MATH 2001
MODULAR ARITHMETIC

Due Wednesday, April 20.

Book exercises: Section 11.4: 6, 7.

Proofs: Final draft of Proof 14 and first draft of Proof 15.

Definition. Let a, b, and n be integers. We say that a is *congruent to b modulo n* if $n \mid (a-b)$, and we write $a \equiv b \pmod n$. (TeX: `a \equiv b \pmod n`)

Exercise 1. Prove that *congruence modulo n* is an equivalence relation.

Exercise 2. The *division algorithm* states that if a and n are integers, then there exist unique integers q and r such that $a = qn + r$ and $0 \leq r < n$.

Prove that $a \equiv r \pmod n$.

As a consequence, a and b have the same remainders when divided by n if and only if $a \equiv b \pmod n$. Since there are exactly n remainders when dividing by n (they are: $0, 1, 2, 3, \ldots, n-1$), there are exactly n equivalence classes modulo n: $[0], [1], [2], \ldots, [n-1]$.

Exercise 3. Write out the equivalence classes modulo 4 explicitly.

$[0] = \{ \qquad \}$ $\quad [1] = \{ \qquad \}$

$[2] = \{ \qquad \}$ $\quad [3] = \{ \qquad \}$

Exercise 4. We define the sum of equivalence classes as follows:

$$[a] + [b] = \{x + y : x \in [a], y \in [b]\}.$$

At the moment, there is no reason that the set on the left should be an equivalence class, but it turns out that is it.

Working modulo 3, write out the following sets explicitly.

$[0] + [0] = \{ \qquad\qquad\qquad\qquad \}$ $[0] + [1] = \{ \qquad\qquad\qquad\qquad \}$

$[1] + [1] = \{ \qquad\qquad\qquad\qquad \}$ $[1] + [2] = \{ \qquad\qquad\qquad\qquad \}$

Exercise 5. Write out the addition table for the integers modulo 4 and modulo 5. (Put the appropriate class in each box.)

+	[0]	[1]	[2]	[3]
[0]				
[1]				
[2]				
[3]				

+	[0]	[1]	[2]	[3]	[4]
[0]					
[1]					
[2]					
[3]					
[4]					

Give a conjecture: $[a] + [b] = [\qquad\qquad\qquad]$ (what class?) Can you prove your conjecture?

Exercise 6. We can do the same for multiplication. In this case, we will simply define $[a] \cdot [b] = [a \cdot b]$. Fill out the multiplication tables for 4 and 5.

$\cdot$	[0]	[1]	[2]	[3]
[0]				
[1]				
[2]				
[3]				

$\cdot$	[0]	[1]	[2]	[3]	[4]
[0]					
[1]					
[2]					
[3]					
[4]					

Exercise 7. We all know that $x^2 = 1$ has two solutions in $\mathbb{R}$ (they are $x = 1$ and $x = -1$). How many solutions are there to $x^2 \equiv 1 \pmod{n}$ when $n = 4$? $n = 5$? $n = 8$? $n = 16$? $n = 24$?