MAT326 Fall 2013 **End-of-term Exam**

The total number of points is 25.

Question 1 (8 points). -
(a) Classify all non-zero elements in $\mathbb{Z}/15\mathbb{Z}$ into units and zero divisors.
(b) Pick any unit that is **not** [1] or [14] from your list and find its order.
(c) Find the inverse of the same element from part (b).
(d) Find the complementary zero divisors for [5].

Question 2 (5 points). Show that the order of [2] in $\mathbb{Z}/125\mathbb{Z}$ is at least 25.

Question 3 (6 points). Show that $n^{19} - n$ is divisible by 7 for all positive integers n.

Question 4 (6 points). -
(a) State Euler's Theorem.
(b) Compute the value of Euler's function for $m = 100$ and restate Euler's Theorem explicitly in the case of $\mathbb{Z}/100\mathbb{Z}$.

SOLUTIONS

1 a $15 = 3 \cdot 5$ So all zero divisors are represented by integers divisible by 3 or 5, so here

1	2	3	4	5	6	7	8	9	10	11	12	13	14
u	u	z	u	z	z	u	u	z	z	u	z	u	u

(u for "unit", z for "zero divisor")

b I pick [7] then $7^2 = 49 \equiv 4 \mod 15$
$7^3 \equiv 4 \cdot 7 = 28 \equiv 13 \mod 15$
$7^4 \equiv 13 \cdot 7 = 91 \equiv 1 \mod 15$

So $o([7]) = 4$

c Since $([7])^4 = [1]$, $[7]^{-1} = [7^3] = [13]$ from the computation in b.

(d) $[5]\underline{X} = [0]$ gives for $[x] = \underline{X}$ the equation $5x + 15y = 0$ (for some y)

$x = 0 + \frac{15}{(5,15)}k = 3k$, so $\underline{X}$ is any of $[0], [3], [6], [9], [12]$, so the zero divisors compl. to $[5]$ are $[3], [6], [9], [12]$

(2) $125 = 5^3$, so $\varphi(125) = 5^3 - 5^2 = 100 = 2^2 \cdot 5^2$

By Euler, $2^{100} \equiv 1 \mod 125$, so

$o([2]) \mid 100 \Rightarrow o([2]) =$ either $2, 4, 5, 10, 25, 50$, or 100.

All $2^2, 2^4, 2^5 = 32$ are < 125 and

$2^{10} = (2^5)^2 = 32^2 = 1{,}024 \equiv 24 \mod 125$

So $o([2]) \geq 25$

(3) If $7 \mid n$ then $7 \mid n^{19} - n$

If $7 \nmid n$ then $[n]$ is a unit in $\mathbb{Z}/7\mathbb{Z}$.

So $n^6 \equiv 1 \mod 7$ by Fermat

So $n^{18} = (n^6)^3 \equiv 1 \mod 7$

So $n^{19} \equiv n \mod 7$.

(4) (a) If $[a]$ is a unit in $\mathbb{Z}/m\mathbb{Z}$ then

$[a]^{\varphi(m)} = [1]$ in $\mathbb{Z}/m\mathbb{Z}$.

(b) Since $m = 100 = 2^2 \cdot 5^2$ then

$$\varphi(m) = \varphi(2^2) \cdot \varphi(5^2) = (2^2 - 2^1)(5^2 - 5^1)$$

$$= 2 \cdot 20 = 40.$$

So Euler's Theorem says, in this case,

if $[a]$ is a unit in $\mathbb{Z}/100\mathbb{Z}$

then $[a]^{40} = [1]$.