Homework

Jon Allen

September 24, 2014

Section 1.4: # 9, 20. Section 2.2: # 7, 9.

1.4

9. Let $(a, n) = 1$. The smallest positive integer k such that $a^k \equiv 1 \mod n$ is called the **multiplicative order** of $[a]$ in $\mathbb{Z}_n^\times$.

   (a) Find the multiplicative orders of [5] and [7] in $\mathbb{Z}_{16}^\times$.

$$\begin{aligned} [5] &= [5] & [25] &= [9] & [45] &= [13] \\ [65] &= [1] \\ [7] &= [7] & [49] &= [1] \end{aligned}$$

   So the multiplicative order of [5] in $\mathbb{Z}_{16}^\times$ is 4. The multiplicative order of [7] in $\mathbb{Z}_{16}^\times$ is 2.

   (b) Find the multiplicative orders of [2] and [5] in $\mathbb{Z}_{17}^\times$.

$$\begin{aligned} [2] &= [2] & [4] &= [4] & [8] &= [8] & [16] &= [16] & & 4 \\ [32] &= [15] & [30] &= [13] & [26] &= [9] & [18] &= [1] & & 8 \\ [5] &= [5] & [25] &= [8] & [40] &= [6] & [30] &= [13] & & 4 \\ [65] &= [14] & [70] &= [2] & [10] &= [10] & [50] &= [16] & & 8 \\ [80] &= [12] & [60] &= [9] & [45] &= [11] & [55] &= [4] & & 12 \\ [20] &= [3] & [15] &= [15] & [75] &= [7] & [35] &= [1] & & 16 \end{aligned}$$

   So the multiplicative order of [2] in $\mathbb{Z}_{17}^\times$ is 8. The multiplicative order of [5] in $\mathbb{Z}_{17}^\times$ is 16.

20. Show that $\varphi(1) + \varphi(p) + \cdots + \varphi(p^\alpha) = p^\alpha$ for any prime number p and any positive integer α

$$\begin{aligned} \varphi(1) + \varphi(p) + \cdots + \varphi(p^\alpha) &= \varphi(1) + \sum_{n=1}^{\alpha} \varphi(p^\alpha) \\ &= 1 + \sum_{n=1}^{\alpha} p^n \left(1 - \frac{1}{p}\right) \\ &= 1 + \sum_{n=1}^{\alpha} \left(p^n - p^{n-1}\right) \\ &= 1 + \sum_{n=1}^{\alpha} p^n - \sum_{n=0}^{\alpha-1} p^n \\ &= 1 + p^\alpha - p^0 \\ &= p^\alpha \end{aligned}$$

2.2 7. Define an equivalence relation on the set $\mathbb{R}$ that partitions the real line into subsets of length 1.

We define $x \sim y$ for all $x, y \in \mathbb{R}$ if $\lfloor x \rfloor = \lfloor y \rfloor$. For all $x \in \mathbb{R}$ we define $\lfloor x \rfloor = n$ where $n \in \mathbb{Z}$ and $x - 1 < n \leq x$. It is trivial to see that this relation satisfies reflexivity, symmetry, and transitivity. Furthermore, because the relation partitions the elements of $\mathbb{R}$ into classes that span $\mathbb{Z}$, it partitions the real line into subsets of length one (the distance between two integers is a multiple of one).

9. Let S be a set. A subset $R \subseteq S \times S$ is called a **circular relation** if (i) for each $a \in S, (a, a) \in R$ and (ii) for each $a, b, c \in S$, if $(a, b) \in R$ and $(b, c) \in R$, then $(c, a) \in R$. Show that any circular relation must be an equivalence relation.

proof

First we note that reflexivity is given. Let's choose some $(b, a) \in R$. Because we are given reflexivity, we know that $(a, a) \in R$. So then by the definition of the circular relation we see that because we have $(b, a) \in R$ and $(a, a) \in R$ then we must have $(a, b) \in R$. And we see that symmetry is preserved in this relation. And finally, lets take $a, b, c \in S$ where $(a, b) \in R$ and $(b, c) \in R$. We are told that $(c, a) \in R$ and we have shown that symmetry holds, so we know that (a, c) is also in R. And that gives us transitivity. Three out of three conditions met. We are done here. $\square$