SEMIGRAPHS AND FERMATS THEOREM

MEENAKSHI.K, HANUMESHA.A.G

Abstract: Graphs have been used to prove fundamental results in areas of number theory. In this paper we study the proof of Fermat's theorem and Euler's theorem using Semigraphs.

Keywords: Semigraphs, Fermat's theorem, Euler's theorem

AMS Classification: 11A41, 11A51, 11A051, 05C30, 05C45

Introduction: Graph theory is becoming increasingly significant as it is applied to other areas of mathematics, science and technology. It is being actively used in fields as varied as biochemistry (genomics), electrical engineering (communication networks and coding theory), computer science (algorithms and computation) and operations research (scheduling).
Prime numbers have fascinated Mathematicians since the ancient Greeks. Euclid has given the first proof for existence of infinity of primes 2,3,5,7,11,13,..... Many Mathematicians were trying to find out the pattern for the same. Prime numbers have remained the main object of study for many years. Some of the important theorems or results related to prime numbers are the Fundamental theorem of Arithmetic, Fermat's theorem, Wilson's theorem, Perfect number conjectures, Prime Number theorem, Goldbach Conjecture and so on. Proof for Prime Factorisation theorem was discussed in [7]. Bichitra Kalita has discussed the graph theoretic proof of Goldbach Conjecture.
Fermat's theorem is an important property of integers to a prime modulus. There are many proofs for Fermat's Little Theorem. The first known proof was communicated by Euler in his letter dated 6th March 1742 to Goldbach. The idea of the graph theoretic proof together with some number theoretic results, was used to prove Euler's generalization to non-prime modulus.

2. Definitions

2.1 Graph A graph $G(V,E)$ consists of a finite non empty set V called as set of vertices together with a set E called the set of edges of undirected pair of distinct points of V.

2.2 Simple graph A graph $G(V,E)$ is said to be simple if it has no self loops and parallel edges.

2.3 Multi graph A graph $G(V,E)$ is said to be a multi-graph if it is not a simple graph.

2.3 Degree of a vertex The number of edges incident with the vertex with self loops counted twice is called as the *degree* of that vertex. A vertex of a graph is called a *pendent vertex* if the degree of the vertex is one.

2.4 Complete graph: A graph $G(V,E)$ is said to be *complete* if there is an edge between every pair of vertices. A complete graph is also called as the *universal graph or a clique*. The degree of every vertex in a complete graph is $n-1$ and it has $\frac{n(n-1)}{2}$ edges. The complete graph of n vertices is denoted by K_n.

2.5 Bipartite graph: A graph $G(V,E)$ is said to be *bipartite graph* if the vertex set V is partitioned into two disjoint subsets say V_1 and V_2 consisting of m and n vertices whose edge has one vertex in V_1 and other vertex in V_2. It is said to be *complete bipartite* if every vertex of V_1 is incident with every other vertex of V_2. It is denoted by $K_{m,n}$. The bipartite graph $K_{1,n}$ is called as the *star* whose vertex set consist of 2 vertex sets V_1 and V_2 consisting of only one vertex and n vertices respectively where one vertex of V_1 is incident with all the n vertices of V_2.

2.6Weighted graph A weighted graph associates a label(weight) with every edge in the graph. Weights are usually real numbers. They may be restricted to rational numbers or integers.

2.7 Equivalent graphs Two graphs are said to be equivalent if the vertices can be relabeled to make them equal.

2.7 Semigraphs Semigraph is a natural generalization of graph, when drawn in a plane and where every concept/result in a graph has a natural generalization. In a Semigraph, the edges are assumed to have many parts and vertices are classified according to their positions.

A Semigraph S is a pair (V,X) where V is a non-empty set whose elements are called vertices of S and X is a set of ordered n-tuples n≥2, called edges of S satisfying the following conditions:

The components of an edge E in X are distinct vertices from V.

Any two edges have at most one vertex in common.

Two edges $E_1=(u_1,u_2,u_3,\ldots.u_m)$ and $E_2=(v_1,v_2,\ldots v_n)$ are said to be equal iff m = n and either

$u_i= v_i$ or $u_i = v_{n-i+1}$ for $1 \le i \le n$.

The vertices in a semigraph are divided into three types namely end vertices, middle vertices and middle end vertices, depending upon their positions in an edge. The end vertices are represented by thick dots, middle vertices are represented by small circles and a small tangent is drawn at the small circles to represent middle-end vertices.

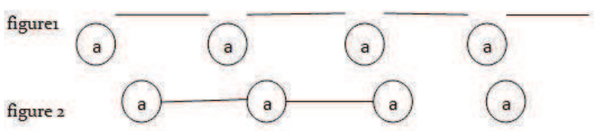
3.Proof of Fermat's theorem using Semigraphs:

3.1Fermat's Theorem For any prime *p* and any *a* in Z such that *a* is not congruent to 0 mod p,

$a^{p-1} \equiv 1(\mathrm{mod}\, p).$

Proof Let G be a semigraph with *p* number of vertices whose every vertex is named a. Let the weight of the semigraph at the end vertex be defined as the product of the prime vertices. The weight of the semigraph at the end vertex is a^p. Remove the edge incident with the end vertex. The resulting semigraph is the disconnected graph G-e. Let the weight of the edge deleted semigraph be defined as the sum of the vertices. The weight of the resulting semigraph is a multiple of *a* that is p times a. Therefore p divides the weight of the resulting semigraph

G-e. The disconnected vertex named *a* is the remainder when $a^p - a$ is divided by p.



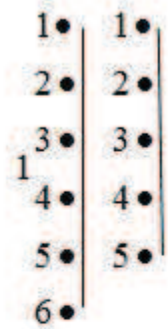
3.2 Euler's theorem: For m ≥ 2 in Z^+ and any $a \in Z$, such that $(a,m)=1,\ a^{\phi(m)} \equiv 1 \bmod m$, where $\phi(m)$ is the number of invertible integers modulo m.

Proof: Construct a semigraph with vertices as natural numbers 1,2,3,.... Let the initial vertex be $a_1=1$ and the end vertex be some positive integer $a_m=m$ greater than or equal to 2. That is the vertex set is $\{a_1,a_2,a_3,\ldots a_m\}$. Consider the edge sets $\{a_1,a_2\},\{a_1,a_3\},\{a_1,a_4\},\{a_2,a_3\},\{a_2,a_4\},\{a_3,a_4\},\{a_3,a_5\},\{a_4,a_5\},\ldots$ ....Let the weight of the semigraph be defined as the sum of the two vertices.

If m = p is prime, all non-zero integers modulo p are invertible, so $\phi(p) = p-1$ and Euler's theorem becomes Fermat's Little theorem. Euler's function $\phi(p) = p-1$ is the number of vertices from the initial vertex to the vertex p-1. That is $\phi(p)$ is the vertex set {1,2,3,...... p-1}.

If m is not prime then the Euler's function is defined as the set of edges comprising of two vertices whose weight is a multiple of m, where both are relatively prime, or the union of edges comprising of two vertices whose weight is a multiple of m, where both are relatively prime.

Figure 3.2.1 for the composite number m = 6 and for the prime no. m = 5.



Example 3.2.1 Let m be the prime p =5. The vertex set is {1,2,3,4,}. Then the Euler function $\phi(5) = \{1,2,3,4\}$.

Example 3.2.2 Let m be the composite number 6. The vertex set is {1,2,3,4,5}. Then the set of edges whose weight is 6 are {1,5},{2,4}. Euler function $\phi(6)$ is the set {1,5}, which consists of only co-primes, where both are relatively prime.

Example 3.2.3 Let m be the prime p=11. The vertex set is {1,2,3,4,5,6,7,8,9,10}. Then the Euler function is same as the vertex set. That is $\phi(11) = \{1,2,3,4,5,6,7,8,9,10\}$.

Example 3.2.4 Let m be the composite number 8. Then the set of edges whose weight is 8 are {1,7},{2,6},{3,5}. Euler function $\phi(8)$ is the union of the edge sets {1,7},{3,5}, which consists of only co-primes, that is the set {1,3,5,7} Euler's function is $\phi(8)$ =4.

Example 3.2.5 Let m be the composite number 15. Then the set of edges whose sum is 15 are {1,14},{2,13},{4,11},{7,8} which consists of only co-primes. Euler's function $\phi(15)$ is the union of the above edges that is the set {1,2,4,7,8,11,13,14}. Euler's function is $\phi(15)$ =8.

Keith Conrad made some changes in Fermat's theorem to get Euler theorem.[4] We will see the proof of the same using graphs.

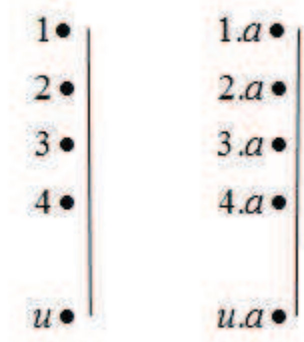
Consider two equivalent graphs G_1 and G_2. Let the vertices of G_1 be named 1,2,3,.....p-1. Let the vertices of G_2 be 1.a,2.a,3.a,........(p-1)a. Let the weights of G1 and G2 be defined as the product of the vertices at the end vertex. The weights of G1 and G2 at the end vertex a_{p-1} are the products 1.2.3....p-1 and a.2a.3a.........(p-1)a. Since G1 and G2 are equivalent, we have their weights also to be equivalent. That is

$$\{1.2.3.......p-1\} \equiv \{a.2a.3a.......(p-1)a\} (\bmod p)$$

$$\Rightarrow 1 \equiv a^{p-1} (\bmod p)$$

.

Figure 3.2.2 vertex 1 to the vertex $u = p-1$



Conclusion: Thus we have discussed the proof of Fermat's theorem and Euler's theorem using semigraphs. We can also explore the proofs of the above theorems using hypergraphs and other graphs

References:

1. S.Vaithyasubramanian, A.Christy, A Practice to Create User Friendly Secured Password; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 3 Issue 1 (2014), Pg 272-274
2. Bichitra Kalita, Graphs and Goldbach Conjecture.
3. Cargal.J.M, Euler's theorem and Fermat's Little Theorem, Discrete Mathematics for Neophytes: Number theory, Probability, Algorithms and other stuff.
4. Mandeep Kumari ,Renu Chugh, An Algorithm for A Finite Family of Nonexpansive Maps; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 3 Issue 1 (2014), Pg 287-290
5. David A.Cox, Introduction to Fermat's Last theorem.
6. Keith Conrad, Euler's Theorem.
7. J. Krishnaveni, J. Subhashini, C. Sekar, Some Separation Properties of Čech Soft Closure Spaces; Mathematical Sciences international Research Journal ISSN 2278 – 8697 Vol 3 Issue 2 (2014), Pg 698-700
8. E.Sampathkumar, Semigraphs.
9. Murugesan.N and Narmadha.D, Some properties of Semigraphs and its associated graphs,
10. Meenakshi.K, Proof of Prime Factorization Theorem using graph theory, International Journal of Science and Technology.
11. Shariefuddin Pirdaza and Ashay Dharwadker, Applications of Graph Theory, Journal of the Korean Society for Industrial and Applied Mathematics, Vol 11, No.4, 2007.
12. *K. Jayalakshmi* , *O*n Prime Derivations With D 3n + 1 Contained in the Center; Mathematical Sciences International Research Journal ISSN 2278 – 8697 Vol 2 Issue 2 (2013), Pg 145-146

***

Meenakshi.K/Associate Professor/CMR Institute of Technology,
Hanumesha.A.G/Associate Professor/SJC Institute of Technology,