Math 521A Exam 1 Solutions

Oct 7, 2009

1. (10 pts) Show that any nonempty set of integers that is closed under subtraction must also be closed under addition.

   Let S be such a set. Since S is nonempty, there is an element $x \in S$. Since S is closed under subtraction, $0 = x - x \in S$.

   Let $x, y \in S$. We need to show $x + y \in S$. First notice that $-y = 0 - y \in S$ by closure under subtraction. For the same reason, $x + y = x - (-y) \in S$.

2. (10 pts) Let $a, b \in \mathbb{Z}^*$. Show that $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z}$.

   To simplify notation, let $m = [a, b]$.

   We will first show $a\mathbb{Z} \cap b\mathbb{Z} \subseteq m\mathbb{Z}$. Since $a\mathbb{Z}$ and $b\mathbb{Z}$ are the sets of multiples of a and b respectively, $a\mathbb{Z} \cap b\mathbb{Z}$ is the set of common multiples of a and b. So any $x \in a\mathbb{Z} \cap b\mathbb{Z}$ is a multiple of both a and b. Therefore $m|x$, and hence $x \in m\mathbb{Z}$. So $a\mathbb{Z} \cap b\mathbb{Z} \subseteq m\mathbb{Z}$.

   Now, we will show $m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$. Let $x \in m\mathbb{Z}$. Then $m|x$. But $a, b|m$, so $a, b|x$. Therefore x is a common multiple of a and b and hence $x \in a\mathbb{Z} \cap b\mathbb{Z}$. This shows $m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$. We can now conclude $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.

3. (10 pts) Solve the following system of congruences.

   $$2x \equiv 5 \mod 7, \qquad 3x \equiv 4 \mod 8.$$

   (Hint: First reduce to the usual form.)

   Since 4 is a multiplicative inverse of 2 modulo 7 and 3 is a multiplicative inverse of 3 modulo 8, multiply the first congruence by 4 and the second by 3:

   $$2x \equiv 5 \mod 7 \implies 4(2x) \equiv 4 \cdot 5 \mod 7 \implies x \equiv 6 \mod 7$$

   $$3x \equiv 4 \mod 8 \implies 3(3x) \equiv 3 \cdot 4 \mod 8 \implies x \equiv 4 \mod 8$$

   From this last congruence, $x = 8n + 4$ for some $n \in \mathbb{Z}$. Hence

   $$8n + 4 \equiv 6 \mod 7 \implies n \equiv 6 - 4 \mod 7 \implies n \equiv 2 \mod 7$$

   This means $n = 7m + 2$ for some $m \in \mathbb{Z}$. Hence $x = 8(7m + 2) + 4 = 20 + 56m$. Or $x \equiv 20 \mod 56$.

   Let's check the solution.

   $$x \equiv 20 + 56m \equiv 20 \equiv 6 \mod 7 \implies 2x \equiv 12 \mod 7 \implies 2x \equiv 5 \mod 7 \quad \surd$$

   $$x \equiv 20 + 56m \equiv 20 \equiv 4 \mod 8 \implies 3x \equiv 12 \mod 8 \implies 3x \equiv 4 \mod 8 \quad \surd$$

4. (a) (3 pts) State the Well-Ordering Principle.

   Any nonempty subset of the natural numbers (or the positive integers) contains a minimal element.

   (b) (12 pts) State and prove the Division Algorithm.

   See Theorem 1.1.3 and its proof in the textbook.

5. Let $n \in \mathbb{Z}^+$.

(a) (5 pts) Define what a zero divisor is in $\mathbb{Z}_n$. Give an example of an element in some $\mathbb{Z}_n$ that is a zero divisor and an element that is not a zero divisor.

An element $[a] \in \mathbb{Z}_n$ is a zero divisor if there is another element $[b] \neq [0]$ such that $[a][b] = [0]$.

(b) (10 pts) Prove that an element in $\mathbb{Z}_n$ has a multiplicative inverse if and only if it is not a zero divisor.

You can give the two-step proof of Proposition 1.4.5 in the textbook. Alternately, here is a more direct proof.
Suppose $[a]$ has a multiplicative inverse $[a]^{-1}$. Then

$$[a][b] = [0] \implies [a]^{-1}([a][b]) = [a]^{-1}[0] \implies ([a]^{-1}[a])[b] = [0] \implies [b] = [0].$$

That is the only element $[b] \in \mathbb{Z}_n$ such that $[a][b] = [0]$ is $[0]$ itself. This shows $[a]$ cannot be a zero divisor.
Now, suppose $[a]$ has is not a zero divisor. Then none of $[a][1], [a][2], \ldots, [a][n-1]$ are $[0]$. If one of them is $[1]$, then $[a]$ has a multiplicative inverse, and we are done. If none of them are $[1]$ (or $[0]$), then two elements on this list must be equal by the Pigeon Hole Principle. This is because other than $[0]$ and $[1]$, $\mathbb{Z}_n$ has only $n-2$ elements left, and the list has $n-1$ elements. So there exist $[b] \neq [c]$ such that $[a][b] = [a][c]$. Hence $[a]([b] - [c]) = [0]$. Since $[b] \neq [c]$, $[b] - [c] \neq [0]$. But this contradicts that $[a]$ is not a zero divisor.

6. (10 pts) **Extra credit problem.** An element $[a]$ of $\mathbb{Z}_n$ is said to be *nilpotent* if $[a]^k = [0]$ for some k. Show that $\mathbb{Z}_n$ has no nonzero nilpotent elements if and only if n has no factor that is a square (except 1).

We will prove that $\mathbb{Z}_n$ has a nonzero nilpotent element if and only if n has a factor $m^2 \neq 1$.

First suppose that n has a square factor m^2. Then $n = m^2 l$ for some $l \in \mathbb{Z}$. Let $a = ml$. Notice that $n \nmid a$, but $n | a^2 = m^2 l^2$. Hence $[a] \neq [0]$, but $[a]^2 = [0]$.

Conversely, let $[a] \neq [0]$ be an element in $\mathbb{Z}_n$ such that $[a]^k = [0]$. Hence $n \nmid a$ and $n | a^k$. Let $d = (n, a)$ and $n = dm$ and $a = db$ where $m, b \in \mathbb{Z}$. We know that $(m, b) = 1$ (this was homework exercise 1.2.8). Note

$$n | a^k \implies dm | (db)^k = d^k b^k \implies m | d^{k-1} b^k.$$

By Prop 1.2.3d, $(m, b) = 1$ implies $(m, b^k) = 1$. Hence $m | d^{k-1}$ by Prop 1.2.3b. Since $m^2 \neq 1 \implies m \neq 1$, there exists a prime divisor p of m. Now

$$p | m \text{ and } m | d^k \implies p | d^k \implies p | d$$

by Exercise 1.1.7 and Prop 1.2.3d (if $p \nmid d$ then $(p, d) = 1$ hence $(p, d^k) = 1$). Now combine $p | m$ and $p | d$ to conclude $p^2 | dm = n$. Hence n has a factor that is a square.