Mathematics 243 – Algebraic Structures
Discussion 2 – Congruences and Congruence Classes
October 23, 2006

Background

Recall that last Friday we showed that for all integers $n > 1$, the *congruence modulo n relation*

$$x \equiv y \bmod n \quad \Leftrightarrow n|(x-y)$$

on $\mathbf{Z}$ satisfies the following properties:

- If we divide n into x and obtain a remainder of r, $0 \leq r < n$, then the equation $x = qn + r$ shows $x - r = qn$, so $x \equiv r \bmod n$. This means that every integer x belongs to (exactly one) of the congruence classes

$$[0], [1], [2], \ldots, [n-1].$$

- (the "substitution laws") If $x \equiv \ell \bmod n$ and $y \equiv m \bmod n$, then

$$x + y \equiv \ell + m \bmod n$$
$$x \cdot y \equiv \ell \cdot m \bmod n$$

Today, we want to use these facts to work with congruences in several additional ways.

Discussion Questions

A) ("warm up") Find all $x \in \mathbf{Z}$ that satisfy the congruence

$$7x + 3 \equiv 23 \bmod 32$$

(Hint: What number y with $0 < y < 31$ satisfies $7y \equiv 1 \bmod 32$?)

B) The substitution laws for congruences imply, for instance that if $n = 3$ and $x \in [1]$ and $y \in [2]$ are any elements, then

$$x + y \equiv 1 + 2 \equiv 0 \bmod 3.$$

Similarly

$$x \cdot y \equiv 1 \cdot 2 \equiv 2 \bmod 3.$$

In fact we can record all possible products and sums in tables for an "addition mod 3" operation ($+_3$) and a "multiplication mod 3" ($\cdot_3$) operation. Those tables look like this:

$+_3$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\cdot_3$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

The question here is: What do the corresponding tables look like for the "addition modulo 7" and "multiplication modulo 7" operations look like? These are two binary operations on the set of congruence classes mod 7:

$$\{[0], [1], [2], [3], [4], [5], [6]\}$$

C) At some point in your "mathematical past", you have probably seen the following "trick" for testing whether an integer is divisible by 3 (or 9): Take the sum of the base 10 digits of the number n, call that sum S, and see whether that sum is divisible by 3 (or 9). Then

$$\begin{aligned} &3|n \Leftrightarrow 3|S \text{ and} \\ &9|n \Leftrightarrow 9|S \end{aligned} \tag{1}$$

For example, if $n = 83843$, then $S = 8 + 3 + 8 + 3 + 4 = 26$. This is divisible by neither 3 nor 9, so n is *not* divisible by either 3 or 9. (In fact it is easy to see that $83843 \equiv 2 \bmod 3$ and $83843 \equiv 8 \bmod 9$. We would need $n \equiv 0 \bmod 3$ to say 3 does divide n, and similarly for 9.) On the other hand if $n = 252$, then $S = 2 + 5 + 2 = 9$, so n is divisible by *both* 3 and 9. The question here is: *Why does this "trick" work*? Give a proof of the equivalences in (1), using the substitution laws and the meaning of the usual base 10 expansion of an integer. For example, when we write $n = 83843$ in base 10, we mean

$$n = 8 \cdot 10^4 + 3 \cdot 10^3 + 8 \cdot 10^2 + 4 \cdot 10^1 + 3 \cdot 10^0.$$

In general, if

$$n = d_k \cdot 10^k + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0 \cdot 10^0$$

where $d_k, \ldots, d_0$ are the base 10 digits of the number, then

$$S = d_k + \cdots + d_2 + d_1 + d_0,$$

and what you need to show is

$$\begin{aligned} &3|n \Leftrightarrow 3|S = d_k + \cdots + d_2 + d_1 + d_0 \text{ and} \\ &9|n \Leftrightarrow 9|S \end{aligned}$$

Assignment

Group writeups due on Friday, October 27.