**Math 299** **Midterm 2 Review** **Nov 1, 2013**

Exam topics

1. Methods of proof
   (a) Direct proof
   (b) Proof of the contrapositive
   (c) Proof by contradiction
   (d) Proof by cases
   (e) Proof by induction
      - Might involve proof by working backward

2. Divisibility of integers
   (a) Definition of divisibility
   (b) Properties of divisibility
   (c) Division Lemma
   (d) Definition of prime and composite numbers
   (e) Definition of *greatest common divisor*
   (f) Definition of coprime numbers
   (g) Definition of **mod**

3. Axioms of Group
   You should be able to give a formal definition of
   (a) closure
   (b) associativity
   (c) identity element
   (d) inverse element

You should know and be able to apply the following theorems.

1. Fundamental Theorem of Arithmetic
2. Every integer greater than or equal to 2 is divisible by at least one prime.
3. If $n$ is composite integer, then it has a factor less than or equal to $\sqrt{n}$.
4. The Euclidean Algorithm
5. Let $g = \gcd(a, b)$. Then $\exists x, y \in \mathbb{Z}$ such that $ax + by = g$.
6. **Euclid's Lemma** Suppose $n, a, b \in \mathbb{N} \setminus \{0\}$. If $n \mid ab$ and $\gcd(a, n) = 1$, then $n \mid b$.

## Practice Problems

1. Prove that for any two sets $A$ and $B$, $(A \cup B)^c = A^c \cap B^c$.

2. Prove that if $n|a$ then $n|a+b \Leftrightarrow n|b$

3. Use Euclid's lemma to prove that if $gcd(m,n) = 1$ and $m|a$ and $n|a$ then the product $m \cdot n$ divides $a$.

4. Prove that if $a, b$ are relatively prime, then $\forall c \in \mathbb{Z}$, $\exists x, y \in \mathbb{Z}$ such that $ax+by = c$.

5. Prove that $gcd(a+3b, b) \leq gcd(a, b+7a)$ for all $a, b \in \mathbb{Z}$ by using the definitions of divisibility and GCD only.

6. Use *proof by induction* to show that $5^{2k} - 1$ is divisible by 4 for all $k \in \mathbb{N}$.

7. Let $n \in \mathbb{N}$. Use induction to show that exactly one element of the set $\{n, n+1, n+2, n+3\}$ is divisible by 4.

8. Let $x \in \mathbb{N} = \{1, 2, 3, ...\}$.

   (a) Prove that $x^2 + x$ is even.

   (b) Prove that $(x^2 + x)/2$ is divisible by $x$ if and only if $x$ is odd.

   (c) Prove that $(x^2 + x)/2$ is divisible by $x + 1$ if and only if $x$ is even.

9. (Houston 26.7 (iii)) Show that if $x^2 - 3x + 2 < 0$, then $1 < x < 2$.

10. (Houston 27.23 (v)) Prove that every common divisor of $a, b \in \mathbb{Z}$ is a divisor of $\gcd(a, b)$.

11. Let $a, b, c \in \mathbb{Z}$. Prove that if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

12. Recall that the Fibonacci numbers are defined by $F_1 = 1, F_2 = 1$, and

$$F_{n+1} = F_{n-1} + F_n, \qquad n \geq 2.$$

   (a) Prove that for all $n \in \mathbb{N}$, $\sum_{i=1}^{n} F_i = F_{n+2} - 1$.

   (b) Prove that every natural number can be written as the sum of distinct Fibonacci numbers. (This is a harder problem. Hint: use strong induction).

13. Let $a, b, c, d \in \mathbb{Z}$ with $a$ and $b$ nonzero. Prove that if $ab \nmid cd$, then $a \nmid c$ or $b \nmid d$.

14. Let $x$ be an irrational real number. Prove that either $x^2$ or $x^3$ is irrational.

## Solutions

1. Prove that for any two sets $A$ and $B$, $(A \cup B)^c = A^c \cap B^c$.

   **Proof:** We need to prove $(A \cup B)^c \subseteq A^c \cap B^c$ and $A^c \cap B^c \subseteq (A \cup B)^c$. In order to prove $(A \cup B)^c \subseteq A^c \cap B^c$, let x be an arbitrary element in $(A \cup B)^c$. Then $x \notin A \cup B$, i.e., $x \notin A$ and $x \notin B$, which implies $x \in A^c$ and $x \in B^c$. This is equivalent to $x \in A^c \cap B^c$. Thus we proved that every element of $(A \cup B)^c$ is also an element of $A^c \cap B^c$ , in other words $(A \cup B)^c \subseteq A^c \cap B^c$ (*).

   Now, in order to prove $A^c \cap B^c \subseteq (A \cup B)^c$, let x be an arbitrary element in $A^c \cap B^c$. That is, $x \in A^c$ and $x \in B^c$, which is equivalent to $x \notin A$ and $x \notin B$. This implies that $x \notin A \cup B$, which in its turn is equivalent to $x \in (A \cup B)^c$. Thus we proved that every element of $A^c \cap B^c$ is also an element of $(A \cup B)^c$ , in other words $A^c \cap B^c \subseteq (A \cup B)^c$ (**).

   Combining (*) and (**) we conclude that $(A \cup B)^c = A^c \cap B^c$.

2. Prove that if $n|a$ then $n|a + b \Leftrightarrow n|b$

   **Proof:** The above statement is biconditional, so we need to prove both directions.

   First, we are going to prove "If $n|a$ and $n|a+b$ then $n|b$". Since $n|a$, then $\exists k \in \mathbb{Z}$ such that $a = kn$. Also, since $n|a + b$, then $\exists m \in \mathbb{Z}$ such that $a + b = mn$. Combining the two equations, we can express $b$ as $b = n(m - k)$. Note that $(m - k) \in \mathbb{Z}$, and thus $n|b$.

   Next, we need to prove "If $n|a$ and $n|b$ then $n|a + b$". In a similar way as above, $n|a$, implies $\exists k \in \mathbb{Z}$ such that $a = kn$. Also, since $n|b$, then $\exists s \in \mathbb{Z}$ such that $b = sn$. Combining the two equations, we can express $a + b$ as $a + b = n(k + s)$. Note that $(k + s) \in \mathbb{Z}$, and thus $n|a + b$.

3. Use Euclid's lemma to prove that if $gcd(m, n) = 1$ and $m|a$ and $n|a$ then the product $m \cdot n$ divides $a$.

   **Proof:** Note that $m|a$ implies $\exists k \in \mathbb{Z}$ such that $a = km$, similarly $n|a$ implies $\exists s \in \mathbb{Z}$ such that $a = sn$ (*). Thus, $km = sn$, which means that $m|sn$. Since, by assumption, $\gcd(m, n) = 1$, by Euclid's lemma we have that $m|s$, i.e., $s = cm$ for some $c \in \mathbb{Z}$. Substituting this into (*) one arrives at $a = cmn$, i.e., $mn|a$.

4. Prove that if $a, b$ are relatively prime, then $\forall c \in \mathbb{Z}$, $\exists x, y \in \mathbb{Z}$ such that $ax+by = c$ (*).

   **Proof:** Since $a, b$ are relatively prime, $\gcd(a, b) = 1$, which implies that $\exists m, n \in \mathbb{Z}$ such that $am + bn = 1$. Let $c$ be an arbitrary integer. Multiply the previous equation by $c$, to arrive at $amc + bnc = c$. Define $x = mc$ and $y = nc$ and note that $x, y \in \mathbb{Z}$. Also $x$ and $y$ are solutions to (*).

5. Prove that $gcd(a + 3b, b) \leq gcd(a, b + 7a)$ for all $a, b \in \mathbb{Z}$ by using the definitions of divisibility and GCD only.

   **Proof:** Let $g = gcd(a + 3b, b)$. Then $g|(a + 3b)$ and $g|b$, i.e., $\exists k, m \in \mathbb{Z}$ such that $a + 3b = gk$ and $b = gm$. Therefore $a = g(k - 3m)$ and $b + 7a = g(7k - 20m)$.

Since $7k - 20m$ and $k - 3m$ are integers, this implies that $g$ is a common divisor of $a$ and $b + 7a$. Therefore it is no larger than the greatest common divisor of these two integers, i.e., $g \leq gcd(a, b + 7a)$.

6. Use *proof by induction* to show that $5^{2k} - 1$ is divisible by 4 for all $k \in \mathbb{N}$.

   **Proof:** The statement is true for the base case $k = 0$, as $4|0$. Assume that the statement holds true for some integer $s$, i.e., $4|(5^{2s} - 1)$. We need to prove that the statement holds true for $n = s + 1$, i.e. $4|(5^{2(s+1)} - 1)$. Note that $5^{2(s+1)} - 1 = 25 \cdot 5^{2s} - 1$ (*). By the inductive hypothesis, there exists an integer $m$ such that $5^{2s} - 1 = 4m$. Substituting this into (*) one arrives at $5^{2(s+1)} - 1 = 25 \cdot (4m + 1) - 1$, which is equivalent to $5^{2(s+1)} - 1 = 4 \cdot (25m + 6)$, and thus $5^{2(s+1)} - 1$ is divisible by 4. Therefore the statement holds true for any integer $k$, by induction.

7. Let $n \in \mathbb{N}$. Use induction to show that exactly one element of the set $\{n, n+1, n+2, n+3\}$ is divisible by 4.

   **Proof:** First note that there is *at most* one element which is divisible by 4, since otherwise an element of the set $\{1, 2, 3\}$ would be divisible by 4.

   Now we use induction to prove that *at least* one element of $\{n, n+1, n+2, n+3\}$ is divisible by 4. The base case is obvious. For the inductive step, assume there is some

   $$x \in \{k, k+1, k+2, k+3\}$$

   that is divisible by 4. We want to show that some element in $\{k+1, k+2, k+3, k+4\}$ is divisible by 4. If $x = k+1, k+2$ or $k+3$, then we are done. If $x = k$, then $k+4$ is divisible by 4, and we are done.

8. Let $x \in \mathbb{N} = \{1, 2, 3, ...\}$.

   (a) Prove that $x^2 + x$ is even.

   **Proof:** If $x = 2k$ is even, then $x^2 + x = 4k^2 + 2k = 2k(2k + 1)$ is even. If $x = 2k + 1$ is odd, then $x^2 + x = 4k^2 + 6k + 2 = 2(2k^2 + 3k + 1)$ is even.

   (b) Prove that $(x^2 + x)/2$ is divisible by $x$ if and only if $x$ is odd.

   **Proof 1:** If $x = 2k+1$ is odd, then $(x^2 + x)/2 = 2k^2 + 3k + 1 = (2k+1)(k+1)$, which is obviously divisible by $x = 2k + 1$.

   For the converse use contradiction. Assume $(x^2 + x)/2$ is divisible by $x$, and $x = 2k$ is even. Then $(x^2 + x)/2 = k(2k + 1)$. Since this is divisible by $x = 2k$, we must have that $k(2k + 1)/2k = (2k + 1)/2$ is an integer. This is impossible since the numerator $2k + 1$ is odd.

   **Proof 2:** Write $(x^2 + x)/2 = x(x + 1)/2$. First suppose $x$ is odd. We want to show that $x(x + 1)/(2x) = (x + 1)/2$ is an integer. This is immediate since the numerator $x + 1$ is even.

Conversely, suppose $x$ divides $(x^2+x)/2$. This implies that $(x+1)/2$ is an integer, and hence $x+1$ is even. It follows that $x$ is odd.

(c) Prove that $(x^2+x)/2$ is divisible by $x+1$ if and only if $x$ is even.

*Proof:* This is similar to Part (b).

9. (Houston 26.7 (iii)) Show that if $x^2-3x+2<0$, then $1<x<2$.

   **Proof:** Write $x^2-3x+2=(x-1)(x-2)$. If this is negative, then we are in one of two cases:

   Case 1: $x-1>0$ and $x-2<0$, or

   Case 2: $x-1<0$ and $x-2>0$.

   The first case is equivalent to $x>1$ and $x<2$, which is impossible. The second case is equivalent to $1<x<2$, as desired.

10. (Houston 27.23 (v)) Prove that every common divisor of $a,b\in\mathbb{Z}$ is a divisor of $\gcd(a,b)$.

    **Proof:** Suppose $c$ divides $a$ and $b$. By Theorem 28.7 we can write

    $$ma+nb=\gcd(a,b)$$

    for some integers $m,n\in\mathbb{Z}$. Since $c$ divides $a$ and $b$, it also divides $ma+nb$, by Theorem 27.5. It follows that $c$ divides $\gcd(a,b)$.

11. Let $a,b,c\in\mathbb{Z}$. Prove that if $\gcd(a,b)=1$ and $\gcd(a,c)=1$, then $\gcd(a,bc)=1$.

    **Proof 1:** Direct proof from previous results. Assume $\gcd(a,b)=\gcd(a,c)=1$. By the Euclidean Algorithm, we can write $ma+nb=1$ and $qa+rc=1$, so that:

    $$\begin{aligned}(1)(1) &= (ma+nb)(qa+rc)\\ &= (ma)(qa)+(nb)(qa)+(ma)(rc)+(nb)(rc)\\ &= (maq+nbq+mrc)a+(nr)(bc).\end{aligned}$$

    That is, $ka+\ell(bc)=1$ for $k,\ell\in\mathbb{Z}$, so Proposition 1(a) above gives $\gcd(a,bc)=1$.
    **Proof 2:** Contrapositive. Assume the contrapositive hypothesis: $d=\gcd(a,bc)>1$. Then $d$ has a prime factor $p|d$, with $p|a$ and $p|bc$. By the Prime Lemma, this means $p|b$, so that $\gcd(a,b)\geq p>1$; or $p|c$, so that $\gcd(a,c)\geq p>1$. In either case, $\gcd(a,b)>1$ or $\gcd(a,c)>1$, which is the contrapositive conclusion.

12. Recall that the Fibonacci numbers are defined by $F_1=1, F_2=1$, and

    $$F_{n+1}=F_{n-1}+F_n, \qquad n\geq 2.$$

Prove that for all $n \in \mathbb{N}$, $\sum_{i=1}^{n} F_i = F_{n+2} - 1$.

**Proof:** Induction. Let $A(n)$ be the formula for a given $n \geq 1$.

Base: $F_1 = 1 = 2 - 1 = F_3 - 1$, so $A(1)$ is true.

Chain. Assume $A(n)$: $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$ for some $n \geq 1$. Then:

$$\begin{aligned} F_1 + F_2 + \cdots + F_n + F_{n+1} &= (F_{n+2} - 1) + F_{n+1} && \text{by inductive hypothesis} \\ &= F_{n+2} + F_{n+1} - 1 = F_{n+3} - 1 && \text{by recurrence for } F_{n+3} \end{aligned}$$

which gives the inductive conclusion $A(n{+}1)$.

13. Let $a, b, c, d \in \mathbb{Z}$ with $a$ and $b$ nonzero. Prove that if $ab \nmid cd$, then $a \nmid c$ or $b \nmid d$.

    **Proof.** Contrapositive. Assume the contrapositive hypothesis $a|c$ and $b|d$. Then $c = na$ and $d = mb$, so that $cd = nmab$. This gives the contrapositive conclusion $ab \mid cd$.

14. Let $x$ be an irrational real number. Prove that either $x^2$ or $x^3$ is irrational.

    **Proof.** Contrapositive. Assume the contrapositive hypothesis $x^2$ and $x^3$ are rational, and $x \neq 0$. (The case $x = 0$ is obvious.) The the quotient of two rational numbers is rational, so $x = x^2/x^3$ is rational, which is the contrapositive hypothesis.