MATH 8
ASSIGNMENT 4: EULER'S THEOREM
JAN 21ST, 2018

In two weeks we are going to start Geometry. Please buy: "The Art of Problem Solving, Volume 1: The Basics" by Sandor Lehoczky and Richard Rusczyk, ISBN-13: 978-0-9773045-6-1. Please do not get the solution manual (or hide it for emergencies). It is important that you try the problems on your own.

Theorem. *If a, m are relative prime, then $a^{\varphi(m)} \equiv 1 \mod m$, where $\varphi(m)$ is Euler's totient function which gives the number of remainders mod m that are relative prime to m.*

Proof. First, we write down all remainders mod m that are relative prime to m: $\{1, r_1, r_2, \ldots, m-1\}$. Since 1 and $m-1$ are relative prime to m, we can see that $\{a, r_1a, r_2a, \ldots, (m-1)a\}$ is a rearrangement of $\{1, r_1, r_2, \ldots, m-1\}$. Since $gcd(a, m) = 1$, $r_ia \equiv r_ja \mod m$ means that $r_i \equiv r_j \mod m$. Since the two lists are the same $modm$, we have:

$$a \cdot r_1a \cdot r_2a \cdots (m-1)a \equiv 1 \cdot r_1 \cdot r_2 \cdots (m-1) \mod m$$

But since all the r_i are relative prime to m, we can cancel them

$$a \cdot a \cdot a \cdots a \equiv 1 \mod m$$

How many a's are there? It is the number of integers less than m and relative prime to m. This function is called Euler's $\varphi(n)$.

$$a^{\varphi(m)} \equiv 1 \mod m$$

□

Theorem. *We proved the following during last class for p prime*

$$\varphi(p) = p - 1$$
$$\varphi(p^k) = p^{k-1}(p-1)$$

Theorem. *$\varphi(n)$ is multiplicative: if m, n are relatively prime, then $\varphi(mn) = \varphi(m)\varphi(n)$.*

Proof. The trick is to write the number of integers from 1 to mn in a grid:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & mn \end{array}$$

Consider an element r that is not relativ prime to m. Then any element in the row:

$$r \quad m+r \quad 2m+r \quad \cdots \quad (n-1)m+r$$

is not relative prime to mn. Thus, when counting elements relative prime to mn, we only need to consider rows starting with elements relative prime to m. There are $\varphi(m)$ such rows. Lets consider such a row, made up of elements $km + r$ for $k = 0, 1, \ldots, (n-1)$. The row contains n elements, and no two of these elements are congruent $\mod n$ (remember that n,m are relative prime). Since we have n elements and no two are congruent, the elements of the row are a rearrangement of $0, 1, \ldots, n-1$. Thus $\varphi(n)$ of these elements are relative prime. All in all, there are $\varphi(m)$ rows of elements relative prime to m, with $\varphi(n)$ elements in each row relative prime to n so there are $\varphi(m)\varphi(n)$ total elements relative prime to mn. □