The Investigation of Euler's Totient Function Preimages for $\varphi(n) = 2^m p_1^\alpha p_2^\beta$ and the Cardinality of Pre-totients in General Case

RUSLAN SKURATOVSKII
Interregional Academy of Personnel Management Kiev, and
National Aviation University, Kiev
and Igor Sikorsky Kiev Polytechnic Institute
Kyiv, UKRAINE

Abstract: This paper shows how to determine all those positive integers x such that $\varphi(x) = m$ holds, where x is of the form $2^a p^b q^c$ and p, q are distinct odd primes and $a, b, c \in \mathbb{N}$.
In this paper, we have shown how to determine all those positive integers n such that $\varphi(x) = n$ will hold where n is of the form $2^a p^b q^c$, where p, q are distinct odd primes and $a, b, c \in \mathbb{N}$. Such n are called pre-totient values of $2^a p^b q^c$. Several important theorems along with subsequent results have been demonstrated through illustrative examples.
We propose a lower bound for computing quantity of the inverses of Euler's function. We answer the question about the multiplicity of m in the equation $\varphi(x) = m$ [1]. An analytic expression for exact multiplicity of $m = 2^{2^n+a}$, where $a \in N$, $a < 2^n$, $\varphi(x) = 2^{2^n+a}$ was obtained. A lower bound of inverses number for arbitrary m was found. We make an new approach to Sierpinski assertion.

Key-Words: Inverses of Euler's totient function, prime numbers, number of pre-totients of Euler's totient function, lower bound of the inverses of Euler's function.

Received: April 7, 2021. Revised: December 22, 2021. Accepted: January 17, 2022. Published: February 9, 2022.

1 Introduction

The Euler totient function $\varphi(n)$ for $n \in N$ is the total number of positive integers which are less than n and coprime with n.

Let n be a positive integer. Then the set Z_n^* containing the positive integers less than or equal to n and relatively prime to n forms a group under multiplication modulo n and the order of this group is denoted by $\varphi(n)$, known as Euler's phi function or the totient function. For example, $Z_8^* = \{1, 3, 5, 7\}$and So $\varphi(8) = 4$. Similarly, $\varphi(11) = 10$ because $Z_{11}^* = \{1, 2, \dots, 10\}$.

In number theory and abstract algebra, Euler's phi function plays a major role in several aspects. There are several important properties and rules to determine the value of $\varphi(n)$ for given $n \in \mathbb{N}$ which can be found in many standard text books related to number theory.

(1) If a, b are relatively prime integers, then $\varphi(ab) = \varphi(a)\varphi(b)$. An immediate consequence of this property is, $\varphi(2^e m) = \varphi(2^e)\varphi(m)$ provided $m \in \mathbb{N}$ is odd and $e \in \mathbb{N}$.

This is an application of our theorem on the number of solutions to an equation with the Euler function i.e. search for the preimage of the Euler function in cryptography. Since p and q are prime numbers, then $\varphi(pq) = \varphi(n) = (p-1)(q-1)$, where $\varphi(x)$ is the Euler function. From the condition of choosing the key d as mutually inverse to e we have: $de(mod\varphi(n)) \equiv 1$, or $de = k\varphi(n) + 1$ for some natural k. Then using Euclid algorithm one can find secret key d. Solving the last equation with respect to d, we actually find the secret key in algorithm RSA [24]. Therefore, in order for this equation to be solved, it is extremely necessary that the possible solutions, i.e. the pre-totients of the function $\varphi(n)$, be as large as possible. Therefore, it is important for us to learn to choose such $n = pq$ that the set $\varphi^{-1}(n)$ is as large as possible for numbers n of this order. To find $\varphi(n)$ we can consider the Sylow p_1-subgroup and Sylow q_1-subgroup of Z_n^* and compute their orders, where pq is divisible on p_1 and Q_1. Orders of p_1-subgroup and q_1-subgroup [16, 18, 17, 19] of Z_n^* depends from its structure and multiplicity p_1 and q_1 in $p-1$ and $q-1$ because of $ord(Z_n^*) = (p-1)(q-1)$.

2 Preliminaries and Notifications

In order to make the presentation simpler, we shall make use of the following symbols. For $a, b, n \in \mathbb{N}$,
$\mathbb{N}_n = \{1, 2, ..., n-1, n\}$,
${}_a\mathbb{N}_b = \{a, a+1, a+2, ..., b-1, b\}$,
${}_a\mathbb{N}_n = \{x \in \mathbb{N} : x \geq a\}$,
$\mathbb{W}_n = \{1, 2, ..., n-1, n\}$,
$\mathbb{W} = \{0\} \cup \mathbb{N}$,

$\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ is a prime number}\}$.

We shall use the symbol $|S|$ to denote the number of elements of the set S. When a positive integer $|x|$ is given, one can compute $\varphi(x)$ easily. But when $\varphi(x)$ is given, determination of x becomes comparatively a difficult task. Here the values $\varphi(x)$ is called a totient number whereas its preimage x under φ is called a pre-totient. Corresponding to a given $n \in \mathbb{N}$, the collection of all pre-totients of n under φ is denoted by $\varphi^{-1}(n)$ i.e. $\varphi^{-1}(n) = \{r \in \mathbb{N} : \varphi(r) = n\}$.

For example, $\varphi^{-1}(2) = \{3, 4, 6\}$. The number 14 has no pre-totients and so $\varphi^{-1}(14)$ is empty set. Moreover, if $n > 2$ is odd, then $\varphi^{-1}(n)$ is an empty set because of the set property 4 given above.
In [2], a general process to determinate the set $\varphi^{-1}(n)$ is discussed along with an example for $n = 576$. However the process demands the assumption that all $\varphi^{-1}(x)$ where $x < 576$ must be known beforehand. Once this table is prepared, the actual determination starts. Another set of works can be found in [2] and [11]. In [11] the determination is done through algorithm, which way become tedious job when n will become severely bigger. In [2] works of determination of pre-totients of some particular cases like $n = 2p, 2^k p$ where p is odd prime have been made. Carmichael showed his process for determination of pre-totients of the number of the form 2^m in [4]. We also did his work on the same set $\varphi^{-1}(2^{2n} + a)$ in our work in arxiv [12].

In this paper we are considering those n that have the form $n = 2^a p_1^{a_1} p_2^{a_2}$, where a, a_1, $a_2 \in N$ and $p_1 < p_2$ are distinct odd primes in an alternative manner. To proceed further, we assume that $x \in \phi^{-1}(n)$. Then x is either even or odd positive integer. For $n \in N$, we take into account the following partition into two sets introduced in [2].

$$E(n) = x \in \varphi^{-1}(n) : x \equiv 0(\text{mod}2) \qquad (1)$$

$$O(n) = x \in \varphi^{-1}(n) : x \equiv 1(\text{mod}2) \qquad (2)$$

Clearly, $\varphi^{-1}(n)$ is disjoint union of $E(n)$ and $O(n)$. Moreover, the set of $O(n)$ is empty provided n is odd. In this case, $\varphi^{-1}(n) = E(n)$. In [2] it is derived that cardinalities of the set $O(2s)$ and $E(2s)$, where s is odd positive integer are equal. We now start with the first case $x \in E(2^a p_1^{a_1} p_2^{a_2})$.

3 Problem Formulation

The aim of this work is to study theoretical numerical properties of the multivalued inversed to Euler's function [13, 14], demonstrate the relevance of the examples.

Subject of study: explore the composition of the function $\varphi(n)$ with itself and the tasks associated with it, it's properties, the number of preimages of the function $\varphi(n)$, behavior of the straight $O(A_n)$, where $A_n(n; \varphi(n))$ and $O(0; 0)$ where $n \to \infty$ [23].

Using Lenstra's factorization method we have deal with group of curve point isomorphic to multiplicative group of ring Z_n which has order $\varphi(n)$. Hence, it is important to know size set of pre-totients for $\varphi(n)$ to choose suitable curve [22, 23].

We going to find a lower estimation for computing quantity of the inverses of Euler's function. Our approach can be further adapted for computing certain functions of the inverses, such as their quantity, the larger.

Of fundamental importance in the theory of numbers is Euler's totient function $\varphi(n)$. Two famous unsolved problems concern the possible values of the function $A(m)$, the number of solutions of $\varphi(x) = m$, also called the multiplicity of m. Of big importance in the cryptography has number of pre-totients of Euler's totient function $\varphi(n)$, $n = pq$. Because it determines cardinal of secret key space in RSA [24].

4 Main result about solution of $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$.

Firstly, we consider the case $x \in E(2^a p_1^{a_1} p_2^{a_2})$.

Theorem 4.1. Let $x \in E(2^a p_1^{a1} p_2^{a_2})$. Then x can never be divisible by 2^P for all $p \in {}_{a+1}\mathbb{N}$.

Proof. Let's make the opposite assumption. Since $x \in E(2^a p_1^{a_1} p_2^{a_2})$, we write $x = 2^{a+r} m_0$ where $m_0 = 2k - 1$ and $k, r \in N$. Then $\varphi(x) = 2^a p_1^{a_1} p_2^{a_2}$ lead us to the contradiction:

$$2^{a+r-1}\varphi(m_0) = 2^a p_1^{a_1} p_2^{a_2}, \qquad (3)$$

$$2^{r-1}\varphi(m_0) = p_1^{a_1} p_2^{a_2}. \qquad (4)$$

In (4), if $r - 1 \in \mathbb{N}$, then left hand side is even number but right hand side is not, a contradiction. If $r - 1 = 0$ i.e. $r = 1$ then (4) reduces to $\varphi(m_0) = p_1^{a1} p_2^{a2}$. Since m_0 is odd, $m_0 = 1$ or $m_0 \geq 3$ will create contradiction in either way. This completes the proof.

Theorem 4.2. For $e \in \mathbb{N}_{\supset}$ the set $E(2^a p_1^{a_1} p_2^{a_2})$ contains elements of the form $2^e m_0$, where $m_0 \equiv 1(mod2)$ iff $m_0 \in O(2^{a+1-e} p_1^{a_1} p_2^{a_2})$.

Proof. Let $x = 2^e m_0$, where $e \in \mathbb{N}_a$ and m_0 is odd. Then $x \in E(2^a p_1^{a_1} p_2^{a_2})$ gives us the following chain of transformations: $2^{e-1}\varphi(m_0) = 2^a p_1^{a_1} p_2^{a_2}$ which implies that $\varphi(m_0) = 2^{(a+1)-e} p_1^{a_1} p_2^{a_2}$. Consequently we obtain $m_0 \in O(2^{(a+1)-e} p_1^{a_1} p_2^{a_2})$.

On the other hand, if

$$O(2^{(a+1)-e} p_1^{a_1} p_2^{a_2})$$

be non-empty for $e \in \mathbb{N}_a$ (we won't take $e = a+1$ since $O\left(p_1^{a_1}p_2^{a_2}\right)$ is empty set), then $x = 2^e m_0 \in E(2^a p_1^{a_1} p_2^{a_2})$. Hence the proof is completed.

Corollary 2.3. Let q^β be a divisor of $x \in \varphi^{-1}(2^a p_1^{\alpha_1} p_2^{\alpha_2})$, $q \in P\backslash\{2, p_1, p_2\}$. Then $\beta = 1$.

Proof. The proof follows from the opposite assumption that $n = 2^e q^\beta m \in \varphi^{-1}(2^a p_1^{\alpha_1} p_2^{\alpha_2})$, where $e \in W_a$, $m \equiv 1(\mathrm{mod}2)$ and $GCD\left(q, 2m\right) = 1$. Then, the initial number $n = 2^a p_1^{a_1} p_2^{a_2}$ can be presented in form of the product $2^a p_1^{a_1} p_2^{a_2} = 2^{e-1} q^{\beta-1}\left(q-1\right)\varphi\left(m\right)$. If $\beta - 1 \in N$ then desired contradiction is already reached.

Statement. If $m \in O(2^a p_1^{a_1} p_2^{a_2})$ then m contains no greater than a number of odd prime divisors.

Proof. Let $m \in O(2^a p_1^{a_1} p_2^{a_2})$. Then m is odd and evidently $m \geq 3$. Hence any prime divisor of m will be odd. Let the total number of such odd prime divisors of m be r. In other words, $r \in \mathbb{N}_a$.

Let the total number of such odd prime divisors of m be r. Then $2^r | \varphi\left(m\right)$ or equivalently $2^r | 2^a p_1^{a_1} p_2^{a_2}$. In other words, $r \in \mathbb{N}_a$ or putting it simply number of odd prime divisors of m is at most a.

Remark 4.1. Till October 2019 only Fermat's prime that have been discovered are F_0, F_1, F_2, F_3, F_4. From F_5 till F_{32} all composite. Primality of F_{33}, F_{34}, F_{35} is still an open problem. From F_{36}, some of the Fermat's numbers have been established as composite. See [5, 8, 9], for latest updates.

2.2 Let $m = p_1^{\beta_1} q_2$, then $\varphi(m) = 2^a p_1^{a_1} p_2^{a_2}$ will produce

$$2^a p_1^{a_1+1-\beta_1} p_2^{a_2} = (p_1 - 1)(q_2 - 1). \qquad (5)$$

Let e_1, e_2 are natural numbers. Evidently, $\beta_1 \in \mathbb{N}_{a_1+1}$ and $q_2 = \left(\frac{2^a p_1^{a_1+1-\beta_1} p_2^{a_2}}{p_1 - 1} + 1\right) \in P$. Moreover, if we assume

$$p_1 - 1 = 2^{e_1},$$

$$q_2 - 1 = 2^{e_1} p_1^{\gamma_{21}} p_2^{\gamma_{22}}$$

where

$$e_1, e_2 \in \mathbb{N}$$

and

$$\gamma_{21}, \gamma_{22} \in W$$

then

$$a = e_1 + e_2,$$

$$a_1 = \gamma_{21} + \beta_1 - 1,$$

$$a_2 = \gamma_{22}.$$

Once again, p_1 is a Fermat's prime $F_{e'_1}$ for some $2^{e'_1} \in \mathbb{N}_{a-1}$ and so $e_2 = a - 2^{e'_1}$. Consequently we can state.

Theorem 4.3. $m = p_1^{\beta_1} q_2 \in O(2^a p_1^{a_1} p_2^{a_2})$ provided

(1) $\beta_1 \in \mathbb{N}_{a_1+1}$,

(2) $p_1 = F_{e_1'}$ for $2_1^{e'} \in \mathbb{N}_{a-1}$ and this $p_1 \in$ P,

(3) $q_2 = 2^{a-2^{e_1'}} F_{e_1'}^{a_1+1-\beta_1} p_2^{a_2} + 1$ and such $q_2 \in$ P,

(4) p_1, q_2 satisfy equation $2^a p_1^{a_1+1-\beta_1} p_2^{a_2} = (p_1 - 1)(q_2 - 1)$ and $\varphi(m) = 2^a p_1^{a_1} p_2^{a_2}$.

The set of such numbers m has size at most $a_1 + 1$.

If we consider the case $\varphi^{-1}\left(n\right) \in E\left(n\right)$ and classify such values of $\varphi\left(n\right)$ by a quantity of prime multipliers, grater then 3 in $\varphi\left(n\right)$.

Now we consider the statement about number of solutions of equation $\varphi\left(n\right) = 2^m p_1^\alpha p_2^\beta$.

Theorem 4.4. If

$$\varphi\left(n\right) = 2^m p_1^\alpha p_2^\beta, \qquad (6)$$

then maximal number of solutions $n = 2 \cdot 3pq$ satisfying equation $\varphi\left(pq\right) = 2^m p_1^\alpha p_2^\beta$ equals to $m(\alpha + 1)(\beta + 1)$. The solutions have the following form:

$$p = 2^{m-m_1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P,$$

$$q = 2^{m_1-1} p_1^{\beta_1} p_2^{\beta_2} + 1 \in P.$$

Proof. Since we search solutions for numbers of the form $n = 2^k \cdot 3pq$. The process of Eulers function computation is determined by the formula:

$\varphi\left(2^k 3pq\right) = 2^{k-1} \cdot 2 \cdot (p-1)\left(q-1\right)$.

Implies that new non-zero power of 2 can contains in $p - 1$ and $q - 1$. But in our case $k = 1$. If we fix that $\varphi\left(n\right) = 2^m p_1^\alpha p_2^\beta$, then structure of dividers of n is the following:

$$m = m_1 + m_2,$$

$$\alpha = \alpha_1 + \alpha_2, \;\; \beta = \beta_1 + \beta_2$$

this follows from equations below

$$\varphi(n) = 2^m \cdot p_1^\alpha q_2^\beta,$$

$$m = m_1 + m_2,$$

$$\alpha = \alpha_1 + \alpha_2, \;\; \beta = \beta_1 + \beta_2,$$

$$p = 2^{m-m_1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P,$$

$$q = 2^{m_1-1} p_1^{\beta_1} p_2^{\beta_2} + 1 \in P,$$

$$n = 2 \cdot 3pq.$$

The number of solutions of $\varphi\left(n\right) = 2^m p_1^\alpha p_2^\beta$ is determined by number of partitions of m in 2 into terms from 0 to m, and there are such $C^1_{m+1} = m + 1$, but the present factor 3 takes 1 term in the power, since $\varphi(3) = 2$ of these two parts, so there are exactly m possibilities for the number of partitions. The number of partitions of the exponent αbetween powers [25] of the factors p and q into parts including the possibility of an empty part is total, including a degenerate partition with an empty part. Entirely similarly, we obtain the number of possible distributions of powers of the number p_2 is equal to $C^1_{\beta+1}$. The exact number of solutions is determined by the number of cases when the following two following conditions pertaining to set of prime of the numbers p and q are satisfied.

$$p = 2^{m-m_1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P,$$

$$q = 2^{m_1-1} p_1^{\beta_1} p_2^{\beta_2} + 1 \in P.$$

Verifying of the condition $\varphi(3pq) = 2^m p_1^{\alpha} p_2^{\beta}$ is providing with using of multiplicity of Euler's function $\varphi(pq) = \varphi(p)\varphi(q)$. The proof is completed. Corollary. In case of

$$n = 2pq,$$

if $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$, (1) then maximal number of equation solutions $\varphi(pq) = 2^m p_1^{\alpha} p_2^{\beta}$ equals to $m(\alpha+1)(\beta+1)$. The solutions have the following form:

$$\varphi(n) = 2^m \cdot p_1^{\alpha} q_2^{\beta}, \ \ m = m_1 + m_2,$$

$$\alpha = \alpha_1 + \alpha_2, \ \ \beta = \beta_1 + \beta_2,$$

$$p = 2^{m-m_1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P,$$

$$q = 2^{m_1} p_1^{\beta_1} p_2^{\beta_2} + 1 \in P.$$

The proof follows from proof of previous Theorem.

Remark 4.2. Minimal number of primes grater then 3 in solution of (1) is possible if one of multipliers factorized on powers of 2 and second multiplier that is $p_2 - 1 = 2^{m_2} p_1^x$.

Proof. The special case arise, when $p_2 - 1 = 2^{m_2} p_1^x$. This condition give us the next solution:

$$\varphi(n) = 2^m \cdot p_1^{\alpha_1}, \quad m = m_1 + m_2,$$

$$p = 2^{m-m_1} p_1^{\alpha_1-x} p_2^{\alpha_2-1} + 1 \in P,$$

$$q = p_2,$$

$$p_2 - 1 = 2^{m_1} p_1^x; \quad\ p_1, p_2 \in P.$$

Then $n = pq$ and $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$.

Secondly, it remains to consider the case $m \in O\left(2^a p_1^{a_1} p_2^{a_2}\right)$.

We consider the case $\varphi^{-1}(n) \in O(n)$– odd numbers and classify such values of $\varphi(n)$ by a quantity of prime multipliers. grater then 3 in $\varphi(n)$.

Theorem 4.4. (About number of solutions of equation $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$). If

$$\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$$

then maximal number of solutions $n = pq$ satisfying equation $\varphi(pq) = 2^m p_1^{\alpha} p_2^{\beta}$ equals to $(m+1)(\alpha+1)(\beta+1)$. The solutions have in general case the following form:

$$p = 2^{m-m_1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P,$$

$$q = 2^{m_1} p_1^{\beta_1} p_2^{\beta_2} + 1 \in P.$$

But in this case $m = m_1 = 0$.

Proof. Since we search first of all solutions for the numbers n used in RSA algorithm then it are numbers of the form $n = pq$. The process of Eulers function computation is determined by the general formula for $n = 3pq$: $\varphi(3pq) = 2 \cdot (p-1)(q-1)$. Implies that new non-zero power of 2 can contains in $p - 1$ and $q - 1$. If we fix that $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$, then structure of dividers of n is the following: $m = m_1 + m_2, \alpha = \alpha_1 + \alpha_2, \ \ \beta = \beta_1 + \beta_2$ this follows from the equations below

$$\varphi(n) = 2^m \cdot p_1^{\alpha} q_2^{\beta}, \ \ m = m_1 + m_2,$$

$$\alpha = \alpha_1 + \alpha_2, \ \ \beta = \beta_1 + \beta_2,$$

$$p = 2^{m-m_1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P,$$

$$q = 2^{m_1} p_1^{\beta_1} p_2^{\beta_2} + 1 \in P.$$

where $n = pq, \quad p, \ q \in P.$

The number of solutions of $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$ is determined by number of partitions of m in 2 into terms from 0 to m, and there are such $C^1_{m+1} = m + 1$, but the present factor 3 takes 1 term in the power, since $\varphi(3) = 2$ of these two parts, so there are exactly m possibilities for the number of partitions. The number of partitions of the exponent αbetween powers of the factors p and q into parts including the possibility of an empty part is total, including a degenerate partition with an empty part. Entirely similarly, we obtain the number of possible distributions of powers of the number p_2 is equal to $C^1_{\beta+1}$. The exact number of solutions is determined by the number of cases when the following two following conditions pertaining to set of prime of the numbers p and q are satisfied.

$$p = 2^{m-m_1-1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P,$$

$$q = 2^{m_1+1} p_1^{\beta_1} p_2^{\beta_2} + 1 \in P.$$

Let's check the condition $\varphi(pq) = 2^m p_1^{\alpha} p_2^{\beta}$ is carried out taking into account the multiplicative property of the Euler function $\varphi(3pq) = \varphi(p)\varphi(q) =$

$(2 \cdot 2^{m-m_1-1} 2 p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2})(2^{m_1} p_1^{\beta_1} p_2^{\beta_2}) = 2^m p_1^{\alpha_1+\alpha_2} p_2^{\beta_1+\beta_2}$. Let's notice, that $p,\ q \in P$ as well as their exponents as 3 adds another factor of 2.

Proposition 4.1 If $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$, then maximal number of solutions of the form $n = pq$ satisfying equation $\varphi(pq) = 2^m p_1^{\alpha} p_2^{\beta}$ equals to $(m+1)(\alpha+1)(\beta+1)$. Minimal number of primes grater then 2 in factorization of $p-1$ and $q-1$ is possible if one of multipliers is

$$p = 2^{m-m_1} p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} + 1 \in P$$

and second multiplier presents as $p_2 - 1 = 2^{m_2} p_1^x$. Proof. The special case arise when $p_2 - 1 = 2^{m_2} p_1^x$ gives us the result.

$$\varphi(n) = 2^m \cdot p_1^{\alpha_1}, \quad m = m_1 + m_2,$$

$$p = 2^{m-m_1} p_1^{\alpha_1-x} p_2^{\alpha_2-1} + 1 \in P,$$

$$p_2 - 1 = 2^{m_1} p_1^x; \qquad p_1, p_2 \in P,$$

$$q = p_2.$$

Then $n = pq$ and $\varphi(n) = 2^m p_1^{\alpha} p_2^{\beta}$.

We now start to classify odd preimages.

Theorem 4.5. Let q^{β} be a divisor of $x \in \phi^{-1}(2^a p_1^{a1} p_2^{a2})$, $q \in P \setminus \{2, p_1, p_2\}$. Then $\beta = 1$.

Proof. Let $a = 2eq^{\beta} m \in \phi^{-1}(2ap^{a_1} p_2^{a_2})$, where $e \in W_a$, q is relatively prime to $2m$ and m is odd. Then, $2^a p_1^{a_1} p_2^{a_2} = 2^{e-1} q^{\beta-1}(q-1)\phi(m)$. If $\beta^{-1} \in N$, then desired contradiction already arrived.

Theorem 4.6. If $m \in O(2^a p_1^{a1} p_2^{a2})$ then m contains at most a number of odd prime divisors.

Proof. Let $m \in O(2^a p_1^{a_1} p_2^{a_2})$. Then m is odd and evidently $\geqslant 3$. Hence any prime divisor of m will be odd. Let the total number of such odd prime divisors of m be r. Then $2r|\phi(m)$ i.e. $2r|2^a p_1^{a_1} p_2^{a_2}$. In other words, $r \in N_a$.

We denote the total number of distinct prime factors of $x \in \mathbb{N}$ by $\omega(x)$.

Theorem 4.7. If $m \in O\,(2^a p_1^{a_1} p_2^{a_2})$ and $\omega(m) = 1$ then m is one of the form

1. $p_2^{a_2+1}$ provided $p_2 = (2^a p_1^{a_1} + 1)$ for case $2^a p_1^{a_1} + 1 \in P$ holds,

2. q_3, where $q_3 = 2^a p_1^{a_1} p_2^{a_2} + 1$ for case $2^a p_1^{a_1} p_2^{a_2} + 1 \in P$.

We are going to find out the explicit forms of x when it is an odd element of the set $\varphi^{-1} 2^a p_1^{a_1} p_2^{a_2}$. By Theorem 4.5. $r \in \{1, 2, ..., a\}$, where r is a total number of odd prime divisor of $x = m \in O(2^a p_1^{a_1} p_2^{a_2})$. We discuss each case of r one by one.

4.7.1 If $r = 1$. In this case, m will be one of the forms

(1) $p_1^{\beta_1}$, $\beta_1 \in$ N,

(2)$p_2^{\beta_2}$, $\beta_2 \in$ N,

(3)$q_3^{\beta_3}$, $\beta_3 \in$ N, where $q_3 \in \mathbb{P} \backslash \{2, p_1, p_2\}$

4.7.1.2 Futhermore if $m = p_1^{\beta_1}$. Then $2^a p_1^{a_1} p_2^{a_2} = \varphi(p_1^{\beta_1}) = p_1^{\beta_1}(p_1 - 1)$ yields

$$2^a p_1^{a_1+1-\beta_1} p_2^{a_2} = (p_1 - 1)$$

The number in left side is divisible by $p_2^{a_2}$ but the number in right side is not. Hence, this case is rejected and so $m \neq p_1^{\beta_1}$.

4.7.1.3 If $m = p_2^{\beta_1}$, then

$$2^a p_1^{a_1} p_2^{a_2+1-\beta_2} = (p_2 - 1). \tag{7}$$

It is evident, $a_2 + 1 - \beta_1 \geq 0$. In other words, $\beta_2 \in \mathbb{N}_{a_2+1}$. If $\beta_2 < a_2 + 1$ then previous equation 7 lead us to contradiction. So, $\beta_2 = a_2 + 1$ and hence

$$2^a p_1^{a1} = (p_2 - 1) \tag{8}$$

which implies that

$$(p_2 = 2^a p_1^{a_1} + 1),\ and\ 2^a p_1^{a_1} + 1 \in \mathbf{P}, \tag{9}$$

if $2^a p_1^{a1} + 1$ is prime indeed, only then it will be taken under consideration as an eligible candidate in the set $\varphi^{-1}(2^a p_1^{a1} p_2^{a2})$.

Furthermore, equation (9) states if $p_2 \equiv 1\,(\text{mod}3)$, $p_1 \equiv 0\,(\text{mod}3)$ and therefore $p_2 = 2^a 3^{a_1} + 1$ and if $2^a 3^{a_1} + 1 \in P$ Thus, $m = p_2^{a_2+1} \in O\,(2^a p_1^{a_1} p_2^{a_2})$ provided (9) is satisfied equation.

4.7.1.4 $m = q_3^{\beta_3}$. According to Corollary 4.3 $\beta_3 = 1$, therefore $m = q_3$. By applying similar arguments as shown above, we shall get $q_3 = (2^a p_1^{a_1} p_2^{a_2} + 1) \in P$. In order words, if $2^a p_1^{a_1} p_2^{a_2} + 1$ be a prime, it will be an element of

$$\varphi^{-1}(2^a p_1^{a_1} p_2^{a_2}).$$

This completes the proof.

Example. Let $F_a < F_b$ be two distinct Fermat's primes and we consider the set $\varphi^{-1}(2F_aF_b)$. Here it is a routine work to show $F_b = 2F_a + 1$. So $F_b^2 \in \varphi^{-1}(2F_aF_b)$. Also, $2F_aF_b + 1 = 0(\text{mod } 3)$. Therefore, the cardinality of the set $\varphi^{-1}(2F_aF_b)$ is 0.

5 The cardinality of pre-totients for $\varphi(m)$.

We propose a exact formula for computing quantity of the inverses of Euler's function for any number of form 2^s.

An old conjecture of Sierpinski asserts that for every integer $k > 2$, there is a number m for which the equation $\varphi(t) = m$ has exactly k solutions the number of solutions t of $\varphi(t) = m$, also called the multiplicity of m. In this section we find multiplicity for numbers of form 2^s.

Example. The set of preimages for 12 is following: $\phi^{-1}(12) = \{13, 21, 26, 28, 36, 42\}$. Also we have $\varphi^{-1}(16) = \{32, 48, 17, 34, 40, 60\}$, $\varphi^{-1}(18) = \{19, 27, 38, 54\}$. We remind, that the number of a form $2^{2^n} + 1$, where n is not-negative integer, is called Fermat number.

Also the recursive formula for Fermat numbers [13, 15, 18, 20] was used: $F_n = F_0 ... F_{n-1} + 2$. Besides Useful for the study of the number of prototypes is Lucas's Theorem: each prime divisor of the Fermat number F_n, where $n > 1$, has a form of $k2^{n+2} + 1$.

Lemma. If $2^m + 1$ is prime, then $m = 2^n$.

Proof. We will prove by contradiction. Suppose there exists a number of a form $2^m + 1$ which is not prime and m is divisible by $p \neq 2$. Since p is prime and it is not 2, it must be odd. Let $m = pt$, so we can rewrite our number like this: $2^m + 1 = (2^t)^p + (1)^p = (2^t + 1)\left((2^t)^{p-1} - ... + (1)^{p-1}\right)$. Expressions in both brackets are grater than 1, but our number is supposed to be prime. Contradiction.

We make of use Theorem about mutually primality of non-prime Fermat number [20].

Theorem 5.1. Let $n \in N \cup \{0\}$. If $2^{2^n} + 1$ is not prime, then for any number of the form 2^{2^n+a}, where $a \in N$, $a < 2^n$, there exists exactly 2^t natural numbers m such that $\varphi(m) = 2^{2^{n+a}}$, where t is amount of prime Fermat numbers, which are less than $2^{2^n} + 1$.

Proof. Consider a set $\{p_1, p_2, ...p_t\}$ of all prime Fermat numbers lesser than $2^{2^n} + 1$. Let $\varphi(x) = 2^{2^n+a}$. According to Lemma 1, $x = 2^s q_1 q_2 ... q_v$, where q_i are different prime Fermat numbers. Since $a < 2^n$, then $2^{2^n+a} < 2^{2^{n+1}}$. That means, that $q_i < 2^{2^{n+1}} + 1$, because $\varphi(x) = \varphi(2^s q_1 q_2 ... q_v) = 2^{2^n+a} < 2^{2^{n+1}}$.

We also know that $q_i \neq 2^{2^n} + 1$, because $2^{2^n} + 1$ is not prime. This yields $q_i < 2^{2^n} + 1$. Other words it can be written like this: $\{q_1, q_2, ...q_v\} \subseteq \{p_1, p_2, ...p_t\}$. For each x we get, that $\{q_1, q_2, ...q_v\}$ is a subset of the set $\{p_1, p_2, ...p_t\}$. We shall prove, that each subset of the set $M_t = \{p_1, p_2, ...p_t\}$ determines such unique x as a unique product of this subset of primes from M_t, that x with a corresponding multiplier 2^s, $s \in N \cup \{0\}$ gives us $x = 2^s t$ such that $\varphi(x) = 2^{2^n+a}$.

For this goal we need to show, that $\varphi(p_1 \cdot p_2 \cdot ...p_t) < 2^{2^n+a}$.

Since $\varphi(p_1 \cdot p_2 \cdot ...p_t)$ is Euler's function of a product of prime Fermat numbers, which lesser than $2^{2^n} + 1$, it is not grater than value of Euler's function of a product of all Fermat numbers, which lesser than $2^{2^n} + 1$, which is equal to

$$\varphi\left(\left(2^{2^0} + 1\right) ... \left(2^{2^{n-1}} + 1\right)\right).$$

That is true, as obvious inequality holds: $\varphi(d) \leq \varphi(db)$. It is also known, that any two Fermat numbers are coprime [20], so

$$\varphi\left(\left(2^{2^0} + 1\right) ... \left(2^{2^{n-1}} + 1\right)\right) =$$

$$= \varphi\left(2^{2^0} + 1\right) ... \varphi\left(2^{2^{n-1}} + 1\right).$$

As known, $\varphi(y) \leq y - 1$, therefore

$$\varphi\left(2^{2^0} + 1\right) ... \varphi\left(2^{2^{n-1}} + 1\right) \leq$$

$$\leq \left(2^{2^0} + 1 - 1\right) \cdot ... \cdot \left(2^{2^{n-1}} + 1 - 1\right) =$$

$$= 2^0 \cdot ... \cdot 2^{2^{n-1}} = 2^{2^n-1}.$$

It was used the formula of the sum of geometric progression, we have $2^0 + 2^1 + ... + 2^{n-1} = 2^n - 1$. Therefore $\left(2^{2^0} + 1 - 1\right) \cdot .. \cdot \left(2^{2^{n-1}} + 1 - 1\right) = 2^{2^0+2^1+..+2^{n-1}} = 2^{2^n-1}$.

Finally,

$$\varphi(p_1 \cdot p_2 \cdot ...p_t) \leq 2^{2^n-1} < 2^{2^n+a},$$

what was needed. That means, that Euler's function of the product of the elements of any subset of the set $\{p_1, p_2, ...p_t\}$ is lesser than 2^{2^n+a}. Let us take an arbitrary subset of $\{p_1, p_2, ...p_t\}$. Let the elements of this set be $\{q_1, q_2, ...q_v\}$. Consider the expression $\varphi(q_1 \cdot q_2 \cdot ... \cdot q_v) = 2^w < 2^{2^n+a}$. This inequality means, that we can choose such natural number s, so $\varphi(2^s \cdot q_1 \cdot q_2 \cdot ... \cdot q_v) = 2^{s-1} \cdot 2^w = 2^{2^n+a}$. In other words, for given subset $\{q_1, q_2, ...q_v\}$, we found such number x, that $\varphi(x) = 2^{2^n+a}$. The last equality means, that each subset defines unique x.

Therefore, each subset gives us the needed the number x that is always determined by some subset. In other words, the amount of needed numbers is exactly the amount of different possible subsets. As well-known fact, this amount is equal 2^t for a set of t elements.

Example. For a non-prime Fermat number $2^{32}+1$, number of preimages for subsequent numbers of the form 2^{2^n+a}, $a \leq 32 - 1$, $n \leq 4$ is equal to 2^{32}.

For generalizing of Theorem 5.1 it is convenient to prove the following statement:

Theorem 5.2 Let $a \in Z$, $0 \leq a \leq 2^n$, then the number of solutions of $\varphi(x) = 2^{2^n+a}$ is equal to the number of sets $\{2^{i_1}, ..., 2^{i_k}\}$, such that: $i_1 < i_2 < ... < i_k$

$2^{i_1} + 2^{i_2} + ... + 2^{i_k} \leq 2^n + a$,
$2^{2^{i_1}} + 1, ..., 2^{2^{i_k}} + 1 \in F_{pr}$,
where F_{pr} is a set of Ferma's prime numbers.

If $2^{2^n}+1$ is not prime, then the number of specified sets (including empty set) is equal to 2^t, where t is a number of Ferma's prime numbers smaller then $2^{2^n} + 1$.

Proof. To construct the necessary preimage x over the set of Ferma's primes with the properties of this Theorem $\varphi(x) = 2^{2^n+a}$ we proceed as follows:

1) We choose a combination of this numbers. Let us call it

$$\left(2^{2^{i_0}}+1\right)...\left(2^{2^{i_{k-1}}}+1\right).$$

2) Then we should find its total power of 2 that is $2^{i_1} + 2^{i_2} + ... + 2^{i_k} = s$, this power be obtained after calculating the Euler's function from the product $\varphi\left(\left(2^{2^{i_0}}+1\right)...\left(2^{2^{i_k}}+1\right)\right)$ and also satisfies the inequality

$$s = 2^{i_1} + 2^{i_2} + ... + 2^{i_k} \leq 2^n + a.$$

We supplement the received power exponent s to the necessary $2^n + a$ by multiplying the product of

$$\left(2^{2^{i_0}}+1\right)...\left(2^{2^{i_k}}+1\right)$$

on 2^{2^n+a-s}. Thus, the necessary preimage x is constructed.

Property. For any number S of the form $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k},\ p_1 > 2$, where $p_1, p_2, ..., p_k$ are odd prime numbers, the following equality holds: $\varphi(S) = \varphi(2S)$.

Proof. Since 2 and $p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k},\ p_1 > 2$ are coprime, then

$$\varphi\left(2p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}\right) = \varphi(2)\,\varphi\left(p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}\right) =$$
$$= \varphi\left(p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}\right).$$

Therefore these numbers has the same of Euler's function.

6 The lower bound for $\varphi^{-1}(m)$.

We suggest a lower bound estimate for computing quantity of the inverses of Euler's function. Our approach can be further adapted for computing certain functions of the inverses, such as their quantity, the larger.

Definition 6.1 Let M_k be a set of first k consecutive primes. We will say, that the number is *decomposed over a set* M_k, if in its canonical decomposition there are only numbers from M_k. Let $x_1, \dots, x_{n+2}$ be such numbers, that $\varphi(x_1) = \varphi(x_2) = ... = \varphi(x_{n+2})$, and at the same time all prime factors of the canonical decomposition belong to the set $M_n = \{p_0, ..., p_n\}$, where $p_0 = 2$ and p_i are all consecutive prime numbers. Let for any natural number n, **we define** $Q_n = (p_0 - 1)(p_1 - 1)...(p_{n-1} - 1)(p_n - 1)$, where p_i is i-th odd prime number, where $i \in N$ and $p_0 = 2$.

Example: $p_1 = 3, p_2 = 5, p_3 = 7$, then $Q_3 = (p_0 - 1)(p_1 - 1)(p_2 - 1)(p_3 - 1) = (3 - 1)(5 - 1)(7 - 1) = 48$.

So the first presentation of 48 over M_3 has canonical form $\varphi(3 \cdot 5 \cdot 7) = 2 \cdot 2^2 \cdot 2 \cdot 3 = 48$, and rest 4 presentations of 48 over M_3 are the following:
$\varphi(2^4 \cdot 3^2) = 2^3 \cdot 3 \cdot 2 = 48$,
$\varphi(5 \cdot 9 \cdot 2^2) = 3 \cdot 2^4 = 48$,
$\varphi(7 \cdot 5 \cdot 2) = 3 \cdot 2^4 = 48$,
$\varphi(7 \cdot 2^4) = 3 \cdot 2^4 = 48$,
thus, we obtain **5 presentations** for Q_3.

Let M_k be a set of k consequent first prime numbers. The following statement about estimation of pre-totients number is true.

Theorem 6.1 For each natural $n \in \mathbb{N}$ there is a set of such various natural numbers
$x_1, x_2, ..., x_n, x_{n+1}, x_{n+2}$, that

$$\varphi(x_1) = \varphi(x_2) = ... = \varphi(x_{n+2}) = Q_n,$$

where every number x_i contains in its canonical decomposition [20] only p_i from M_n (i.e. $p_i < p_n$ if $i < n$), and

$$x_{n+2} = p_0 p_1 ... p_{n-1} p_n$$

holds.

Proof. We prove it by the mathematical induction.

Base case: given $n = 1$, then $P_1 = (p_1 - 1) = 2$ has at least three preimages. This statement is true, because $\varphi(3) = \varphi(4) = \varphi(6) = 2 = Q_2$. The base case is proved.

Step case: if for $n = k$ it holds, we will prove, that for $n = k + 1$ it holds too. By the assumption we have, that for natural number n were found such various natural $x_1, x_2, ..., x_{k+1}, x_{k+2}$, that

$$\varphi(x_1) = \varphi(x_2) = ... = \varphi(x_{k+1}) =$$
$$= \varphi(x_{k+2}) = Q_k = Q,$$

where $Q_k = p_0^{\beta_0} p_1^{\beta_1} ... p_k^{\beta_k}$,

$$x_{k+1} = p_1 p_2 ... p_{k-1} p_k,\ x_{k+2} = p_0 p_1 p_2 ... p_{k-1} p_k.$$

Let us make induction transition. Prove, that for $n = k + 1$ exist such various natural $y_1, y_2, ..., y_{k+2}, y_{k+3}$, for which holds:

$$\varphi(y_1) = \varphi(y_2) = \ ... \ =$$
$$= \varphi(y_{k+2}) = \varphi(y_{k+3}) = Q_{k+1}, \qquad (10)$$

each of which has a canonical decomposition over $M_k \cup p_{k+1}$. Clear, that $\varphi(p_{k+1})$ has a canonical decomposition into elements of M_k because of all previous primes are in M_k and $\varphi(p_{k+1}) < p_{k+1}$.

Therefore, it can be presented as

$$\varphi(p_{k+1}) = p_0^{\beta_0} p_1^{\beta_1} \dots p_k^{\beta_k}.$$

Let's construct new numbers $y_1, y_2, \dots, y_{k+1}, y_{k+2}, y_{k+3}$ in such a way:

$$y_1 = x_1 p_{k+1},\ y_2 = x_2 p_{k+1},\ \dots, y_{k+1} =$$

$$= x_{k+1} p_{k+1},\ y_{k+2} = x_{k+2} p_{k+1}.$$

In this case, the value of the Euler function is $Q_{k+1} = p_0^{\beta_0} p_1^{\beta_1} \dots p_k^{\beta_k}$. Let us show, that all $y_1, \dots, y_{k+2}, y_{k+3}$ are different.

Since numbers $x_1, x_2, \dots, x_{k+1}, x_{k+2}$ from (1) have different canonical decompositions, so the decompositions of numbers $y_1, y_2, \dots, y_{k+1}, y_{k+2}$ over M_k are different too, but they all have a new factor p_{k+1}, but do not decompose over M_k. A last one y_{k+3} also decomposes over M_k and does not contain a factor p_{k+1}. But value $Q_{k+1} = p_0^{\beta_0} p_1^{\beta_1} \dots p_n^{\beta_n}$ does not contain p_{k+1} in the decomposition, so there is at least one number y_{k+3} with decomposition over M_k, such, that $\varphi(y_{k+3}) = Q_{k+1}$ holds.

Since $Q_{k+1} > Q_k$, then a new preimage y_{k+3} does not coincide with any of the numbers $y_1, y_2, \dots, y_{k+1}, y_{k+2}$ which give the value of Euler's function equal Q_k.

Moreover such y_{k+3} can be not unique number that can be constructed over M_k such, that $\varphi(y_{k+3}) = Q_{k+1}$. Consequently beyond $y_1, y_2, \dots, y_{k+1}, y_{k+2}$, which decomposed over M_{k+1}, we have at least one new y_{k+3}, which can be decomposed over M_k in product of primes. Thus Q_{k+1} has at least $k+3$ different preimages.

We propose method of constructing of such pretotients set.

Let $p_0 = 2, p_1 = 3, p_2 = 5, \dots, p_n$ be consecutive prime numbers, where $n = k+1$. Note, that $\varphi(p_0 p_1, \dots, p_n) = (p_0 - 1)(p_1 - 1)\dots(p_n - 1)$. Let us construct some new numbers $x_0, \dots, x_n$, for which $\varphi(x_0) = \varphi(x_1) = \dots = \varphi(x_n) = \varphi(p_0, p_1, \dots, p_n) = (p_0 - 1)(p_1 - 1)\dots(p_n - 1)$. Namely, let

$x_0 = (p_0 - 1)p_0, \dots, p_n$,
$x_1 = p_0(p_1 - 1)p_2, \dots, p_n$,
$\dots$
$x_n = p_0 p_1, \dots, p_{n-1}(p_{n-1} - 1)$.

Now we will prove, that $\varphi(p_0 p_1 \dots p_{k-1}(p_k - 1)p_{k+1} \dots p_n) = (p_0 - 1)(p_1 - 1)\dots(p_n - 1)$ for every $k \in \{0, 1, \dots, n\}$. Obviously, $p_0 \dots p_{k-1}(p_k - 1)$ and $p_{k+1} \dots p_n$ are coprime, so $\varphi(x_k) = \varphi(p_0 p_1 \dots p_{k-1}(p_k - 1)) \times \varphi(p_{k+1} \dots p_n) = \varphi(p_0 p_1 \dots p_{k-1}(p_k - 1)) \times (p_{k+1} - 1)\dots(p_k - 1)$. That is, we have to prove the equality $\varphi(p_0 p_1 \dots p_{k-1}(p_k - 1)) = (p_0 - 1)(p_1 - 1)\dots(p_k - 1)$.

Let for induction step $y_{k+3} = x_{k+2}(p_{k+1} - 1)$.

Since only $p_0 p_1, \dots, p_{k-1}$ are the prime numbers, which are not more than $(p_k - 1)$, we have $p_k - 1 = \alpha_0 \alpha_1, \dots, \alpha_{k-1}$ for some non-negative integer $\alpha_0 \alpha_1, \dots, \alpha_{k-1}$.

By direct calculation we obtain $\varphi(\mathrm{p}_0 p_1 \dots p_{k-1}(p_k - 1)) = \varphi(p_0^{\alpha_0+1} p_1^{\alpha_1+1} \dots p_{k-1}^{\alpha_{k-1}+1}) =$
$(p_0 - 1)\dots(p_{k-1} - 1)p_0^{(\alpha_0+1)-1} \dots p_{k-1}^{(\alpha_{k-1}+1)-1} =$
$= (p_0 - 1)(p_1 - 1)\dots(p_{k-1} - 1)p_0^{\alpha_0} \dots p_{k-1}^{\alpha_{k-1}} =$
$(p_0 - 1)(p_1 - 1)\dots(p_{k-1} - 1)(p_k - 1)$.

Also we may subtract 1 from more than one p_k, if $(p_k - 1)$ has the decomposition into prime factors, which does not contain some p_j, $(j < k)$. For example, $\varphi(p_0 p_1 p_2 p_3) = \varphi(2 \times 3 \times 5 \times 7) = 48$. Except $(2-1) \times 3 \times 5 \times 7, 2 \times (3-1) \times 5 \times 7, 2 \times 3 \times (5-1) \times 7$ and $2 \times 3 \times 5 \times (7-1)$, we may take as preimage, for example, $2 \times (3-1)(5-1) \times 7$, because $(3-1) = 2$ and $(5-1) = 2^2$. Hence $\varphi(2 \times (3-1)(5-1)) = (2-1)(3-1)(5-1)$ by the same arguments, as for $p_0, \dots, p_{k-1}(p_k - 1)p_{k+1}, \dots, p_n$. So, we may construct at most 2^n products of the form $p_0 q_1, \dots, q_n$, where $q_k = p_k$. Also $(p_0 - 1)p_1, \dots, p_n$ fits for the requirement $\varphi(p_0 - 1)p_1, \dots, p_n = (p_0 - 1)\dots(p_n - 1)$, so we have at most $2^n + 1$ numbers, which give us the same meaning of φ, as $p_0, \dots, p_n$. Note, that it is not necessarily the complete set of such numbers x, for which $\varphi(x) = p_0 p_1, \dots, p_n$, but it is the set, which may be obtained by the given by us scheme.

The case when a number of form $f(m)$ is prime we denote by $(f(m))_p$. We denote Mersenne number by M_m, where $M_m = 2^m - 1$.

Corollary. If $M_a < M_b$ for $m \in N$, then set $\varphi^{-1}(2M_a M_b)$ contains an element M_b^2 if and only if $b = a + 1$. On the other hand, if $2M_a M_b + 1 \in \mathbb{P}$ then $\varphi^{-1}(2M_a M_b) \subseteq \{\{2M_b^2, 2(2M_a M_b + 1)_P, M_b^2, (2M_a M_b + 1)_P\}; a + 1 = b\} \cup$
$\cup \{\{2(2M_a M_b + 1)_P, (2M_a M_b + 1)_P\}; a + 1 \neq b\}$.

7 Possible questions for further research.

For an introduction, interested reader can refer [10] for further study, from which we collect some of the important properties of $\varphi(n)$. $\varphi(m) = 2^a \prod_{i=1}^{k} p_i^{a_i}$.

8 Conclusion.

The analytic expression for exact multiplicity of inverses for $m = 2^{2^n + a}$, where $a \in N$, $a < 2^n$ and $\varphi(t) = m$ was obtained. As it turned out, it depends on the number of prime numbers Fermat. The method of constructing of preimages set for obtained by us lower bound was proposed by us. These results can be applied not only to the cryptanalysis of cipher RSA [24] and in the coding theory [21]. The author is grateful to Volodya Karlovskyi for correcting remarks.

References:

[1] *Kevin Ford,* The Number of Solutions of $\varphi(x) = m$ Annals of Mathematics, Second Series, Vol. 150, No. 1 (1999), P. 283-312.

[2] Coleman, R., On the image of Euler's Totient Function, http://arxiv.org/pdf /0910.2223v1.pdf

[3] Gupta, Hansraj, Euler's Totient Function and Its Inverse, Indian Journal of Pure and Applied Mathematics, 12(1), January 1981, 22-30

[4] On Euler's Phi Function, R.D.Carmichael

[5] FermatSearch.org, http://fermatsearch.org

[6] Keller, Wilfrid, Prime Factors of Fermat Numbers, http://www.protsearch.net/fermat.html

[7] Weisstein. Eric W., Fermat Number, http://mathworld.wolfram.com/FermatNumber.html

[8] http: //numbertheory.org/php/carmichael.html

[9] Tsang, Cindy, Fermat Numbers, M414 Number Theory

[10] http://prothsearch.net/fermat.htmlSurnmary

[11] Burton, David, Elementary Number Theory, McGraw Hill Education(India) Private Limited, 2012.

[12] *Skuratovskii, Ruslan.* On Investigation of Euler's Totient Function Preimages, (2019). https://arxiv.org/abs/1812.00067

[13] *Michal Kevek, Florian Luca, Lawrence Somer* 17 Lectures on Fermat Numbers: From Number Theory to Geometry, Springer, CMS Books 9, ISBN 0-387-95332-9.

[14] *Rodney Coleman* On the image of Euler's totient function. Journal of Computer mathematics Sci. (2012), Vol.3 (2), P. 185-189.

[15] *Ruslan Skuratovskii,* "The investigation of Euler's totient function preimages" Sixth International Conference on Analytic Number Theory. Voronoy Conference" Book of abstracts. P. 37-39.

[16] *R. V. Skuratovskii.* On commutator subgroups of Sylow 2-subgroups of the alternating group, and the commutator width in wreath products. / Ruslan V. Skuratovskii // European Journal of Mathematics. **vol. 7**: 1. (2021), P. 353-373. doi.org/10.1007/s40879-020-00418-9.

[17] *Ruslan V. Skuratovskii, Aled Williams* Irreducible bases and subgroups of a wreath product in applying to diffeomorphism groups acting on the Möbius band. Rendiconti del Circolo Matematico di Palermo Series 2. 2020, V. 70, pp. 351-364.

[18] *R. V. Skuratovsky,* Corepresentation of a sylow p-subgroup of a group S_n. Cybernetics and Systems Analysis 2009. 45(1), pp. 25-37. https://doi.org/10.1007/s10559-009-9080

[19] *R. Skuratovskii*, The Derived Subgroups of Sylow 2-Subgroups of the Alternating Group and Commutator Width of Wreath Product of Groups. Mathematics, Basel, Switzerland, (2020) № 8(4), pp. 1-19.

[20] *Ivan Vinogradov,* Elements of Number Theory Dover Publications, 5th ed. 2016. P. 236.

[21] *R.V Skuratovskii.* A method for fast timer coding of texts". Cybernetics and Systems Analysis. 2013. 49 (1), 133-138. https://doi.org/10.1007/s10559-013-9493-4

[22] *Osadchyy, V., Skuratovskii, R.* Criterions of supersinguliarity and groups of Montgomery and Edwards curves in cryptography. WSEAS Transactions on Mathematics 19, 2020. pp. 709-722.

[23] *Skuratovskii, R., Osadchyy, V.* The order of Edwards and Montgomery curves WSEAS Transactions on Mathematics. 19, 2020. pp. 253-264.

[24] *Buhler, J. Lenstra, H. Pomerance, Carl.* (2006). Factoring integers with the number field sieve. 10.1007/BFb0091539.

[25] *Nongluk Viriyapong, Chokchai Viriyapong* On the Diophantine Equation $n^x + 13^y = z^2$ where $n = 2(mod 39)$ and $n+1$ is not a Square Number, WSEAS Transactions on Mathematics, vol. 20, pp. 442-445, 2021.

Contribution of individual authors to the creation of a scientific article (ghostwriting policy)

This is the monic paper

Follow: www.wseas.org/multimedia/contributor-role-instruction.pdf