MTH 310 HW 2 Solutions

Jan 29, 2016

Section 1.3, Question 7

Prove if $a, b, c \in \mathbb{Z}$ and p is a prime that divides a and $a + bc$, then $p|b$ or $p|c$.
Answer. Note that $p|a$, so there is an integer q with $a = pq$. Similarly as $p|(a + bc)$ then there is an integer k with $a+bc = pk$. Then we obtain $bc = a+bc-a = pk-pq = p(k-q)$, so $p|bc$. By Theorem 1.5 (Hungerford), since p is prime, $p|b$ or $p|c$.

Section 2.1, Problem 9b

Prove that if $n \in \mathbb{Z}$, $(2n - a)^2 \equiv a^2 (\text{mod } 4n)$.
Answer. Note that $(2n - a)^2 = 4n^2 - 4na + a^2 = 4n(n - a) + a^2$ and $a^2 = 0(4n) + a^2$ so $(2n - a)^2 \equiv a^2 (\text{mod } 4n)$.

Section 2.2, Question 14c

Prove that if p is prime that the only solutions to $x^2 + x = [0]$ in $\mathbb{Z}_p$ are [0] and [p-1].
Answer. Assume $x^2+x = [0]$ in $\mathbb{Z}_p$. Then we have $p|(x^2+x)$, so $p|(x(x+1))$. By Theorem 1.5 (Hungerford), since p is a prime that divides the product of two integers (namely, x and x+1), either $p|x$ or $p|(x + 1)$. If $p|x$, then $x = [0]$ in $\mathbb{Z}_p$. If $p|x + 1$, Then there is an integer q with $x + 1 = pq$. Therefore $x = pq - 1 + p - p = p(q - 1) + (p - 1)$, so in $\mathbb{Z}_p, x = [p - 1]$.