Math 252 - Midterm 1 Review Sheet

The final exam will be 3 hours long. During the exam, you will be required to complete 4 or 5 proofs. You will also need to answer several short answer questions similar to the problems from the midterms.

1. Be ready to prove each of the following claims (and any similar claims too!). Some of these will be on the final.
   (a) Prove: If $d|a$ and $d|b$, then $d|(a+b)$.
   (b) Prove: If $a \equiv b \pmod{n}$, then for all $k \in \mathbb{N}$, $a^k \equiv b^k \pmod{n}$.
   (c) Prove: For $a, b \in \mathbb{N}$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = 1$ iff $(a, b) = 1$.
   (d) Prove: $\sqrt{3}$ is irrational.
   (e) Prove: There are infinitely many prime numbers.
   (f) Prove: For fixed $a, b, n \in \mathbb{Z}$ with $n > 0$, the congruence $ax \equiv b \pmod{n}$ has integer solutions iff $(a, n)|b$.
   (g) Prove: Let $m, n \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $(a, n) = 1$. If $a^m \equiv 1 \pmod{n}$, then $\text{ord}_n(a)|m$.
   (h) Prove: The sum of the first n odd integers is n^2.
   (i) Prove: Let $a, n \in \mathbb{Z}$ with $n > 1$. If $(a, n) = 1$, then **there exists a unique** $b \in \mathbb{Z}_n$ such that $ab \equiv 1 \pmod{n}$.

2. In general, the most important theorems and axioms tend to get names. You should know the following.
   (a) The Principle of Mathematical Induction.

   (b) The Division Algorithm.

   (c) The Euclidean Algorithm.

   (d) The Fundamental Theorem of Arithmetic.

   (e) The Little Theorem of Fermat.

   (f) Euler's Theorem

   (g) The Cancellation Law (for modular arithmetic).

3. Without looking anything up, define as many of the following terms as you can:
   (a) Divisible by d.

   (b) Congruent modulo n.

   (c) Greatest common divisor.

   (d) Prime number.

   (e) Order of a modulo n.

   (f) Complete Residue System.

   (g) Canonical Complete Residue System.

   (h) The Euler ϕ-function.

4. For the logical statement "If the ball is red, then it is not a baseball."
   (a) What is the converse of the statement above?

   (b) What is the contrapositive of the statement above?

5. You should be able to solve problems like the following (without a calculator!).
   (a) Find $(63, 45)$.

   (b) Use Euclid's algorithm to find $(121, 55)$.

   (c) Find all integer solutions to $17x + 12y = 1$.

   (d) Find $\text{ord}_{16}(5)$.

   (e) What is the multiplicative inverse of 5 in $\mathbb{Z}_{16}$?

   (f) Find $x \in \mathbb{Z}_{16}$ such that $5x \equiv 7 \pmod{16}$.

   (g) Find all solutions to $3x \equiv 4 \pmod 7$.

   (h) Let $x \in \mathbb{N}$. If $x \equiv 4 \pmod 7$ and $x \equiv 2 \pmod 6$, then what is the smallest possible value of x?

   (i) Find 234^{222} mod 23.

   (j) Find the last digit of 17^{34}.

   (k) Find $\phi(990)$.

6. You should know what each of the following mathematical symbols/shorthand means.
   (a) iff
   (b) $\forall$
   (c) $\exists$
   (d) $\mathbb{Z}$
   (e) $\mathbb{N}$
   (f) $\mathbb{Z}_n$.

7. Know the different proof techniques.
   (a) Suppose that I wanted to use a proof by contradiction to prove: "If n is even, then n^2 is even." What would be a good first sentence for that proof?

   (b) How do you prove an if and only if statement?