Number Races : An Elementary Exposition

This is an expository article aimed at secondary school students explaining the beauty of the construct of integer modulo but not rigorous proofs. We shall see how this leads to Euler's theorem. The reader is expected to know basic definition of natural numbers, integers, prime numbers, LCM, GCD and rudimentary operations with them. The reader is expected to keep trying things on his/her own as one keeps reading the article.

Consider the following sequences,

$$S_a = \{ka, \forall k = \{1, 2, 3, \dots\}\} = a, 2a, 3a, \dots$$

$$S_b = \{kb, \forall k = \{1, 2, 3, \dots\}\} = b, 2b, 3b, \dots$$

where a, b are positive integers. One would observe that if $b > a$ the second sequence would run faster than the first one. Let us ask the following questions:

1. Do the two sequences meet for all values of a and b ? More precisely, do we have indexes i, j so that $S_a(i) = S_b(j)$?

2. Let us mark all the values attained by S_b by red points on the number line. Similarly let the values attained by S_a be marked by blue points. Lets take every red point and perform the following operation. Find the distance (is always assigned positive sign irrespective of the direction) between the red point and its nearest (on either of the sides) blue point and tabulate it. Once all red points are exhausted, operate similarly on the blue points. Append both the lists and the look for the smallest positive number (the smallest distance)in the list. What would you observe?

A quick observation would shall lead to observation the indexes $i = b$ and $j = a$ where $S_a(i) = S_b(j)$. Therefore we answer the first question in affirmative. As of the second question, an attentive reader could have some genuine concerns like
(i) Since the sequences have very long length that never stops (or *infinite* length), can we have a finite distance list ?
(ii) We could be recounting a lot of distances by first counting red list and then the blue list as there could be repetitions. If we are lucky enough, this could even solve (i). [1]

Reader acquainted with the concept of *Least common multiple (LCM)* shall find that S_a and S_b first meet at $[a, b] = LCM(a, b)$ (and indeed they keep meeting exactly at the sequence $S_l = \{k \cdot [a, b], k = \{1, 2, 3, \dots\}\}$). This shows that the arrangement of red and blue points repeats after a certain interval and the smallest length of the interval happens to be the LCM. This would mean, all we need to study is a small interval and rest follows the suit. This motivates the concept of integer modulo. A word of caution for the reader before we go into integer modulo - All facts we discussed also holds good for integers in with *minor* modifications.

Let $a = 4$ and $b = 6$. The sequences meet at $[4, 6] = 12$. Our integer modulo is a finite world consisting of $\{1, 2, 3, \dots, 12\}$. What about 13 and further integers, 0 and other negative integers? 13 is to be treated as 1, 14 as 2 and so on until 24 is treated as 12 and similarly further. This makes sense as the distribution of red and blue points shall remain same in the 13 to 24 range as in 1 to 12 range. One can perceive this as folding the number line between two fixed points. The reader is advised to spend some time working out various examples. A convenient notation shall be to consider the integer modulo set starting from 0 like $\{0, 2, 3, \dots, 11\}$ since for any integer not belonging to the set, the equivalent integer in the set is the remainder when divided by 12.

The reader may find the results pretty surprising and nice, wonder about the construction of integer modulo. One is advised to think about finding equivalents for negative integers (you will have to conduct negative races and find some invariant), think why remainder figures out in the discussion by writing some pictures of some races and convince oneself of its validity. Once the reader is able to feel the result, he/she is advised to prove it in general for all a, b. [2]

We are now in a position to generalize the argument in the previous paragraph. An attentive reader would have observed that integer modulo set can be constructed with respect to any positive integer, not necessarily the $[a, b]$. But in that case the properties could differ and our basic intent of constructing integer modulo goes in vain! As a coach of a famous football team once said *'Not so fast my friend ...'* Lets experiment with arbitrary modulo construction and see what it offers us.

[1] We leave these question to the reader. One shall find clues to answer later in the article.
[2] Please ask your instructor for further help

Lets look at the integer modulo 7, the corresponding set is $\{0, 2, \ldots, 6\}$. Do spend some time thinking about arbitrary integer moduli, look for the races of the elements of the set. An surprising observation shows that equivalents of elements in the sequence of the 2's race $(2, 4, 6, \ldots)$ include every number in the moduli set. A quick check shows that same is not the case with $\{0, \ldots, 3\}$ (which is the modulo set of 4) as 3 is never attained. Again an attentive reader shall see the link between this and first set of questions we asked at the beginning of the article.

If you have come till this point, understanding and experimenting through all material till now, here are some facts which are quoted without proof. You would like to experiment again and read more in a book or ask your instructor. You would learn the concise modulo notation.

1. (Gauss's theorem) For the integer modulo $\{0, \ldots, p\}$ where p is a prime, the race of any element other than 0 in the integer modulo with p shows that every distance is attained equivalently every equivalents of elements in the race include every number in the moduli set.

2. (Euler's theorem) For the integer modulo $\{0, \ldots, n\}$, Gauss's theorem's property holds in the racing element say e and n if they are relatively prime that is $GCF(e, n) = 1$

Happy exploration! [3]

[3]You may write to the author: sriperso@yahoo.co.in