Math 110AH Fall 18

HOMEWORK 3 - SOLUTIONS

Problem 1. Given $k \in \mathbb{N}$, denote the sum of its digits by $\varsigma(k)$. If $k > 9$, $\varsigma(k) < k$. Indeed, in that case we can write $k = \sum_{i \geqslant 0} a_i 10^i$ with at least one a_j non zero with $j > 0$. Then $a_j < a_j 10^j$, so:

$$\varsigma(k) = \sum_{i \geqslant 0} a_i < \sum_{i \geqslant 0} a_i 10^i = k.$$

And if $k \leqslant 9$, $\varsigma(k) = k$.

Now given $n \in \mathbb{N}$, define a sequence inductively by $n_0 = n$, and $n_{i+1} = \varsigma(n_i)$ for all $i \geqslant 0$. The property above shows that if $(n_i)_i$ does not stabilize, it is a decreasing sequence in $\mathbb{N}$, which does no exist. Hence $(n_i)_i$ stabilizes to a value that we call $f(n)$.

To prove that $n \equiv f(n) \bmod 3$, we show that for all $k \in \mathbb{N}$, $k \equiv \varsigma(k) \bmod 3$. Let $k \in \mathbb{N}$, let us write its digit development $k = \sum_{i \geqslant 0} a_i 10^i$. Since $10 \equiv 1 \bmod 3$, we have $10^i \equiv 1 \bmod 3$ for all $i \geqslant 0$. Hence:

$$k = \sum_{i \geqslant 0} a_i 10^i \equiv \sum_{i \geqslant 0} a_i = \varsigma(k) \quad \bmod 3.$$

Problem 2. The operation is associative by assumption, let us show that it also has an identity element and that every element admits a two-sided inverse.

Let $g \in G$. Associativity allows to consider the sequence $(g^n)_{n \geqslant 1}$. Since G is finite, this sequence is not injective, so we can find $m < n$ such that $g^m = g^n$. Let $e := g^{n-m}$, let us prove that e is an identity element. For all $a \in G$ we have:

$$g^m ea = g^m g^{n-m} a = g^n a = g^m a$$

Left cancellation by g^m gives $ea = a$. Similarly, we have $aeg^m = ag^m$, so right cancellation by g^m gives us $ae = e$. Thus e is an identity element.

Now let $a \in G$, let us prove that a has a two-sided inverse. The map:

$$\begin{cases} G & \to & G \\ x & \mapsto & ax \end{cases}$$

is injective by left cancellation. Since G is finite, it is a bijection. So we can find $b \in G$ such that $ab = e$, *i.e.* b is a right inverse to a. Multiplying on the right by a gives us:

$$aba = ea = a = ae$$

the last two equalities coming from the fact that e is an identity element. Then left cancellation yields $ba = e$. Hence b is a two-sided inverse of a.

So G is a group for that operation.

Problem 3. Let $a, b \in G$. The assumption can be written:

$$abab = aabb.$$

Multiplying on the left by a^{-1} and on the right by b^{-1} gives $ba = ab$. This holds for all $a, b \in G$, so G is abelian.

Problem 4. Note first that multiplication in $\mathbb{Z}/m\mathbb{Z}$ is associative and commutative, since it is induced by the multiplication in $\mathbb{Z}$. We will denote by $[n]$ the class of an integer n in $\mathbb{Z}/m\mathbb{Z}$.

We start by proving that multiplication is a binary operation on $(\mathbb{Z}/m\mathbb{Z})^\star$ (so we have to check that this set is closed under multiplication). Let $a, b \in (\mathbb{Z}/m\mathbb{Z})^\star$. We can find $u, v \in \mathbb{Z}/m\mathbb{Z}$ such that $au = [1] = bv$. Then $abvu = au = [1]$. So $ab \in (\mathbb{Z}/m\mathbb{Z})^\star$: multiplication is a binary operation on $(\mathbb{Z}/m\mathbb{Z})^\star$.

It is associative by the remark above. The identity element is $[1]$. Finally, every element in $(\mathbb{Z}/m\mathbb{Z})^\star$ has an inverse by definition. So $(\mathbb{Z}/m\mathbb{Z})^\star$ is a group under multiplication.

Let us now prove the following: given $n \in \mathbb{Z}$, $[n]$ is multiplicatively invertible in $\mathbb{Z}/m\mathbb{Z}$ if and only if n and m are coprime.
Assume first that n and m are coprime. Then we can find integers k, l such that $km + nl = 1$. Reducing modulo m gives $[n]\,[l] = [1]$, so $[n]$ is multiplicatively invertible in $\mathbb{Z}/m\mathbb{Z}$.
Conversely, if $[n]$ is multiplicatively invertible in $\mathbb{Z}/m\mathbb{Z}$, we can find $i \in \mathbb{Z}$ such that $[n]\,[i] = [1]$. Thus $m|(ni - 1)$, from which we deduce $nl - 1 = mj$ for some $j \in \mathbb{Z}$. Hence m and n are coprime.

So a list of the distinct elements in $(\mathbb{Z}/m\mathbb{Z})^\star$ is given by the classes $[n]$ for $n < m$ coprime with m. Thus there are $\phi(m)$ elements in $(\mathbb{Z}/m\mathbb{Z})^\star$.