Proceedings of the 3rd International Conference on Computing Innovation and Applied Physics
DOI: 10.54254/2753-8818/31/20241069

Research on Euler totient function equation $k\varphi(n) = n - 1$

Jiaqi Shi

Department of Mathematics, Sichuan University, Chengdu, China

shijiaqi_0927@163.com

Abstract. Let φ denote Euler's Totient function. There are some properties about $\varphi(n)$, when n is a prime or $n = p_1^{r_1} \cdots p_k^{r_k}$. The Euler's function equation, $k\varphi(n) = n - 1(1)$, where k is a positive integer, and n is a composite number, is called Lehmer's conjecture. Lehmer mentioned a series of properties of n that satisfy the equation in his own thesis and provided some proof. Afterwards, Ke Zhao and Sun Qi conducted further research. In previous studies, this conjecture was considered correct, but it is difficult to prove it. The case $k = 2$ has been discussed and proved that when $k = 2$ and $n = p_1p_2$,... p_i are different prime numbers. Also, some properties of the composite numbers that satisfy the equation have also been proven. Some conclusions can be proven, by using elementary number theory methods. Using these conclusions, we can conclue that when k=2, the solution of (1) is at least the product of 12 odd prime numbers.

Keywords: Number Theory, Euler Totient Function, Lehmer's Conjecture

1. Introduction

Euler Totient Function, $\varphi(n)$, is a number theory function defined on positive integers. For a positive integer n, the number of positive integers (including 1) that are less than or equal to n and are coprime with n is written as $\varphi(n)$. About the Euler Totient Function (Unless otherwise specified below, $\varphi(n)$ only refers to Euler Totient Function), some related equations have been proposed and discussed the solutions of these equations which is a significant topic in elementary number theory. Besides, around $\varphi(n)$, there have been rich conclusions and put forward many conjectures with contributions.

In 1932, Derrick Henry Lehmer proposed a conjecture that no composite number satisfies $\varphi(n) \mid n - 1$. In other words, for each positive integer k, $k\varphi(n) = n - 1$ has no solutions. In Lehmer's thesis [1], if n is a solution of (1), then n is a prime or the product of seven or more distinct primes. In 1963, K. Zhao and S. Qi proved that such a composite number n is at least the product of 12 different odd prime numbers [2]. Moreover, in 1980, Cohen and Haggis further proved that it is a product of at least 14 different odd prime numbers. In 2009, William D Banks and Florian Luca proved that such an n is at most $x^{1/2}/(\log x)^{1/2+o(1)}$ as $x \to +\infty$. Unfortunately, there is still no definitive answer to this question, but the academic community has come up with many reasonable conclusions. This article will discuss some n properties that can be derived from this equation and briefly discuss the case where $k = 2$.

This article will summarise some previous methods and use elementary methods to draw some conclusions for the case of $k = 2$.

DOI: 10.54254/2753-8818/31/20241069

2. Properties of n which satisfies the Equation

2.1. Readiness Knowledge

There are some basic theorems about Euler functions. [2] The Euler function is denoted by $\varphi(n)$.

Theorem 1. Let the standard decomposition formula of n be: $n = p_1^{r_1} p_2^{r_2} \cdots p^{ar_k}$, then,

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) \tag{1}$$

To prove Theorem 1, it is needed to prove some inferences and theorems. Intuitively, the correctness of this theorem is obvious. For example, let n be $24 = 3 * 2^3$, the reduced residue system $(1 \le r \le n)$ is $\{1,5,7,11,13,17,19,23\}$, hence $\varphi(24) = 8$, and using the formula above, $\varphi(24) = 24\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 8$. However, to prove this theorem, some pre-conclusions are needed. Here are two lemmas given without proof.

Lemma 1. Let $n \ge 1$, then:

$$\sum_{(d|n)} \varphi(d) = n \tag{2}$$

Lemma 2. Let$(m, n) = 1$, $T_1 := \{t_1 : t_1 \mid m\}$, $T_2 := \{t_2 : t_2 \mid n\}$, then $T = \{t_1 t_2 : t_1 \in T_1, t_2 \in T_2\}$ includes all the factors of mn. In other words, $T = \{t : t \mid mn\}$.

Then there is the theorem:

Theorem 2. Let$(m, n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$.

Proof. Let $h = mn$, using induction method: if $h = 1$, it is obvious; suppose that if $h = 1,2,\cdots, nm - 1$, the conclusion is valid, let $t|nm, t = t_1 t_2, t_1|m, t_2 \mid n$, by the assumption above, except for $t_1 = m, t_2 = n$, the equation $\varphi(t_1 t_2) = \varphi(t_1)\varphi(t_1)$ holds.

Hence, by Lemma 2,

$$\sum_{(t_1|m)} \varphi(t_1) \sum_{(t_2|n)} \varphi(t_2) = \left(\sum_{(t|mn)} \varphi(t) - \varphi(mn)\right) + \varphi(m)\varphi(n) \tag{3}$$

From Lemma 1, $mn = \big(mn - \varphi(mn)\big) + \varphi(m)\varphi(n)$, which is equivalent to $\varphi(mn) = \varphi(m)\varphi(n)$.

So, Theorem 1 can be proved.

The proof of Theorem 1. From Theorem 2,

$$\varphi(n) = \varphi\big(p_1^{\alpha_1}\big) \cdots \varphi\big(p_k^{\alpha_k}\big). \tag{4}$$

Then, it is just needed to prove $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. From the definition of $\varphi(n), \varphi(p^\alpha) = p^\alpha - \sum_{i \in I} i, I = \{i \mid i \text{ and } p \text{ are mutually prime }\} = \{i \mid i \text{ is a multiple of } p\}$. At the same time, the number of multiples of p from 1 to p^α is $p^{\alpha-1}$, hence $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Meanwhile, here is another theorem.

Theorem 3.

1.Let $(m, n) = d$, then $\varphi(mn) = \varphi(m)\varphi(n) \cdot \frac{d}{\varphi(d)}$.

2. If $a \mid b$, then $\varphi(a) \mid \varphi(b)$.

Proof. (1)

DOI: 10.54254/2753-8818/31/20241069

$$\frac{\varphi(mn)}{mn} = \prod_{(p|mn)}\left(1-\frac{1}{p}\right) = \frac{\prod_{(p|m)}\left(1-\frac{1}{p}\right)\prod_{(p|n)}\left(1-\frac{1}{p}\right)}{\prod_{(p|(m,n))}\left(1-\frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}} \quad (5)$$

Thus $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$.

(2) Let $b = ac$, from (1), $\varphi(b) = \varphi(ac) = \varphi(a)\varphi(c)\frac{d}{\varphi(d)} = d\varphi(a)\frac{\varphi(c)}{\varphi(d)}$, where $(a, c) = d$.

Since $d \mid c$, $\frac{d\varphi(c)}{\varphi(d)} = \frac{c\prod_{p|c}\left(1-\frac{1}{p}\right)}{\prod_{p|d}\left(1-\frac{1}{p}\right)}$ is an integer(because the factors of c include the factors of d). Hence $\varphi(a) \mid \varphi(b)$.3

2.2. Lehmer's Conjecture

There has been systematic research in the academic community on the properties of Euler Totient Functions and their divisibility with some other functions. In 1932, an American mathematician, Derrick Henry Lehmer, supposed a conjecture:

Proposition 1. There is no composite number n such that:

$$\varphi(n) \mid n-1.$$

As mentioned earlier, it is tough to solve this problem completely, but some n properties can be obtained. Firstly, in case $k = 1$, it is evident that n satisfies (1) is equivalent to n is a prime. Thus, consider k as an integer greater than 1 in the following discussion.

Theorem 4. Let $k \geq 2, k\varphi(n) = n-1$, then:

1. n is the product of different odd prime numbers.
2. If odd prime p satisfies $p \mid n$, then n does not contain prime factors in the form of $pt+1$.
3. If $k \not\equiv 1(\bmod 3)$, then $n \not\equiv 0(\bmod 3)$.

Proof. Since $k \geq 2$, then $n > 2$, and since $2 \mid \varphi(n)$, so $2 \nmid n$; if prime $p \mid n, n$ has prime factors with the form $pt+1$ or $p^2 \mid n$, $p \mid \varphi(n)$, thus $p \mid n-1$ (because $k\varphi(n) = n-1$), and it is impossible. So, the first and the second conclusion can be proved.

When $k \equiv 0(\bmod 3)$, the conclusion is right. When $k \equiv 2(\bmod 3)$, if $n \equiv 0(\bmod 3)$, assume $n = p_1 \cdots p_s, p_1 = 3, p_2, \cdots, p_s$ are different odd prime numbers. Thus,

$$2k\prod_{j=2}^{s}(p_j - 1) = 3\prod_{j=2}^{s}p_j - 1,$$

And from conclusion 2, $p_j \equiv -1(\bmod 3)$, and module 3, then:

$$1 \equiv 2(\bmod 3),$$

And it is impossible.

Thus:

Inference 1. If n satisfies (I) and $n = p_1 \cdots p_s$, then:

$$\varphi(n) = \prod_{i=1}^{s}(p_i - 1) \quad (6)$$

Proof. Obviously.

First, discuss a simple case where $k = 2$ and n is the product of two prime numbers:

$$2\varphi(n) = n-1.$$

DOI: 10.54254/2753-8818/31/20241069

It is equivalent to:

$$\begin{aligned} 2(p_1-1)(p_2-1) &= p_1p_2-1, \\ p_1p_2-2(p_1+p_2)+3 &= 0 \\ (p_1-2)(p_2-2) &= 1. \end{aligned}$$

Thus, $p_1 = p_2 = 3$ is impossible because p_i are different prime numbers. Similarly, it can be proved that when $n = p_1p_2p_3$, no n satisfies $2\varphi(n) = n-1$.

Moreover, here is another theorem proved by K. Zhao [3].

Theorem 5. Let n satisfy (1) and $n = p_1 \cdots p_s$, then:

$$k < \prod_{i=1}^{s} \frac{p_i}{p_i - 1} \tag{7}$$

Proof. From (1) and Inference 1:

$$k\prod_{i=1}^{s} p_i - 1 = \prod_{i=1}^{s} p_i - 1$$

Thus,

$$k = \prod_{i=1}^{s} \frac{p_i}{p_i-1} - \prod_{i=1}^{s} \frac{1}{p_i-1} < \prod_{i=1}^{s} \frac{p_i}{p_i-1}.$$

By theorem 5, it can be directly obtained:

Inference 2. If $n = p_1 \cdots p_s, s \leq 11$ is a solution of (1), then $k = 2$ or $k = 3$.

Proof. From (2),

$$\begin{aligned} k &< \prod_{i=1}^{s} \frac{p_i}{p_i-1} \\ &\leq \frac{3}{2}\cdot\frac{5}{4}\cdot\frac{7}{6}\cdot\frac{11}{10}\cdot\frac{13}{12}\cdot\frac{17}{16}\cdot\frac{19}{18}\cdot\frac{23}{22}\cdot\frac{29}{28}\cdot\frac{31}{30}\cdot\frac{37}{36} < 4 \end{aligned}$$

Thus, $k = 2$ or $k = 3$.

Through a proof process and calculation process similar to the above proof, the following theorem can be proved:

Theorem 6. If $k = 2$, the solution (1) is at least the product of 12 odd prime numbers.

3. Conclusion

When $k = 2$, the solution of (1) is at least the product of 12 odd prime numbers. Using computers, it can be reached that when $k = 2$, the solution is at least the product of 14 or more prime numbers. Unfortunately, it is not easy to push the conclusion to positive infinity, to completely solve the conjecture, in addition to the methods of elementary number theory, some analytical methods of number theory are necessary. William D Banks and Florian Luca's thesis [4] proved that $\#L(x) << x^{1/2}\log x^3/4$., where L(x) is the solution set of (1), which provides a significant method of researching this problem. Meanwhile, G Tenenbaum provided some relevant research on analytical number theory [5].

DOI: 10.54254/2753-8818/31/20241069

References

[1] DH Lehmer. On euler's totient function. 1932.
[2] Godfrey Harold Hardy and Edward Maitland Wright. An introduction to the theory of numbers. Oxford university press, 1979.
[3] K.Zhao and S.Qi. On equation $k\varphi(n) = n - 1$. Journal of Sichuan University (Natural Science Edition), pages 13-21, 1963.
[4] Florian Luca and Carl Pomerance. On composite integers n for which $\phi(n) \mid n - 1$. Bol. Soc. Mat. Mexicana, 17(3):13-21, 2011.
[5] G Tenenbaum. Cambridge stud. adv. math. 46, 1995.