MATHEMATICS 300–FALL 2011
INTRODUCTION TO MATHEMATICAL REASONING
INSTRUCTOR: H. J. Sussmann
SOLUTIONS TO THE PROBLEMS OF THE FIRST MIDTERM EXAM.

0. State the Well Ordering Principle.
   ANSWER: Every nonempty set of natural numbers has a smallest member.

1. Prove that if $a, b$ are arbitrary real numbers, then $ab \leq \frac{a^2 + b^2}{2}$.
   PROOF:
   We want to prove that $(\forall a, b \in \mathbb{R}) ab \leq \frac{a^2 + b^2}{2}$.
   Let $a, b$ be arbitrary real numbers. We will prove that $ab \leq \frac{a^2 + b^2}{2}$.
   We will do a proof by contradiction.
   Assume $\sim ab \leq \frac{a^2 + b^2}{2}$.
   Then $ab > \frac{a^2 + b^2}{2}$.
   Therefore $2ab > a^2 + b^2$.
   Hence $0 > a^2 + b^2 - 2ab$.
   It follows that $0 > (a - b)^2$, because $a^2 + b^2 - 2ab = (a - b)^2$.
   So $0 \leq (a - b)^2$.
   But $0 \leq (a - b)^2$, because the square of every real number is nonnegative.
   Therefore $0 \leq (a - b)^2 \Leftrightarrow 0 \geq (a - b)^2$, which is a contradiction.
   Hence $ab \leq \frac{a^2 + b^2}{2}$.
   So $(\forall a, b \in \mathbb{R}) ab \leq \frac{a^2 + b^2}{2}$.

2. (i) Give a precise mathematical definition of the predicate “divides” (or “is a factor of”), or—after changing the order of the arguments—“is divisible by”, or “is a multiple of”.
   ANSWER: Let $a, b$ be integers. We say that $a$ divides $b$ if there exists an integer $k$ such that $b = ak$.
   (ii) Prove the following statement: If $n$ is any odd integer, then $n^3 - n$ is divisible by 8.
   PROOF:
   Let $n$ be an arbitrary integer.
   Assume $n$ is odd.
   Then $n^3 - n = n(n^2 - 1) = n(n - 1)(n + 1)$.
   The integers $n - 1$ and $n + 1$ are both even, because $n$ is odd.
   Furthermore, one of these two integers is divisible by 4.
   So $(n - 1)(n + 1)$ is divisible by 8.
   Therefore $n(n - 1)(n + 1)$ is divisible by 8, so $n^3 - n$ is divisible by 8.
3. The division theorem says that if $a, b$ are integers and $b \neq 0$, then there exist unique integers $q, r$ such that $a = bq + r$ and $0 \leq r < |b|$. Prove the uniqueness part of the statement.

**Proof:**
To prove uniqueness, we have to show that if $q_1, r_1, q_2, r_2$ are integers such that $a = bq_1 + r_1$, $0 \leq r_1 < |b|$, $a = bq_2 + r_2$, and $0 \leq r_2 < |b|$, then $q_1 = q_2$ and $r_1 = r_2$.

Let $q_1, r_1, q_2, r_2$ be arbitrary integers.
Assume that $a = bq_1 + r_1$, $0 \leq r_1 < |b|$, $a = bq_2 + r_2$ and $0 \leq r_2 < |b|$.
Assume that $r_1 \leq r_2$.
Then $bq_1 + r_1 = bq_2 + r_2$.
So $r_2 - r_1 = b(q_1 - q_2)$.
Since $r_1 \leq r_2$, we have $r_2 - r_1 \geq 0$.
Since $r_1 \geq 0$ and $r_2 < |b|$, we have $r_2 - r_1 < |b|$.
So $0 \leq r_2 - r_1 < |b|$.
Since $r_2 - r_1 = b(q_1 - q_2)$, we have

$$r_2 - r_1 = |r_2 - r_1| = |b||q_1 - q_2|.$$ 

If $q_1 \neq q_2$ then $|q_1 - q_2| \geq 1$ (because $q_1$ and $q_2$ are integers), so $r_2 - r_1 \geq |b|$, contradicting the fact that $r_2 - r_1 < |b|$.

Hence $q_1 = q_2$, and then $r_1 = r_2$.
So we have proved that if $r_1 \leq r_2$, then $q_1 = q_2 \land r_1 = r_2$.
The same argument works if $r_1 \geq r_2$.

So we have proved that $q_1 = q_2 \land r_1 = r_2$.

4. i. Give a precise mathematical definition of “absolute value”.

**Answer:** Let $x$ be a real number. The absolute value of $x$ is the real number $|x|$ given by $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$.

ii. Prove that if $x$ is any real number then if $|x - 2| > 4$ it follows that $|x| > 2$.

**Proof:**

We want to prove that $(\forall x \in \mathbb{R})(|x - 2| > 4 \iff |x| > 2)$.
Let $x$ be an arbitrary real number. We want to prove that $|x - 2| > 4 \iff |x| > 2$.

Assume that $|x - 2| > 4$. We want to prove that $|x| > 2$.
We consider two cases, namely, $x - 2 \geq 0$ and $x - 2 < 0$,

**First Case:** Assume that $x - 2 \geq 0$.
Then $|x - 2| = x - 2$.
Since $|x - 2| > 4$, we have $x - 2 > 4$, so $x > 6$, and then $|x| > 6$, so $|x| > 2$.

**Second Case:** Assume that $x - 2 < 0$.
Then $|x - 2| = -(x - 2) = 2 - x$.
Since $|x - 2| > 4$, we have $2 - x > 4$, so $x < -2$, and then $|x| = -x$, while on the other hand $-x > 2$, so $|x| > 2$.

So we have proved that $|x| > 2$ in both cases. Hence $|x| > 2$.
Therefore $|x - 2| > 4 \implies |x| > 2$. 

2
5. i. Give a precise mathematical definitions of “rational number” and “irrational number.”

ANSWER: Let $x$ be a real number. We say that $x$ is rational (or that $x$ is a rational number), if there exist integers $m, n$ such that $n \neq 0$ and $x = \frac{m}{n}$. We say that $x$ is irrational if it is not rational.

ii. Prove that $\sqrt{2}$ is irrational.

PROOF:

We do a proof by contradiction.

Assume $\sqrt{2}$ is rational.

Then there exist integers $m, n$ such that $n \neq 0$ and $\sqrt{2} = \frac{m}{n}$.

Pick such integers $m, n$.

We may assume that $m$ and $n$ are both positive (because $m$ and $n$ must have the same sign, since $\frac{m}{n} > 0$, and if they are both negative me may replace them by $-m$ and $-n$).

We may also assume that $m$ and $n$ are not both divisible by 3 (because if they are divisible by 3 we may replace them by $\frac{m}{3}$ and $\frac{n}{3}$, and if the resulting numbers are divisible by 3 again then we may divide them by 3 again, and continue this procedure until it stops; the procedure will have to stop at some point because of the Well Ordering Principle, and when it stops we get two positive integers that are not both divisible by 3).

From the fact that $\sqrt{2} = \frac{m}{n}$, we conclude that $2n = \frac{m^2}{n^2}$.

Therefore $21n^2 = m^2$.

Hence $m^2$ is divisible by 3.

So $m$ is divisible by 3 (because if a prime divides a product $ab$ of integers $a, b$ then it must divide one of the factors, and 3 is prime).

So we may pick an integer $k$ such that $m = 3k$.

So $21n^2 = 9k^2$ and then $7n^2 = 3k^2$.

Hence $7n^2$ is divisible by 3.

Since 3 does not divide 7, it must divide $n^2$.

Therefore 3 divides $n$.

So we have shown that both $m$ and $n$ are divisible by 3.

But this contradicts the fact that $m$ and $n$ are not both divisible by 3.

So we have reached a contradiction, proving that $\sqrt{2}$ is irrational.

6. i. Give a precise mathematical definition of “prime number”.

ANSWER: A prime number is an integer $p$ such that $p > 1$, having the property that whenever $j, k$ are positive integers for which $jk = p$ it follows that $j = 1 \vee k = 1$.

ii. Prove that there exists a prime number $p$ such that

$$p > 10,000,000,000,000,000,000,000,000,000,000,000,000$$

PROOF:

Let $N = 10,000,000,000,000,000,000,000,000,000,000,000,000$.

We want to prove that there exists a prime number $p$ such that $p > N$.

Let $M = N! + 1$. (Here $N!$ is the factorial of $N$, i.e., the product $\prod_{k=1}^{N} k$ of all the natural numbers from 1 to $N$.)

Then $M$ has a prime factor, i.e., (exists $k \in \mathbb{N}$($k$ divides $M \land k$ is prime). (Reason: Every natural number $m$ such that $m > 1$ has a prime factor.)

Pick a prime factor of $M$ and call it $p$.

Then $p$ is prime and $p$ divides $M$.

We will now prove (by contradiction) that $p > N$.

Assume that $p \leq N$.

Since $N!$ is the product of all the natural numbers from 1 to $N$, and $p$ is one of those numbers, it follows that $p$ divides $N!$.

Since $p$ divides $N!$ and $p$ divides $M$, it follows that $p$ divides $M - N!$.

But $M - N! = 1$.
So $p$ divides 1.
Therefore $p \leq 1$, so $\sim p > 1$.
But $p > 1$ because $p$ is prime.
So $p > 1 \sim p > 1$, which is a contradiction.
Therefore $p > N$.

7. The theorem on the greatest common divisor says that “if $a, b$ are integers that are not both zero, and $c$ is the greatest common divisor of $a$ and $b$, then $c$ is a linear combination of $a$ and $b$.” **Complete the following proof of the theorem.**

PROOF: Let $S$ be the set of all positive integers that are linear combinations of $a$ and $b$. Then $S$ is nonempty, because $a^2 + b^2 \in S$. So by the Well-ordering Principle $S$ has a smallest member $c$. We now prove that $c$ is the greatest common divisor of $a$ and $b$.

COMPLETION OF THE PROOF: We have to prove that

(i) $c$ divides $a$ and $b$.
(ii) If $d$ is any integer that divides both $a$ and $b$, then $d \leq c$.

First we use the fact that $c$ is a linear combination of $a$ and $b$ to pick integers $m, n$ such that $c = ma + nb$.

We now prove that $c$ divides $a$.

Using the division theorem, we pick integers $q, r$ such that $a = cq + r$ and $0 \leq r < c$.
Then $a = (ma + nb)q + r$, so $r = (1 - mq)a + (-mq)b$. So $r$ is a linear combination of $a$ and $b$.
If $r > 0$ it would follow that $r \in S$, so $r$ would be a member of $S$ smaller than $c$, contradicting the fact that $c$ is the smallest member of $S$. So $r = 0$.
Then $a = cq$, so $c$ divides $a$.

The proof that $c$ divides $b$ is similar, so we omit it.

Finally, we prove Property (ii) above.

Let $d$ be an integer that divides $a$ and $b$.

Pick integers $u, v$ such that $a = ud$ and $b = vd$.
Then $c = ma + nb = uda + vdb = (ua + vb)d$,
So $d$ divides $c$.

Therefore, $d \leq c$ (because, if $c = kd$, $k \in \mathbb{Z}$, then $c = |c| = |k||d| \geq |d| \geq d$, using the fact that $|k| \geq 1$, which follows because $k \in \mathbb{Z}$ and $k \neq 0$; the fact that $k \neq 0$ is a consequence of the equality $c = kd$ and the inequality $c > 0$).

So we have proved (i) and (ii).