Math 1C03 Introduction to Mathematical Reasoning
Term 2 Winter 2014–2015
Study guide for final exam

Definitions You should be able to state all of the following definitions precisely. Know an example of a situation for which the definition is true and one for which it is false. Know how to prove that something satisfies the definition.

- prime, relatively prime, divisible
- gcd
- congruent modulo n
- rational number (fraction of two integers, not as congruence class), irrational number
- domain, codomain, range
- injective surjective, bijective
- cardinality, countably infinite
- complex numbers: modulus, argument, cartesian form, polar form

Techniques You should be able to use the following techniques.

- division algorithm
- euclidean algorithm (both to find gcd and to solve the equation $ax + by = \gcd(a, b)$
- modular arithmetic
- induction, strong induction
- binomial theorem
- convert from fraction to periodic decimal and back again
- construction of function to show a set is countably infinite
- convert complex numbers from cartesian to polar form and back
- solve simple polynomial equations over $\mathbb{C}$
- describe sets in $\mathbb{C}$ geometrically
- RSA

Theorems You should be able to state, prove and use the following theorems (the numbers refer to the location in the textbook).

- 2.28 If $c|ab$ and $\gcd(a, c) = 1$ then $c|b$.
- 2.52 There exist infinitely many primes
- 3.42 Fermat's Little Theorem: If $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$ (you don't have to be able to prove this)
- 4.11 Inductive property of the positive integers (you don't have to be able to prove this)
- 5.21 $\sqrt{2}$ is irrational
- 6.67 $\mathbb{Z}$ is countably infinite
- 8.61 DeMoivre's theorem