Math 300.2 **Review questions for Exam 2** **November 15, 2007**

The exam covers the material from Problem Sets 4–8 and involves the content from the end of Section 1.1 through the beginning of Section 2.4 (probably ending with Proposition 2.4.11—to be determined later).

Define the following:

- The **addition** operation for natural numbers (recursive definition).
- The **factorial function**.
- The sequence of **Fibonacci numbers**.
- **Summation** $\sum_{j=1}^{n} a_j$ of natural numbers (recursive definition).
- A real number is **rational**.
- A **least** element of a subset of $\mathbb{Z}$; a **greatest** element of a subset of $\mathbb{Z}$.
- A **lower bound** of a subset of $\mathbb{Z}$ in $\mathbb{Z}$; an **upper bound** of a subset of $\mathbb{Z}$ in $\mathbb{Z}$; a subset of $\mathbb{Z}$ is **bounded below** in $\mathbb{Z}$; a subset of $\mathbb{Z}$ is **bounded above** in $\mathbb{Z}$.
- The **binomial coefficient** $\binom{n}{k}$.
- For a positive integer n and an integer m, the integers $m \bmod n$ and $m \operatorname{div} n$.
- For a positive integer d and an integer n, the statement d **divides** n.
- Integers m and n not both 0 are **relatively prime** to one another.
- $gcd(m, n)$ for integers m and n not both 0.
- An **ideal** in $\mathbb{Z}$.
- A **prime number**.
- A set is **finite**; a set is **infinite**.
- For integers $m > 1$ and a and b, the statement $a \equiv b \pmod{n}$.

State:

- The Well-Ordering Principle.
- The Principle of Strong Induction.
- The Binomial Theorem.
- The "Division Theorem" (the one about $m = q\,n + r$).
- The Principal Ideal Theorem for $\mathbb{Z}$.
- Euclid's Divisor Theorem [about expressing $\gcd(m, n)$].
- The Fundamental Theorem of Arithmetic.
- Euclid's Theorem about the number of primes.
- The Congruence Cancelation Law.

Do the following calculations—supply your own values for m and n:

- A binomial coefficient $\binom{m}{n}$.
- By using the Euclidean algorithm, $\gcd(m, n)$ and the representation of this gcd as an "integral linear combination" $m\,s + n\,t$ of m and n.
- The prime power representation of an integer n.

Prove:

1. $m + 1 = 1 + m$ for all natural numbers m. Use the recursive definition for addition; you may also use the associative law for addition without proving it.
2. The Addition Formula $\binom{n+1}{j} = \binom{n}{j-1} + \binom{n}{j}$ for binomial coefficients.
3. If b is an integer with $b > 1$, then for every natural number a there is some natural number m for which $b^m > a$.
4. If d divides integers a and b, then d divides $a\,s + b\,t$ for all integers s and t.
5. An integer n is odd if and only if $n = 2\,k + 1$ for some integer k.
6. If integer m is odd, then m^2 is odd.
7. A nonempty subset A of $\mathbb{N}$ that has an upper bound in $\mathbb{N}$ has a greatest element.
8. If m and n are integers that are not both 0, then $m/\gcd(m, n)$ is relatively prime to $n/\gcd(m, n)$.
9. The number $\sqrt{2}$ is irrational.
10. If J is an ideal in $\mathbb{Z}$ and if $m, n \in J$, then $m - n \in J$. (Do this *without* using the Principal Ideal Theorem.)
11. The Principal Ideal Theorem. (*Hint:* Let J be an ideal in $\mathbb{Z}$ and suppose $J \neq \{0\}$. Show that $J = \{\,k\,g : k \in \mathbb{Z}\,\}$ for a suitable g.)
12. Euclid's Divisor Theorem. (*Hint:* The proof involves showing that $\{\,m\,s + n\,t : m, n \in \mathbb{Z}\,\} = \{\,k\,g : k \in \mathbb{Z}\,\}$.)
13. Let a and b be integers that are not both 0 and let d be a positive integer. If d is relatively prime to a and if $d \mid a\,b$, then $d \mid b$.
14. If a and b are relatively prime positive integers and if both a and b divide integer n, then $a\,b$ divides n, too.
15. Each integer greater than 1 has a prime divisor.
16. If p is prime and if p divides the product $m\,n$ of integers m and n, then p divides m or p divides n.
17. If prime p divides the product $\prod_{j=1}^{n} q_j$ of primes $q_1, q_2, \ldots q_j$, then $p = q_j$ for some j.
18. Each integer greater than 1 is a product of one or more primes.
19. There are infinitely many primes.

20. The transitive property for congruence modulo m.

21. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a\,c \equiv b\,d \pmod{m}$.

Prove or disprove:

1. If m^2 is divisible by 3, then m is divisible by 3.

   If J is a subset of $\mathbb{Z}$ for which $0 \in J$ and for which $m + n \in J$ whenever $m \in J$ and $n \in J$, then J is an ideal in $\mathbb{Z}$.

2. If positive integer d divides the product $m\,n$ of two integers m and n, then it divides at least one of them.

3. If integers m and n both divide integer b, then their product $m\,n$ divides b.

4. If p_1, p_2, p_3 are primes, then $p_1\,p_2\,p_3 + 1$ is prime.

5. If $a + c \equiv b + d \pmod{m}$, then $a \equiv b \pmod{m}$.

Give an example of:

- A nonempty subset of $\mathbb{Z}$ that does not have a greatest element.
- An infinite subset of $\mathbb{Z}$ that is *not* an ideal in $\mathbb{Z}$.
- Integers a and b for which $a \neq b$ but $a \equiv b \pmod{10}$.