Math 310 Spring 2021 Problem set 6

Problem (Ex2.1) Suppose that $a, n \in \mathbb{Z}$ and $n > 1$. Show that if $[a]_n = [1]_n$, then $\gcd(a, n) = 1$.

Proof. Suppose that $a, n \in \mathbb{Z}$ and $n > 1$, and $[a]_n = [1]_n$. By Theorem 2.3, $a \equiv 1$ (mod n). By definition of congruence, $n \mid (a-1)$. Then by definition of divides, $a - 1 = nk$ for some $k \in \mathbb{Z}$. We can rewrite this as $a = nk + 1$. By Theorem 1.T.6 $gcd(a, n) = gcd(n, 1)$. Let's try to find $gcd(n, 1)$. Let $b \in \mathbb{Z}$ be a divisor of 1. We know by Lemma 1.T.5 that $-|1| \leq b \leq |1|$. From this we see that the greatest possible value for b is $|1|$ or 1. By Lemma 1.T.4, 1 is a divisor of 1, also 1 is a divisor of n. $gcd(n, 1) = 1$ by definition of Greatest Common Divisor. $gcd(a, n) = gcd(n, 1)$, therefore $gcd(a, n) = 1$. □

Problem (Ex2.2)(b) For $\mathbb{Z}_6$: (i) write out the addition table, write out the multiplication table, (iii) find all of the units, and (iv) find all of the zero divisors. (In this problem no proof is needed; you only need to give your final answers.)

Answer.

(i)

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

(ii)

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

(iii) [1], [5]
(iv) [2], [3], [4] □

Problem (Ex2.4) Let p be a prime integer with $p \geq 5$. Prove that $[p] = [1]$ or $[p] = [5]$ in $\mathbb{Z}_6$.

Proof. Suppose p is a prime integer with $p \geq 5$. By Corollary 2.5, $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. Also by Corollary 2.5, $[p]_6 = [r]_6$ where $r \in \mathbb{Z}$ and is the remainder of p divided by 6. By the definition of The Division Algorithm, let $p = 6q + r$ with unique integers q, r and $0 \leq r < 6$.

(Case 1): $[p]_6 = [0]_6$. By Corollary 2.5, $p = 6q + 0$ with $q \in \mathbb{Z}$, then $p = 6q$. And by definition of divides, $6 \mid p$, which is a contradiction because the only divisors of p are ± 1 and $\pm p$ by Definition of Prime. $[p]_6 \neq [0]_6$

(Case 2): $[p]_6 = [2]_6$. By Corollary 2.5, $p = 6q + 2$ with $q \in \mathbb{Z}$. We can rewrite this as $p = 2(3q + 1)$. Then $2 \mid p$ by definition of divisibility. p

cannot be 2 because $p \geq 5$, and similarly to Case 1, there's a contradiction, so $[p]_6 \neq [2]_6$.

(Case 3): $[p]_6 = [3]_6$ By Corollary 2.5, $p = 6q + 3$ with $q \in \mathbb{Z}$. We can rewrite this as $p = 3(2q + 1)$. Then $3 \mid p$ by definition of divisibility. Similarly to Case 1, there's a contradiction, so $[p]_6 \neq [3]_6$.

(Case 4): $[p]_6 = [4]_6$) By Corollary 2.5, $p = 6q + 4$ with $q \in \mathbb{Z}$. We can rewrite this as $p = 2(3q + 2)$. Then $2 \mid p$ by definition of divisibility. Similarly to Case 2, there's a contradiction, so $[p]_6 \neq [4]_6$.

(Case 5): $[p]_6 = [1]_6$ By Corollary 2.5, $p = 6q + 1$ with $q \in \mathbb{Z}$. When $q = 2$, $p = 13$. This fits our definition for p where p is prime and $p \geq 5$. This shows that it's possible for $[p]$ to equal $[1]$ for some p.

(Case 6): $[p]_6 = [5]_6$ By Corollary 2.5, $p = 6q + 5$ with $q \in \mathbb{Z}$. When $q = 1$, $p = 11$. Similarly to Case 5, $[p]$ may equal $[5]$.

The above shows that only two cases are possible, $[p] = [1]$ or $[p] = [5]$. □

Problem (Ex2.5) Let n be an integer with $n > 1$. Show that if $[a]$ is a unit in $\mathbb{Z}_n$ and $[b]$ is a zero divisor in $\mathbb{Z}_n$, then $[a] \odot [b]$ is a zero divisor in $\mathbb{Z}_n$.

Proof. Suppose n is an integer with $n > 1$ and that $[a]$ is a unit in $\mathbb{Z}_n$ and $[b]$ is a zero divisor in $\mathbb{Z}_n$. By Corollary 2.T.12, $[a] \neq [0]$ and $[b] \neq 0$. Using definition of a unit, there's an element $[j]$ where $a * j = 1$ in $\mathbb{Z}_n$. Because $[j]$ is a unit, we know by Corollary 2.T.12 that $[j] \neq [0]$. Using definition of a zero divisor, there's an element $[k]$ where $[k] \neq 0$ and $b * k = 0$ in $\mathbb{Z}_n$. $[aj][bk] = [0]$ because $1 * 0 = 0$. By the commutative property, $[ab][jk] = [0]$. By definition of zero divisor, $[ab]$ is a zero divisor. Using the definition of multiplication in $\mathbb{Z}_n$, $[a] \odot [b] = [ab]$. Therefore $[a] \odot [b]$ is a zero divisor in $\mathbb{Z}_n$. (TODO: Show that $[ab], [jk] \neq 0$.) □

Problem (Ex2.6)(b) Suppose that n is an integer with $n > 1$ and suppose that $[a] \in \mathbb{Z}_n$ with $[a] \neq [0]$. Show that $[a]$ is not both a unit and a zero divisor.

Proof. Suppose that n is an integer with $n > 1$ and suppose that $[a] \in \mathbb{Z}_n$ with $[a] \neq [0]$. Suppose $[a]$ is a unit. Using the definition of a unit, there's [b] such that $[ab] = [1]$. Also suppose $[a]$ is a zero divisor. By definition of zero divisor, there's some $[c] \neq [0]$ where $[ac] = [0]$. By Theorem 2.7 (m2) $[c] = [c][1]$. Then $[c] = [c][ab]$. Since $[c] = [ca][b]$ and $[ac] = [ca]$ by Theorem 2.7 (a4). $[ca] = [0]$, then $[c] = [0][b]$. Which can be rewritten as

$[c] = [0]$. Thus we have a contradiction and [a] cannot be both a unit and a zero divisor. □