{b},$$

where $gcd(\overline{a}, \overline{b}) = 1$. Because we have already proved the proposition for this case, we can write

$$1 = \overline{a}x - \overline{b}y.$$

Multiplying through by c, we have

$$c = c\overline{a}x - c\overline{b}y = (c\overline{a})x - (c\overline{b})y = ax - by.$$

This is what we needed to show.