Selected Solutions to Homework 2

Tim Smits

2.1.22

(a) Give an example to show that the following statement is false: If $ab \equiv ac \bmod n$ and $a \not\equiv 0 \bmod n$, then $b \equiv c \bmod n$.

(b) Prove that the statement is true when $(a, n) = 1$.

Solution:

(a) $2 \cdot 0 \equiv 2 \cdot 2 \bmod 4$, but $2 \not\equiv 0 \bmod 4$.

(b) Suppose $ab \equiv ac \bmod n$. This says $n \mid a(b - c)$. Since $(a, n) = 1$, this means $n \mid (b - c)$, so $b \equiv c \bmod n$.

2.2.14 Solve the following equations:

(a) $x^2 + x = [0]$ in $\mathbb{Z}/5\mathbb{Z}$.

(b) $x^2 + x = [0]$ in $\mathbb{Z}/6\mathbb{Z}$.

(c) $x^2 + x = [0]$ in $\mathbb{Z}/p\mathbb{Z}$ where p is prime.

Solution: For the first two, just plug in the different congruences classes and see which ones work.

(a) $x = [0], [4]$.

(b) $x = [0], [2], [3], [5]$.

(c) Suppose that $x(x + [1]) = [0]$ in $\mathbb{Z}/p\mathbb{Z}$. Since p is prime, $\mathbb{Z}/p\mathbb{Z}$ is a field, so it has no zero divisors. This means that either $x = [0]$, or $x + [1] = [0]$, i.e. $x = [p - 1]$.

2.3.10 Prove that every non-zero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero divisor, but not both.

Solution: If $[a] \in \mathbb{Z}/n\mathbb{Z}$ is not a unit, then $(a, n) = d > 1$, write $a = dk$ and $n = d\ell$ for some integers k, ℓ. We then see that $n \mid a\ell$, so $[a][\ell] = [0]$ in $\mathbb{Z}/n\mathbb{Z}$, so that $[a]$ is a zero-divisor. $[a]$ cannot be both a unit and zero divisor, because if so, then we have $[a][x] = [1]$ and $[a][b] = [0]$ for some $[x], [b] \neq [0] \in \mathbb{Z}/n\mathbb{Z}$. Multiplying the second equation by $[x]$ says $[b] = [0]$, contradicting that $[a]$ is a zero divisor.

General comments

Presumably, you want feedback on your homework. Make you sure leave enough space between problems for me to write comments, please!

- When you define a variable, you *must* declare where it lives otherwise it is meaningless. Similarly, do not forget to quantify your variables (e.g. $a = nk$ for *some* $k \in \mathbb{Z}$).
- If you are claiming that something is true, you have to justify it. If you are using a theorem, make this clear. In particular, you need to mention *where* in your proof the hypotheses are being used.
- Make sure you double check your computations. A few of you gave an example in 2.1.22a) with $a \equiv 0 \bmod n$. Similarly, a few of you forgot solutions in 2.2.14a, b).
- In 2.1.22b), the condition that $(a, n) = 1$ does not mean that n is prime. It's also important to note that $(a, n) = 1$ is a *stronger* condition that just saying that $n \nmid a$. It was commonly written that "since $n \mid a(b - c)$ and $(a, n) = 1$, then $n \nmid a$ so $n \mid (b - c)$" The latter is not the point! If you drop the relatively prime condition, part a) says this statement is *false*.
- A general confusion among the problems is the difference between an integer $a \in \mathbb{Z}$ and the equivalence class $[a] \in \mathbb{Z}/n\mathbb{Z}$. The latter is a *set*, so it's nonsense to write things like "$p \mid [a]$" or "suppose $(a, n) = 1$ for $a \in \mathbb{Z}/n\mathbb{Z}$". This was particularly common in 2.2.14c) where x is written to mean an element of $\mathbb{Z}/n\mathbb{Z}$ and not an integer. To avoid these sorts of issues, write something like "let $x \in \mathbb{Z}/n\mathbb{Z}$ with $x = [a]$ for some $a \in \mathbb{Z}$".
- In 2.3.10, you should really be proving exercise 9 as part of your proof.