MTH 310 HW 2 Solutions

Jan 29, 2016

Section 2.3 Problem 1ab and 2ab

Find all units and zero divisors in $\mathbb{Z}_7$ and $\mathbb{Z}_8$.
Answer. Since $1(1) = 2(4) = 3(5) = 6(6) = 1 \bmod 7$, so there are no zero divisors in $\mathbb{Z}_7$ and all nonzero elements in $\mathbb{Z}_7$ are units. Similarly as $1(1) = 3(3) = 5(5) = 7(7) = 1 \bmod 8$ and $0 = 2(4) = 6(4) = 4(4) \bmod 8$, the units are 1,3,5,7 and the zero divisors are 2,4,6 (recall that zero is not a zero divisor with the general rule "you can't divide by zero"–although I didn't take points off for this).

Section 2.3, Problem 17

Prove that the product of two units in $\mathbb{Z}_n$ is also a unit.
Answer. Let $a, b \in \mathbb{Z}_n$ be units. Then there are elements c, d such that $ac = 1 \bmod n$ and $bd = 1$ mod n. This implies that $(ab)(dc) = abdc = a(1)c = ac = 1$ mod n, so ab is a unit with inverse dc.

Section 3.1, Problem 8

Is $\{1, -1, i, -i\}$ a subring of $\mathbb{C}$?
Answer. No. Note that $1 + 1 = 2 \notin \{1, -1, i, -i\}$, so $\{1, -1, i, -i\}$ is not closed under addition and hence not a subring. (If you go on to take MTH 411, you will find that this IS a group!)

Section 2.3, Problem 14

Let $a, b, n \in \mathbb{Z}$ with $n > 1$. Let $d = gcd(a, n)$ and assume $d|b$. Prove that the equation $[a]x = [b]$ has d distinct solutions in $\mathbb{Z}_n$.
Answer. Note: This problem was not graded, but here is a solution.
Theorem 1. The solutions listed in exercise 13b are distinct.

Proof. Using the notation from 13b, assume two elements of the solutions in 13b are equal. Then $[ub_1 + k_1 n_1] = [ub_1 + k_2 n_1]$ for some $k_1, k_2 \in \{0, 1, ..., d-1\}$. This implies that $ub_1 + k_1 n_1 \equiv ub_1 + k_2 n_1 \mod n$, so n divides their difference. Specifically, $n|(n_1(k_2 - k_1))$. Then there is some $j \in \mathbb{Z}$ with $nj = (n_1(k_2 - k_1))$. But since $n = n_1 d$, $dj = k_2 - k_1$, so $d|k_2 - k_1$ so $k_1 \equiv k_2 \mod d$. This implies since $k_1, k_2 \in \{0, 1, ..., d-1\}$, they must be equal. □

Theorem 2. If $x = [r]$ is any solution of $[a]x = b, [r] = [ub_1 + kn_1]$ for some integer $k \in \{0, 1, ..., d-1\}$.

Proof. We have that $ar \equiv b \equiv aub_1$ mod n, so n divides their difference, namely $n|(a(r - ub_1))$. Thus there is some $j \in \mathbb{Z}$ with $nj = a(r - ub_1)$. Dividing both sides of this equation by d, we obtain $jn_1 = a_1(r - ub_1)$, so $n_1|(a_1(r - ub_1))$. We have that the $gcd(a_1, n_1) = gcd(a, n)/d = 1$ so by theorem 1.4 $n_1|(r - ub_1)$ so there is some $k \in \mathbb{Z}$ with $kn_1 = r - ub_1$, so adding ub_1 to both sides of this equation proves our claim. □