MATH 430 Worksheet 4 Problem 6

Qilin Ye

October 3, 2020

Worksheet 4 Problem 6

Let p be a prime.

(1) Let $\mathcal{T} = \{1, 2, \ldots, p-1\}$. Pick $a \in T$. Let $\mathcal{S}$ be a multiset such that

$$\mathcal{S} = \{[ma]_p \mid m \in [1, p-1]\}.$$

Show that $\mathcal{S}$ has $p-1$ elements and that $\mathcal{S} = \mathcal{T}$.

(2) Multiply all elements in $\mathcal{S}$ and multiply all elements in $\mathcal{T}$. Give an alternate proof for Fermat's Little Theorem.

Solution

(1) Since $\mathcal{T}$ has $p-1$ elements and each element of $\mathcal{T}$ corresponds to an element of the *multiset* $\mathcal{S}$ (though not necessarily distinct in general cases), we know that $\mathcal{S}$ has $p-1$ elements.

Instead of treating elements of $\mathcal{S}$ and $\mathcal{T}$ as integers in $\mathbb{Z}$, the way $\mathcal{S}$ is defined reminds us to treat them as elements of $(\mathbb{Z}/p\mathbb{Z})^*$. Then it follows that, by the closure of a group, for any $m \in (\mathbb{Z}/p\mathbb{Z})^*$ we always have $[ma] \in (\mathbb{Z}/p\mathbb{Z})^*$. Therefore *all* elements of $\mathcal{S}$ are elements of $\mathcal{T}$, i.e., $\mathcal{S} \subset \mathcal{T}$.

Having shown $|\mathcal{S}| = |\mathcal{T}|$ and $\mathcal{S} \subset \mathcal{T}$, all that remains to show is that **the elements of $\mathcal{S}$ are distinct**: if this is the case, then there are $p-1$ distinct elements in $\mathcal{S}$, each of which happens to also be in $\mathcal{T}$. Then it follows naturally that $\mathcal{S} = \mathcal{T}$ since they contain exactly the same elements.

Suppose, by contradiction, that the elements of $\mathcal{S}$ were *not* distinct. Then for some $1 \leqslant m_1 < m_2 \leqslant p-1$ we have (in $(\mathbb{Z}/p\mathbb{Z})^*$)

$$am_1 = am_2.$$

But cancellation law states that $a^{-1}am_1 = a^{-1}am_2 \implies m_1 = m_2$; contradiction. Hence there cannot be repeating elements in $\mathcal{S}$. Therefore $\mathcal{S} = \mathcal{T}$.

(2) From (1) we know (in $(\mathbb{Z}/p\mathbb{Z})^*$)

$$\{a, 2a, \ldots, (p-1)a\} = \mathcal{S} = \mathcal{T} = \{1, 2, \ldots, p-1\}.$$

Clearly $\mathcal{S}$ simply permutes elements of $\mathcal{T}$. Now if we multiply everything in $\mathcal{S}$ and multiply everything in $\mathcal{T}$ we should get the same answer. Then the equation becomes

$$(p-1)!\, a^{p-1} = (p-1)!$$

(where ! stands for factorial, not exclamation mark, of course). Since $(p-1)!$ is obtained by multiplying elements of $(\mathbb{Z}/p\mathbb{Z})^*$ it follows that $(p-1)! \in (\mathbb{Z}/p\mathbb{Z})^*$ and so its inverse exists. Then,

$$[(p-1)!]^{-1}\,(p-1)!\, a^{p-1} = [(p-1)!]^{-1}\,(p-1)! \implies a^{p-1} = e = 1.$$

Hence we've proven Fermat's Little Theorem using a different method.

Remark

For (1), a more elegant way is to show that

$$\text{mult}_a : (\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^* \text{ defined by } [m] \mapsto [am]$$

is a bijection. First thing: the codomain is indeed $(\mathbb{Z}/p\mathbb{Z})^*$ since closure guarantees $am \in (\mathbb{Z}/p\mathbb{Z})^*$. By the pigeonhole principle, since the domain and codomain are finite with equal cardinality, it suffices to show mult_a is injective. (If $f : A \to B$ with $|A| = |B| < \infty$ then f is injective if and only if it is surjective.) Suppose mult_a were not injective, then for some $m_1 \neq m_2$ we have $am_1 = am_2$. Again this implies $a^{-1}am_1 = a^{-1}am_2 \implies m_1 = m_2$, contradiction. Hence mult_a is injective, surjective by pigeonhole, and bijective by definition. Now notice that $\mathcal{T}$ is precisely the domain of mult_a and $\mathcal{S}$ the image. Therefore $\mathcal{S} = (\mathbb{Z}/p\mathbb{Z})^* = \mathcal{T}$.

To generalize this:

Theorem

For $m \in \mathbb{N}$ and a with $\gcd(a, m) = 1$, the function

$$\text{mult}_a : (\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/m\mathbb{Z})^* \text{ defined by } [x] \mapsto [ax]$$

is a bijection. Furthermore, this theorem can be used directly to prove Euler's Theorem.