Understanding the Distribution of Totatives

Karen Amagrande, Mathematics
Advisor: Dr. Mitsuo Kobayashi
Kellogg Honors College Capstone 2012
California State Polytechnic University, Pomona

Introduction

Understanding the distribution of totatives is useful in bounding primitive *nth* roots of unity of irreducible polynomials when other methods fail. D. H. Lehmer, in his paper "The Distribution of Totatives", uses Euler's totient function to study the distribution of numbers less than, and relatively prime to, any given positive integer, *n*. Those positive integers are called the totatives of *n*, and the number of totatives for any given *n* can be calculated by using the formula for Euler's totient function,

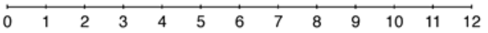
$$\varphi(n) = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k}$$

where *n* is the number being considered, and each *p* represents a distinct prime factor of *n*.

The question considered in Lehmer's paper is this: how are the *φ(n)* numbers of any given *n* distributed over the interval *[0,n]* and can a general formula be derived to determine under what circumstances those totatives are uniformly distributed? The purpose of this project is to make the math in Lehmer's paper understandable to other undergraduate students by bridging the gaps in Lehmer's mathematical derivations using techniques from number theory.

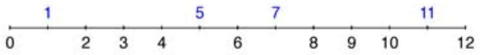
A Distribution Test

Let's examine what happens when n=12.

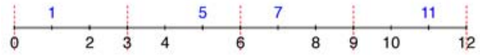


To determine if a number is a totative of 12, we need to check the greatest common divisor of 12 and each integer less than 12; a gcd of 1 indicates that the two numbers are relatively prime, and the smaller number is a totative of 12. Note that the proper divisors of 12 are 1,2,3,4 and 6.

gcd (1,12)=1 gcd(2,12)=2 gcd(3,12)=3
gcd(4,12)=4 gcd(5,12)=1 gcd(6,12)=6
gcd(7,12)=1 gcd(8,12)=4 gcd(9,12)=3
gcd(10,12)=2 gcd(11,12)=1



The gcd test reveals that 1, 5, 7 and 11 are the totatives of 12. Charting these numbers we can see that they are not clustered together but are distributed over the interval. How can we determine what type of distribution this represents?



If we divide the interval [0,12] into equal subintervals we can see if the totatives fall evenly into each section. Here we have divided the interval into 4 such subintervals. Divide 12 by 4 and you have intervals of width 3.

The graph shows that each interval contains exactly one totative. When each subinterval contains the same number of totatives, we say that the totatives are **uniformly distributed with respect to k** where k represents the number of subintervals.

The goal of Lehmer's paper was not to test every number *n* and every *k* subintervals for each n, but rather to arrive at a general formula that could be applied to any *n*.

Lehmer's Approach

Lehmer approached this problem by using the following formula:

$$E(k,q,n) = \varphi(n) - k\varphi(k,q,n)$$

where *k* is the number of subintervals, *q* represents which subinterval is being tested (*q=0,1,…, k-1*), *n* is the positive integer being examined, and $\varphi(n)$ is Euler's totient formula. Euler's totient formula counts the number of totatives less than n and $\varphi(k,q,n)$ is the number of totatives in the *qth* of *k* subintervals.

This *excess* or *error* formula tells us that if $E(k,q,n) = 0$ then the totatives are evenly distributed on the qth interval; if $E(k,q,n) > 0$ then the subinterval contains too many totatives to be evenly distributed; finally, if $E(k,q,n) < 0$ then the subinterval contains too few totatives to be evenly distributed.

Now, for the totatives to be evenly distributed, we must have

$$E(k,0,n) = E(k,1,n) = E(k,2,n) = \cdots = E(k,k-1,n) = 0 \qquad (1)$$

over all k subintervals. It is also apparent that because

$$E(k,q,n) = \varphi(n) - k\varphi(k,q,n) = 0$$

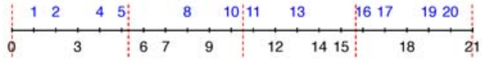
we have $\varphi(n) = k\varphi(k,q,n)$

so we know that *k* divides $\varphi(n)$. Clearly it is necessary for $\varphi(n)$ to be a multiple of *k* if we want the totatives distributed evenly. The question is, is it sufficient to guarantee uniform distribution?

Consider the case where *n*=21 and *k*=4. By Euler's formula,

$$\varphi(21) = \varphi(7*3) = \varphi(7)*\varphi(3) = (7-1)*(3-1) = 6*2 = 12$$

Clearly 4 divides 12, and we expect to see 3 totatives in each of the 4 subintervals if *k* dividing $\varphi(n)$ is the only necessary condition for uniform distribution. However, when we graph the given conditions we see that there are not an equal number of totatives in each subinterval



and we find that $E(4,0,21) = E(4,3,21) = -4$

$$E(4,1,21) = E(4,2,21) = 4$$

And so by (1) uniform distribution does not exist.

Results

Lehmer's results reveal, among other things, that

- If n is divisible by k^2 then n's totatives are uniformly distributed with respect to k
- $E(k,q,n) = \sum_{\delta|n} \left\{\delta + k\left[\frac{q\delta}{k}\right] - k\left[\frac{(q+1)\delta}{k}\right]\right\} \mu\left(\frac{n}{\delta}\right)$, which gives us that $E(k,0,n) = \sum_{\delta|n} r_k(\delta)\mu\left(\frac{n}{\delta}\right)$ for q=0 where r is the least positive remainder when δ is divided by k
- If a prime p of the form $kx + 1$ divides n, then the totatives of n are uniformly distributed with respect to k
- Additionally, Lehmer derives explicit formulas for determining $E(k,q,n)$ for the cases where $k = 3$, $k = 4$, and $k = 6$
- Explicit formulas are relatively difficult to derive. Further work has been done on this subject by Paul J. McCarthy and Paul Erdős.