Math 109 Spring 2006 HW 7

HW Due Friday 5/26/06 in class

Exercise and page numbers refer to Fletcher and Patty, 3rd edition. Check them against a friend’s book if you have another edition. Working with a classmate is fine, but the final writeup should be your own work.

Part 0

These are suggested exercises for extra practice if you feel you need it. Do not hand these exercises in.

FP, Chapter 4, #67, 68, 72, 82, 84
FP, Chapter 5, #1, 7

Part 1

Turn these exercises in.
FP, Chapter 4, #80, 81, 83
FP, Chapter 5, #6, 9, 17

Part 2

These are more challenging and/or longer exercises.

1. Let $p$ be an odd prime number. We say that $a \in \mathbb{Z}$ is a square modulo $p$ if there exists some $b \in \mathbb{Z}$ such that $b^2 \equiv a \mod p$. Prove that among the numbers $\{0, 1, 2, \ldots, p - 1\}$, exactly $(p + 1)/2$ are squares modulo $p$. 
2. The “First year calculus student’s dream” is the tempting formula 

\[(x + y)^n = x^n + y^n,\]

which is, of course, false in general (otherwise we would not need the binomial theorem.) However, there is a variant of the calculus student’s dream which is correct. Prove that if \(p\) is a prime number and \(a, b \in \mathbb{Z},\) then \((a + b)^p \equiv a^p + b^p \mod p.

3. In this problem, you will explore injective and surjective are related for functions from a finite set to itself (these observations are useful to remember.)

(a). Prove that if \(S\) is a set with finitely many elements and \(f : S \to S\) is an injective function, then \(f\) is actually bijective. Give an example which shows that the same result does not hold in general for infinite sets \(S.\)

(b). Prove that if \(S\) is a set with finitely many elements and \(f : S \to S\) is an surjective function, then \(f\) is actually bijective. Give an example which shows that this result does not hold in general for infinite sets \(S.\)

4. A function \(f : \mathbb{R} \to \mathbb{R}\) is called \(\textit{increasing}\) if \(f(a) \leq f(b)\) whenever \(a < b,\) and \(\textit{strictly increasing}\) if \(f(a) < f(b)\) whenever \(a < b.\)

(a). Show by example that an increasing function \(f : \mathbb{R} \to \mathbb{R}\) is not necessarily injective.

(b). Show that a strictly increasing function \(f\) is injective. Give an example of a strictly increasing function which is not surjective.

(c). By part (b), if \(f\) is a strictly increasing function which is also surjective, then \(f\) is bijective. In this case, show that \(f^{-1} : \mathbb{R} \to \mathbb{R}\) is also strictly increasing.

5. Let \(A, B, C\) be sets. Let \(f : A \to B, g : B \to C,\) and \(h : A \to B\) be functions.

(a). Prove that if \(g \circ f\) is injective, then \(f\) is injective. Show by example that \(g \circ f\) being injective does not force \(g\) to be injective.

(b). Prove that if \(f\) and \(g\) are both injective, then \(g \circ f\) is injective.

(c). Prove that if \(g\) is injective and \(g \circ f = g \circ h,\) then \(f = h.\)