Math 330-01: Intro to Higher Math, Fall 2009
Term Project
Due Friday, December 11

Main reference: Our textbook, Section 6.2. (You might also find Section 6.3 helpful but it is not necessary.)

I would like you to do as many as you can of the problems and proofs. *I do not expect you to answer every question.* Also, quality is more important than quantity. Answering every question, but badly, will get a bad grade. My advice is: Think about your work! Check it carefully. For instance, make sure you don't make unwarranted assumptions.

You may always use the preceding results in your proofs, even if you didn't solve them. Some of the problems are straight from Section 6.2, but others are not.

Remember that you should work on this alone. This is your very own project! But at any time you may e-mail me with questions, and I will be as available for discussions as I can be in the time remaining.

The Project: Arithmetic Modulo n

Fix a natural number $n \geq 2$. On the set $\mathbb{Z}$ define a relation $\equiv$ by declaring $a \equiv b$ if and only if n divides $b - a$ (also written $n | b - a$); make sure you know the definition.

(Names: The relation $\equiv$ is called *congruence.* n is called the *modulus* of the relation. If $a \equiv b$, we say a and b are *congruent.* Note: This "congruence" has nothing to do with geometry!)

Problem 1. *Prove that $\equiv$ is an equivalence relation. (Remark: This is part of proposition 6.19). How many equivalence classes are there? Describe all the equivalence classes in the simplest way possible.*

Define $\mathbb{Z}_n$ to be the set of all equivalence classes of $\equiv$, that is, the set of all $[a]$ for $a \in \mathbb{Z}$. We call $\mathbb{Z}_n$ *the integers modulo n* and we call calculations done in $\mathbb{Z}_n$ *modular arithmetic*, or to be more specific, *arithmetic modulo n.*

Problem 2. *The equivalence class named $[0]$ has other names. List three alternative names for it. How are those names related?*

Here is a definition of operations on $\mathbb{Z}_n$, which are called "addition", written $\oplus$, and "multiplication", written $\odot$. For any $a, b \in \mathbb{Z}$ define $[a] \oplus [b] = [a + b]$ and $[a] \odot [b] = [a \cdot b]$. Here $+$ and $\cdot$ denote addition and multiplication in $\mathbb{Z}$, as usual. We need to prove these operations are "well defined". That means they don't depend on which integers a, b we use to label the equivalence classes $[a], [b]$. Proving that is the next problem.

Problem 3. *Prove that if $[a_1] = [a_2]$ and $[b_1] = [b_2]$, then $[a_1 + b_1] = [a_2 + b_2]$ and $[a_1 \cdot b_1] = [a_2 \cdot b_2]$.*

This means for any $a, b \in \mathbb{Z}$, there is only one equivalence class $[a] \oplus [b]$ and there is only one equivalence class $[a] \odot [b]$. That is, changing the names of the equivalence classes (without changing the classes) does not alter the result of the "addition" and "multiplication" operations. That's what we mean by saying $\oplus$ and $\odot$ are "well defined".

The following properties hold for all $[a], [b], [c] \in \mathbb{Z}_n$:

(i) $([a] \oplus [b]) \oplus [c] = [a] \oplus ([b] \oplus [c])$ (associative law);

(ii) $[a] \oplus [b] = [b] \oplus [a]$ (commutative law);

(iii) $([a] \odot [b]) \odot [c] = [a] \odot ([b] \odot [c])$ (associative law);

(iv) $[a] \odot [b] = [b] \odot [a]$ (commutative law);

(v) $[c] \odot ([a] \oplus [b]) = ([c] \odot [a]) \oplus ([c] \odot [b])$ (left distributive law);

(vi) there exists $\mathbf{0}_n \in \mathbb{Z}_n$ such that for all $[a] \in \mathbb{Z}_n$, $[a] \oplus \mathbf{0}_n = [a]$;

(vii) for every $[a] \in \mathbb{Z}_n$ there exists $-[a] \in \mathbb{Z}_n$ such that $[a] \oplus (-[a]) = \mathbf{0}_n$;

(viii) there exists $\mathbf{1}_n \in \mathbb{Z}_n - \{\mathbf{0}_n\}$ such that for all $[a] \in \mathbb{Z}_n$, $[a] \odot \mathbf{1}_n = [a]$.

Problem 4. *Prove properties* (i), (vi), (vii), (viii) *(notice that in particular you need to explicitly define* $\mathbf{0}_n, -[a], \mathbf{1}_n$*). Prove also at least one of the remaining properties. (Remark: This is part of proposition 6.21.)*

You should notice that all the properties (i)–(viii) above hold true in $\mathbb{Z}$ and $\mathbb{R}$. But there are two major properties missing from our list:

(ix) if $[c] \odot [a] = [c] \odot [b]$ and $[c] \neq \mathbf{0}_n$, and if $[c] \neq \mathbf{0}_n$, then $[a] = [b]$;

(x) for every $[a] \in \mathbb{Z}_n - \{\mathbf{0}_n\}$ there exists $[a]^{-1} \in \mathbb{Z}_n$ such that $[a] \odot [a]^{-1} = \mathbf{1}_n$.

The first is an axiom in $\mathbb{Z}$ and a proposition in $\mathbb{R}$. The second one is an axiom in $\mathbb{R}$ but doesn't hold true in $\mathbb{Z}$.

Problem 5. *Find a value of n for which property* (ix) *succeeds, and a value for which it fails. The same for property* (x). *Justify your answers, of course. (Hint: Try very small values of n.)*

Now that you've tried a couple of values of n, let's prove the general theorems. Remember the definition of a prime number (you will find this in Section 6.3): A *prime number* is a natural number $m > 1$ that is divisible only by 1, -1, m, and $-m$. A *composite number* is a natural number $m > 1$ that is not prime.

It is a fact that $\mathbb{Z}_n$ satisfies properties (ix) and (x) if and only if n is prime; but we can't prove that right away. First we need lemmas and a proposition.

Lemma 6. *If p and q are distinct primes, then p does not divide q and q does not divide p.*

Lemma 7. *Let $m \in \mathbb{Z}$ and $m > 1$. If m is not prime then there exist $x, y \in \mathbb{N}$ such that $1 < x < m$, $1 < y < m$, and $m = xy$.*

Proposition 8. *Every integer greater than* 1 *is either a prime or a product of primes.*

Hint: Use induction and lemma 7.

Now we can start to find out when $\mathbb{Z}_n$ satisfies property (ix) or (x).

Problem 9. *Prove that, if n is composite, then $\mathbb{Z}_n$ does not satisfy either* (ix) *or* (x).

Hint: Use lemma 7, and think about what that tells us about some of the equivalence classes that are elements of $\mathbb{Z}_n$.

Theorem 10. $\mathbb{Z}_n$ *satisfies property* (ix) *if and only if n is a prime number.*

Hint: Use lemmas 7 and 6 and (of course) problem 9.

Theorem 11. $\mathbb{Z}_n$ *satisfies property* (x) *if and only if n is a prime number.*