**Math 300.2** **Exam 2 Answers** **November 15, 2007**

1. (a) [5%] For every integer $m$, there exist *unique* integers $q$ and $r$ [2.5%] such that $m = 5q + r$ and $0 \le r < 5$. [2.5%]

   (b) [8%]
   *Proof. Assume* $5 \mid m^2$. *Write* $m = 5q + r$ *with* $q$ *and* $r$ *as in (a). Then*

   $$m^2 = (5\,q + r)^2 = 25\,q^2 + 10\,qr + r^2 = 5(5\,q^2 + 2\,qr) + r^2. \qquad [2\%]$$

   Since 5 divides both $m^2$ and $5(5\,q^2 + 2\,qr)$, it divides their difference $r^2$. [2%] Now $r = 0, 1, 2, 3,$ or 4 so that $r^2$ is one of

   $$0^2 = 0, \quad 1^2 = 1, \quad 2^2 = 4, \quad 3^2 = 9, \quad 4^2 = 16. \qquad [1\%]$$

   But 5 does not divide any of these numbers except 0, so that $r^2 = 0$. [2%] Then $r = 0$, and $m = 5\,q + 0 = 5\,q$. Thus 5 divides $m$. [1%] □

   (c) [7%] *Proof.* Just suppose $\sqrt{5}$ is rational, so that

   $$\sqrt{5} = \frac{m}{n} \qquad (*)$$

   for some integers $m$ and $n$ with $n \neq 0$. [2%]
   Without loss of generality, we may assume that $m$ and $n$ are relatively prime (if they are not, divide each by their gcd). [2%]
   Square (*) to obtain

   $$5\,n^2 = m^2. \qquad [1\%]$$

   Since 5 divides $5\,n^2$, it also divides $m^2$. [1%] From (b), 5 divides $m$. [1%] . . .

2. (a) [10%] *Proof:* Assume $a + c \equiv b + c \pmod{m}$. [1%] Then

   $$m \mid \big((a + c) - (b + c)\big) \qquad [3\%]$$

   and, since $(a + c) - (b + c) = a - b$, [3%]

   $$m \mid (a - b). \qquad [2\%]$$

   This means $a \equiv b \pmod{m}$.[1%] □

   (b) [10%] The implication is **not true** in general. [2%]
   Take, for example, $m = 2$ and take $a = 2, b = 3, c = 4$. [6%] Then $2 \cdot 4 \equiv 3 \cdot 4 \pmod{2}$ and $4 \neq 0$, but $2 \not\equiv 3 \pmod{2}$. [2%]

3. (a) [5%] Integer $n > 1$ is *not* prime when there exists an integer $d$ such that $d \mid n$ but $d \neq 1$ and $d \neq n$.

   (b) [5%] *Well-Ordering Principle:* Each nonempty subset of $\mathbb{N}$ has a least element.

(c) [10%] *Proof:* We are going to use the Well-Ordering Principle. Let

$$A = \{\, n \in \mathbb{Z} : n > 1 \quad \& \quad \underline{n \text{ has } \textbf{\textit{no}} \text{ prime divisor}} \,\}. \qquad [2\%]$$

Just suppose some integer greater than 1 has no prime divisor, in other words, $A$ is nonempty. [1%]

By the Well-Ordering Principle, $A$ has a least element $n_1$. [1%]

Since $n_1$ has no prime divisor, then in particular, $n_1$ itself is not prime. [1%] This means that $n_1$ has a divisor $d$ with $1 < d < n_1$. [2%]

Because $d > 1$ and $d < n_1$, the least element of $A$, then $d \notin A$. This means that $d$ has some prime divisor $p$. Then $p \mid d$ and, since $d \mid n_1$, then also $p \mid n_1$. This is impossible because $n_1 \in A$. [3%] □

4. (a) [5%] Define:

$$\begin{cases} a^0 = 1, & & [1\%] \\ a^{n+1} = a\, a^n & (n \geq 0) & [4\%] \end{cases}$$

[*Note:* You could equally well take $a^{n+1} = a^n\, a$ as the recursive relation, and then you would need to alter some of the steps in (b). You could also take as the recursive relation $a^n = a\, a^{n-1}$ for $n \in \mathbb{N}^*$, but in view of the induction done in (b), it's easier to use the $a^{n+1} = \ldots$ form.]

(b) [15%] Fix $n \in \mathbb{N}$. We use induction on $m$ to prove that $a^{m+n} = a^m\, a^n$ for all $n \in \mathbb{N}$.[2%]

*Base step* ($m = 0$): For every $n \in \mathbb{N}$, $a^{0+n} = a^n = 1 \cdot a^n = a^0\, a^n$ [3%]

*Inductive step:* Let $m \in \mathbb{N}$ and assume

$$a^{m+n} = a^m\, a^n \qquad \text{for } \textit{all } n \in \mathbb{N}. \qquad [2\%]$$

(What must be deduced is that $a^{(m+1)+n} = a^{m+1}\, a^n$ for *all* $n \in \mathbb{N}$. [2%])

Let $n \in \mathbb{N}$. Then:

$$\begin{aligned} a^{(m+1)+n} &= a^{m+(n+1)} && \text{(by properties of addition in } \mathbb{Z}) && [1\%] \\ &= a^m\, a^{n+1} && \text{(by the inductive assumption)} && [2\%] \\ &= a^m\, (a\, a^n) && \text{(by the recursive definition)} && [1\%] \\ &= (a\, a^m)\, a^n && \text{(by properties of multiplication in } \mathbb{R}) && [1\%] \\ &= a^{m+1}\, a^n && \text{(by the recursive definition again)} \quad \square && [1\%] \end{aligned}$$

*Notes:*

- The value of $n$ was fixed in the proof above, so that the predicate $P(m)$ being proved by induction is $a^{m+n} = a^m\, a^n$, where $n$ is that fixed value. If you do not fix $n$, then the predicate $P(m)$ to be proved by induction would be that $a^{m+n} = a^m\, a^n$ *for all* $n \in \mathbb{N}$—and you should explicitly say so.
- You could carry out the induction on $n$ instead of on $m$.

5. (a) **[5%]** The set $A$ of all *even* integers is infinite and differenced. (More generally: any nonzero ideal in $\mathbb{Z}$; in other words, for any integer $g \neq 0$, the ideal $\{\, k\, g : k \in \mathbb{Z} \,\}$.)

   (b) **[5%]** The set $A$ of all *odd* integers is infinite, but it is *not* differenced. (Another example: the subset $\mathbb{N}$ of $\mathbb{Z}$.)

   (c) **[10%]** First, since $A$ has some element $k$ and $0 = k - k$, then

$$0 \in A. \qquad \textbf{[3\%]} \tag{1}$$

[*Note:* The preceding needs to be a separate step. It is *not* enough to start something like this: "Let $m, n \in A$. Then $0 = m - m \in A$." The trouble with that is that you don't have any particular element of $A$ yet; you explicitly have to invoke that $A$ is nonempty to get such.]

Next, for each $n \in A$, its negative

$$-n = 0 - n \in A \qquad \textbf{[3\%]} \tag{2}$$

from (**??**) and the definition of "differenced".

Finally, for every $m, n \in A$, the sum

$$m + n = m - (-n) \in A \qquad \textbf{[4\%]}$$

from (**??**) and the definition of "differenced)". □

*Another version of the proof: fix $m$ and $n$ at the start.* Let $m, n \in A$. Since $m \in A$, from the definition of "differenced" we have $0 = m - m \in A$. Next, since $0 \in A$ and $n \in A$, then $-n = 0 - n \in A$. Finally, since $m \in A$ and $-n \in A$,

$$m + n = m - (-n) \in A.$$

*Yet another version of the proof.* This arrangement of the proof does not explicitly involve showing that $0 \in A$. (Thanks, Colette!) Let $m, n \in A$. Then $m - n \in A$ since $A$ is differenced. Next,

$$-n = (m - n) - m \in A,$$

again since $A$ is differenced. Finally, as above,

$$m + n = m - (-n) \in A,$$

once more because $A$ is differenced. □