CS205 - Functions and Modular Arithmetic

Chetan Tonde

October 23, 2011

1 Topics

1. Functions - domain, range, image, preimage, one-one, onto, into, inverse, left inverse, right inverse, composition, increasing, decreasing, bounded, unbounded
2. Modular Arithmetic - congruences, if $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $a + c \equiv b + d(mod\ m)$ and $ac \equiv bd(mod\ m)$, FTA, Infinity of primes, PNT.

2 Warm up

If $f(x) = x - 1$ and $g(x) = x^2 - 1$. Find formulas for fog and gof. Try to graph them and classify whether they are increasing, decreasing, bounded, etc.

3 Problem 1

Prove/Disprove that,

1. The compositions of two injections is an injection.
2. The compositions of two surjections is an surjection.
3. The compositions of two bijections is an bijection.
4. If $f : A \to B$ and $g : B \to C$ are bijections $(fog)^{-1} = f^{-1}og^{-1}$.

4 Problem 2

Suppose $f : A \to B$, $g : B \to C$ and $h : gof$. For each statement below, give a proof or a counter example.

1. If h is injective, then f is injective.
2. If h is injective, then g is injective.
3. If h is surjective, then f is surjective.
4. If h is surjective, then f is surjective.

5 Warm up

Solve the congruence $2x \equiv 7(mod\ 17)$.

6 Problem 3

Prove, If $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$ then $a + c \equiv b + d(mod\ m)$ and $ac \equiv bd(mod\ m)$

7 Problem 4

Prove, There are infinity of primes.
Hint: Assume the opposite and generate a new prime.

8 Problem 5

Prove, The Fundamental Theorem of Arithmetic, i.e. Every integer has a unique prime factorization.
Hint: Prove existence by decomposition and uniqueness by contradiction.