Math 321 Review for Exam #1

General Review the numerical problems from old homework assignments, and be sure you know how to do them. You should also review any proofs that do not (re)appear on this sheet. This review sheet is intended to provide a sample of the types of proofs you can expect to see on the exam. induction.

You will also be responsible for knowing proofs of the three “big theorems” covered in class:

- the infinitude of the primes,
- the fundamental theorem of arithmetic, and
- the irrationality of $\sqrt{2}$.

At least one of those proofs is guaranteed to appear on the exam.

Rigor Proofs Note: No salvages are necessary. These statements are all true. You may use the axioms for $\mathbb{Z}$ and definitions. You may use previous problems as lemmas (whether or not you have solved that problem), but if you use any other facts, you should prove them. In other words, show and justify every step of your proof.

1. For every integer $m$, $m \mid m$.

2. For all integers $a, b$ and $c$, if $a \mid b$ and $b \mid c$ then $a \mid c$.

3. Let $a, b, c \in \mathbb{Z}$. If $a \mid b$ and $a \mid c$ then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.

4. For all $m \in \mathbb{Z}$, $m \mid 0$.

5. For all $a \in \mathbb{Z}$, $-1 \cdot a = -a$.

6. For all $a, b \in \mathbb{Z}$, $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$.

7. Multiplication distributes over subtraction. That is, $a(b - c) = ab - ac$.

8. $1 \in \mathbb{N}$.

9. $\mathbb{Z}$ has no zero divisors.

10. If $ac = bc$ and $c \neq 0$, then $a = b$ for all integers $a, b, c$.

11. If $a \neq 0$ then $a^2 > 0$.

12. If $a > b$ and $c > 0$ then $ac > bc$.

13. If $a > b$ and $c < 0$ then $ac < bc$. 
Other Proofs Note: No salvages are necessary. These statements are all true. You may use the axioms for $\mathbb{Z}$ and definitions. You may may also use any lemma from the homework or from class, as long as you clearly state the fact you are using. (But stating that the problem itself was proved in class or the homework is not sufficient.)

14. If $a, b \in \mathbb{N}$ and $a \mid b$ then $a \leq b$.

15. For $a, b \in \mathbb{N}$, there exist integers $q$ and $r$ such that
   \[ a = bq + r \quad \text{and} \quad 0 \leq r < b. \]

16. For positive integers $a$ and $b$, $\gcd(a, b) = 1$ if and only if there exist integers $x$ and $y$ such that $ax + by = 1$.

17. The only units in $\mathbb{Z}[i]$ are $\pm 1$ and $\pm i$.

18. Let $p$ be a prime in $\mathbb{Z}$. If $p \mid ab$ for integers $a$ and $b$, then $p \mid a$ or $p \mid b$.

19. $\pi$ is a prime in $\mathbb{Z}[i]$ if and only if
   - $N(\pi)$ is a prime in $\mathbb{Z}$, or
   - $\pi$ is an associate of a prime $p \in \mathbb{Z}$ such that $p \equiv 3 \pmod{4}$.
   (We say that $a$ is an associate of $b$ if $a = bu$ for $u$ a unit.)

20. Let $u \in U_m$. Then $u^{\phi(m)} \equiv 1 \pmod{m}$. 