Math 521A Exam 1 Solutions

Oct 5, 2011

1. (5 pts) Let a, b, c be integers. Show that if $b|a$ and $b \nmid c$ then $b \nmid (a + c)$.

   Let $b|a$. We will prove the contrapositive: if $b|(a + c)$ then $b|c$. Since $b|a$ and $b|(a + c)$, there exist $m, n \in \mathbb{Z}$ such that $a = mb$ and $a + c = nb$. Hence

   $$c = (c + a) - a = nb - mb = (n - m)b.$$

   Since $m, n \in \mathbb{Z}$, $n - m \in \mathbb{Z}$. So $b|c$.

2. (10 pts) Perhaps a more natural definition of the greatest common divisor is the following:

   Definition 1. Let a and b be integers, not both 0. An integer d is called the *greatest common divisor* of a and b if
   (a) $d|a$ and $d|b$,
   (b) $c|a$ and $c|b$ implies $d \geq c$.

   Show that this definition is equivalent to

   Definition 1.1.5. Let a and b be integers, not both 0. An integer $d > 0$ is called the *greatest common divisor* of a and b if
   (a) $d|a$ and $d|b$,
   (b) $c|a$ and $c|b$ implies $c|d$.

   Suppose d_1 satisfies Definition 1 and d_2 satisfies Definition 1.1.5. We will prove that $d_1 = d_2$.

   First, observe that $d_1 > 0$ because $1|a$ and $1|b$ implies $1 \leq d_1$. Since $d_1|a$ and $d_1|b$, by Definition 1.1.5(b), $d_1|d_2$. Hence $d_2 = nd_1$ for some $n \in \mathbb{Z}$. Since d_1 and d_2 are both positive, so is n. Also, since $d_2|a$ and $d_2|b$, by Definition 1(b), $d_2 \leq d_1$. So

   $$d_1 \leq nd_1 = d_2 \leq d_1.$$

   Hence the $\leq$'s are equalities, and $d_1 = d_2$.

3. (10 pts) Prove that there exist infinitely many prime numbers of the form $4m + 3$, where $m \in \mathbb{Z}$.

   This can be shown similarly to Euclid's proof of the infinitude of primes. Suppose there are finitely many such primes $p_1, \ldots, p_k$. Let $a = 4p_1 \cdots p_k - 1$. Then $p_i \nmid a$. This is because $p_i|a + 1$ so if $p_i|a$ then $p_i|(a + 1) - a = 1$. Now, a is of the form $4m + 3$. Since $a \neq p_i$ for any i, a cannot be prime. Then a must have some prime factor. Obviously, a is odd. So its only prime factors must be of the form $4m + 1$, that is congruent to 1 modulo 4. But the product of numbers congruent to 1 modulo 4 is also 1 modulo 4. Hence no such product can be equal to a. Now, we have a contradiction.

4. (10 pts) Let $p \in \mathbb{Z}^+$. Prove that p is prime if and only if it satisfies the following property: for all $a, b \in \mathbb{Z}$ if $p|ab$ then either $p|a$ or $p|b$.

   See Lemma 1.2.5 in your textbook.

5. Let $n \in \mathbb{Z}^+$.
   (a) (3 pts) State the definition of a zero divisor in $\mathbb{Z}_n$.

   An element $[a]$ of $\mathbb{Z}_n$ is a zero divisor if $[a][b] = [0]$ for some nonzero congruence class $[b]$ of $\mathbb{Z}_n$.

(b) (2 pts) Choose an $n \in \mathbb{Z}^+$ such that $\mathbb{Z}_n$ has a zero divisor and give an example of a zero divisor in this $\mathbb{Z}_n$. Be sure to justify your example.

In $\mathbb{Z}_4$, $[2][2] = [0]$. Hence $[2]$ is a zero divisor in $\mathbb{Z}_4$.

(c) (10 pts) Let $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. Prove that $[a]$ is a zero divisor in $\mathbb{Z}_n$ if and only if n and a are not relatively prime. Obviously, you are not allowed to use Proposition 1.4.5 or its variant which we gave in class, because they say exactly this.

Suppose that $\gcd(a, n) = d > 1$. Let $b = n/d$. Then $b \in \mathbb{Z}$ and $1 \leq b < n$. So $[b] \neq [0]$. Now

$$ab = a\frac{n}{d} = \frac{a}{d}n.$$

Since $a/d \in \mathbb{Z}$, $n|ab$. Hence $[a][b] = [0]$.
Suppose that $\gcd(a, n) = 1$. Then $1 = sa + tn$ for some $b, c \in \mathbb{Z}$. Hence $[s][a] = [sa] = [1 - tn] = [1]$. If $[a][b] = [0]$, then

$$[0] = [s][0] = [s]([a][b]) = ([s][a])[b] = [b].$$

So $[a]$ cannot be a zero divisor.

6. (10 pts) **Extra credit problem.** Let $n \in \mathbb{Z}^+$.

(a) Prove that if for some $a \in \mathbb{Z}$, the congruence equation $x^2 \equiv a \pmod{n}$ has more than two distinct solutions, then $\mathbb{Z}_n$ contains at least one nonzero equivalence class $[b]$ which does not have a multiplicative inverse.

Let a be such that $x^2 \equiv a \pmod{n}$ has more than two distinct solutions. Let b_1, b_2, b_3 be distinct solutions. Then

$$b_1^2 \equiv a \equiv b_2^2 \pmod{n} \implies (b_1 + b_2)(b_1 - b_2) \equiv b_1^2 - b_2^2 \equiv 0 \pmod{n}.$$

Since b_1 and b_2 are distinct $b_1 - b_2 \not\equiv 0 \pmod{n}$. Now there are two possibilities. If $b_1 + b_2 \not\equiv 0 \pmod{n}$, then $[b_1 + b_2] \neq [0]$ and is a zero divisor. Hence it cannot have a multiplicative inverse (by Proposition 1.4.5(b)) and we are done.
If $b_1 + b_2 \equiv 0 \pmod{n}$, then we consider $b_1 + b_3$. If $b_1 + b + 3 \equiv 0 \pmod{n}$ then

$$b_1 + b_2 \equiv b_1 + b_3 \pmod{n} \implies b_2 \equiv b_3 \pmod{n}.$$

But we know this is not the case. So $b_1 + b_3 \not\equiv 0 \pmod{n}$. But

$$b_1^2 \equiv a \equiv b_3^2 \pmod{n} \implies (b_1 + b_3)(b_1 - b_3) \equiv b_1^2 - b_3^2 \equiv 0 \pmod{n}.$$

Since $b_1 - b_3 \not\equiv 0 \pmod{n}$ either, $[b_1 + b_3] \neq [0]$ is a zero divisor. Hence it cannot have a multiplicative inverse.

(b) Is the converse of the statement in (a) true? If so, prove it. If not, give a counterexample.

The converse is false. $\mathbb{Z}_4$ contains the zero divisor $[2]$ since $[2][2] = [0]$. But no congruence equation of the form $x^2 \equiv a \pmod{n}$ has more than two solutions in $\mathbb{Z}_4$:

$$x^2 \equiv 0 \pmod{4} \text{ has solutions } x = 0 \text{ and } x = 2,$$

$$x^2 \equiv 1 \pmod{4} \text{ has solutions } x = 1 \text{ and } x = 3,$$

$$x^2 \equiv 2 \pmod{4} \text{ has no solutions,}$$

$$x^2 \equiv 3 \pmod{4} \text{ has no solutions.}$$