NNTDM 2 (1996) 4, 41-48

THE NUMBERS WHICH CANNOT BE VALUES OF EULER'S FUNCTION φ

Mladen Vassilev - Missana
5, Victor Hugo Str., Sofia-1124, BULGARIA

In this paper we shall describe all elements of the set of these natural numbers which cannot be values of the Euler's function φ (see e.g. [1]).

Initially, we shall give some definitions. Let

$$A = 2^{g} . \prod_{i=1}^{r} q_{i}^{\beta_{i}}, \qquad (1)$$

where g, r, β_1, $\beta_2, \ldots, \beta_r \geq 1$ are natural numbers and $2 < q_1 < q_2 < \ldots < q_r$ are prime numbers. Let $k: \{1, 2, \ldots, r\} \to \{1, 2, \ldots, r\}$ be a permutation function.

DDefinition 1: The h-tuple $Q = \langle q_{k(1)}, q_{k(2)}, \ldots, q_{k(h)} \rangle$, where $1 \leq h \leq r$, will be called a real-component (R-component) of A iff

$$\prod_{i=1}^{h} (q_{k(j)} - 1) = 2^{\gamma} . \prod_{j=1}^{r} q_{j}^{\Gamma_{j}}, \qquad (2)$$

where $1 \leq \gamma \leq g$ and $0 \leq \Gamma_j \leq \beta_j$ for $1 \leq j \leq r$.

Definition 2: The h-tuple $Q = \langle q_{k(1)}, q_{k(2)}, \ldots, q_{k(h)} \rangle$, where $1 \leq h \leq r$, will be called a solvable R-component (SR-component) of A iff

$$\prod_{j=1}^{h} (q_{k(j)} - 1) = n . 2^{\gamma} . \prod_{j=1}^{h} q_{k(j)}^{\Gamma_{k(j)}}, \qquad (3)$$

where

$$n = \prod_{j=1}^{r} q_{j}^{\beta_{j}} \Big/ \prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)}} \qquad (4)$$

and $1 \leq \gamma \leq l$ and $0 \leq \Gamma_{k(j)} \leq \beta_{k(j)}$ for $1 \leq j \leq h$.

Obviously, every SR-component of A is a R-component of A, too.

The validity of the following assertion follows from (2) and (3).

LEMMA 1. Let $q_{k(1)} < q_{k(2)} < \ldots < q_{k(h)}$, where $1 \leq h \leq r$. The necessary condition $Q = \langle q_{k(1)}, q_{k(2)}, \ldots, q_{k(h)} \rangle$ to be a SR-component of A is the following: at least one number $\gamma_{k(j)}$ for some $j \in \{1, 2, \ldots, h\}$ to be equal to 0.

Definition 3: The s-tuple $P = \langle p_1, p_2, \ldots, p_s \rangle$, where $s \geq 1$ is a natural number and $2 < p_1 < p_2 < \ldots < p_s$ are prime numbers will be called a solvable imaginary component (SI-component) of A iff

$$A = \prod_{i=1}^{s} (p_i - 1). \qquad (5)$$

Let A have the form from (1) and let

$$A = \prod_{i=1}^{t} A_i, \qquad (6)$$

where

$$A_i = 2^{g_i} . \prod_{j=1}^{n_i} q_{i,j}^{\beta_{i,j}}, \qquad (7)$$

g_i, $n_i \geq 1$ and $\beta_{i,j} \geq 0$ for every i $(1 \leq i \leq t)$ are natural numbers and $2 < q_{i,1} < q_{i,2} < \ldots < q_{i,n}$ are prime numbers.

LEMMA 2: The necessary and sufficient condition for that the number A does not have a SI-component is the following: in every factorization of A in the form (6), at least one of the numbers $A_i + 1$ for $1 \leq i \leq t$ to be a composite number.

The proof is obvious.

Below we shall discuss the question related to the solutions of

$$\varphi(x) = A, \qquad (8)$$

where A is an arbitrary natural number. For A = 1 we have $\varphi(1) = \varphi(2) = 1$, so x = 1 and x = 2 satisfy (8). If A > 1 is an odd number, then Euler's formula for φ (see e.g. [1]) shows that (8) does not have solutions. If $A = 2^g$ $(g \geq 0)$, then (8) is satisfied at least for $x = 2^{g+1}$. It remains only the case when $A \neq 2^m$ for every natural number m, but A is an even number. Then A is given by (1). The following theorem solved this case completely.

THEOREM 1: Let A be given by (1). The equation (8) does not have solutions iff the following three conditions are valid simultaneously:

(a_1) A does not have a SR-component;

(b_1) if $Q = \langle q_{k(1)}, q_{k(2)}, \ldots, q_{k(h)} \rangle$ is a SR-component of A (see Def. 2) and if μ, n^* and $z_{k(j)}$ are natural numbers for which: $1 \leq \mu \leq g - \gamma$, $n^* = \prod_{j=1}^{r} q_j^{\beta_j - \Gamma_j} / \prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)} - \Gamma_{k(j)}}$, $0 \leq z_{k(j)} \leq \beta_{k(j)} - \Gamma_{k(j)}$ $(1 \leq j \leq h)$, then the number $A_1 \equiv A_1(\mu, z_{k(1)}, z_{k(2)}, \ldots, z_{k(h)}) = 2^{\mu} . \prod_{j=1}^{h} q_{k(j)}^{z_{k(j)}} . n^*$ does not have a SI-component;

(c_1) for every μ which satisfies the inequality $1 \leq \mu \leq 1$, the number

$$A_2 \equiv A_2(\mu) = 2^{\mu} . \prod_{j=1}^{r} q_j^{\beta_j}$$ does not have a SI-component.

Proof: Let Q be a SR-component of A. Let $x = 2^{g-\gamma+1} . \prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)} - \Gamma_{k(j)} + 1}$.

From (3) and (4) it follows that (8) is valid. Therefore condition (a_1) is a necessary one for the theorem.

Let Q be a R-component of A and let $P = \langle p_1, p_2, \ldots, p_t \rangle$ be a SI-component of $A_1 = 2^{\mu} . \prod_{j=1}^{h} q_{k(j)}^{z_{k(j)}} . n^*$ from (b_1). Then from (5) it follows that $\prod_{j=1}^{s}(p_j - 1) = 2^{\mu}.n^{*}.\prod_{j=1}^{h} q_{k(j)}^{z_{k(j)}}$, from where

$$2^{g-\gamma-\mu}.\prod_{j=1}^{h}(q_{k(j)} - 1).q_{k(j)}^{\beta_{k(j)}-\Gamma_{k(j)}-z_{k(j)}}.\prod_{i=1}^{s}(p_i - 1) = A,$$

because Q is a R-component of A.

Now it is easy to verify directly that the number x given by

$$x = 2^{g-\gamma-\mu+1}.\prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)}-\Gamma_{k(j)}-z_{k(j)}+1}.\prod_{i=1}^{s} p_i$$

is a solution of (8). Therefore condition (b_1) is a necessary one for the above theorem, too.

Let $P = \langle p_1, p_2, \ldots, p_t\rangle$ be a SI-component of A_2. Then

$$2^{g-\mu}.\prod_{j=1}^{s}(p_j - 1) = 2^{g}.\prod_{j=1}^{r} q_j^{\beta_j} = A.$$

We set $x = 2^{g-\mu+1}.\prod_{j=1}^{s} p_j$ and see that x is a solution of (8), i.e. condition (c_1) is also a necessary one for the theorem. Therefore the three above conditions are simultaneously necessary.

Let (8) have a solution x and let x have the form $x = 2^{\alpha_0}.\prod_{j=1}^{s} p_j^{\alpha_j}$, where $\alpha_0 \geq 1$,, because $\varphi(2x) = \varphi(x)$ if x is an odd number.

Therefore

$$2^{\alpha_0 - 1}.\prod_{j=1}^{s} p_j^{\alpha_j - 1}.(p_j - 1) = A. \qquad (9)$$

There are two possibilities for p_i and q_j, where $1 \leq i \leq s$ and $1 \leq j \leq r$. The first case is: $p_i \neq q_j$ for every i and for every j satisfying the above inequalities. From (9) it follows that $\alpha_i = 1$ for every i $(1 \leq i \leq s)$. Then the equality $A_2(\mu) = \prod_{i=1}^{s}(p_i - 1) = A_2$ is valid for some μ $(1 \leq \mu \leq g)$. Hence $P = \langle p_1, p_2, \ldots, p_t\rangle$ is a SI-component of A_2. The second case is: $p_j = q_{k(j)}$ for every j $(1 \leq j \leq h)$ and $h \leq s$. There are two subcases: $h = s$ and $h < s$.

Let $h = s$. From $1 \leq h \leq r$ we obtain

$$2^{\alpha_0 - 1}.\prod_{j=1}^{h} q_{k(j)}^{\alpha_{k(j)} - 1}.(q_{k(j)} - 1) = A. \qquad (10)$$

From the obvious inequalities $\alpha_{k(j)} - 1 \leq \beta_{k(j)}$ for $1 \leq j \leq h$ and from (10) we obtain $\prod_{j=1}^{h}(q_{k(j)} - 1) = 2^{\gamma}.n.\prod_{j=1}^{h} q_{k(j)}^{\Gamma_{k(j)}}$ (cf. (4)), where $\gamma = g - \alpha_0 + 1$, $\Gamma_{k(j)} = \beta_{k(j)} - \alpha_{k(j)} + 1$, for $1 \leq j \leq h$. Therefore

$P = \langle p_1, p_2, \ldots, p_s \rangle$ be a SR-component of A.

Let $h < s$ be the greatest number for which $p_j = q_{k(j)}$ for every j $(1 \le j \le h)$. Then

$$2^{\alpha_0 - 1} \cdot \prod_{j=1}^{h} q_{k(j)}^{\alpha_{k(j)}-1} \cdot (q_{k(j)} - 1) \cdot \prod_{i=h+1}^{s} p_i^{\alpha_i - 1} \cdot (p_i - 1) = A, \qquad (11)$$

where it is necessary to be valid that $0 \le \alpha_{k(j)} - 1 \le \beta_{k(j)}$ for $1 \le j \le h$ and $\alpha_i = 1$ for $h + 1 \le i \le s$. On the other hand, A has the form (1) too. From (11) it follows that:

$$\prod_{i=h+1}^{s} (p_i - 1) = \frac{2^{g-\alpha_0+1} \cdot \prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)}-\alpha_{k(j)}+1}}{\prod_{j=1}^{h} (q_{k(j)} - 1)} \cdot \frac{\prod_{j=1}^{r} q_j^{\beta_j}}{\prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)}}} . \qquad (12)$$

We rewrite (12) in the form:

$$\prod_{j=1}^{h} (q_{k(j)} - 1) = \frac{2^{g-\alpha_0+1} \cdot \prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)}-\alpha_{k(j)}+1} \cdot \prod_{j=h+1}^{r} q_{k(j)}^{\beta_{k(j)}}}{\prod_{i=h+1}^{s} (p_i - 1)} .$$

The denominator of the right-hand side of the above equality is a divisor of A and it does not have prime divisors different from 2 and q_j, for $1 \le j \le r$, because of (9). So the last equality means that $Q = \langle q_{k(1)}, q_{k(2)}, \ldots, q_{k(h)} \rangle$ is a R-component of A. Therefore

$$\prod_{j=1}^{h} (q_{k(j)} - 1) = 2^{\gamma} \cdot \prod_{j=1}^{r} q_j^{\Gamma_j}, \qquad (13)$$

where $1 \le \gamma \le g - \alpha_0 + 1$, $0 \le \Gamma_j \le \beta_j$ $(1 \le j \le r)$. From (12) and (13) directly it follows

$$\prod_{i=h+1}^{s} (p_i - 1) = 2^{g-\alpha_0-\gamma+1} \cdot n_1^{*} \cdot \prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)}-\alpha_{k(j)}-\Gamma_{k(j)}+1}, \qquad (14)$$

where

$$n_1^{*} = \frac{\prod_{j=1}^{r} q_j^{\beta_j - \Gamma_j}}{\prod_{j=1}^{h} q_{k(j)}^{\beta_{k(j)}-\Gamma_{k(j)}}} .$$

Using that $1 \le g - \alpha_0 - \gamma + 1 \le g - \gamma$ and $0 \le \beta_{k(j)} - \alpha_{k(j)} - \Gamma_{k(j)} + 1 \le \beta_{k(j)} - \Gamma_{k(j)}$, we set $\mu = g - \alpha_0 + \gamma + 1$, $z_{k(j)} = \beta_{k(j)} - \alpha_{k(j)} - \Gamma_{k(j)} + 1$ for every j $(1 \le j \le h)$ and note the right-hand side of (14) by $A_1 = A_1(\mu, z_{k(1)}, \ldots, z_{k(h)})$. Then from (14) we obtain that $P = \langle p_{h+1}, p_{h+2}, \ldots, p_s \rangle$ is a SI-component of A_1.

Therefore, the simultaneous validity of conditions (a_1), (b_1) and (c_1) is a sufficient condition for the fact that the equation (8) does not have a solution. With this the theorem is proved.

Theorem 1 gives an algorithm for checking of all even numbers A (A $\neq 2^n$, for every natural number n), which are not values of φ-function. It is the following:

1. Check of condition (c_1) with the help of Lemma 2.
2. Construct the set Q of all R-components of A.
3. Construct the set $Q - Q_1$, where Q_1 is the set of all SR-components of A.
4. Check of condition (b_1) for the R-components of A belong to set $Q - Q_1$.

The number s will be called an order of a component (R- or SI-) $P = \langle p_1, p_2, \ldots, p_s \rangle$. The following assertion is obvious.

LEMMA 3: Every R-component of A from order r is a SR-component of A. There are only one R-component of A from an order r.

The R-components which are not SR-components of A we shall call a unsolvable R-components (UR-components) of A.

The following assertion is related to the necessity for separating of Q and Q_1. Its validity follows from the above lemma.

LEMMA 4: A R-component $Q = \langle q_{k(1)}, q_{k(2)}, \ldots, q_{k(h)} \rangle$ of A is a UR-component of A iff the following conditions are valid simultaneously:

(a) $1 \leq h \leq r$,

(b) There is $j_0 \in \{1, 2, \ldots, r\} - \{k(1), k(2), \ldots, k(h)\}$ such that the prime q_{j_0}, from the factorization of primes for $B = \prod_{j=1}^{h} (q_{k(j)} - 1)$, has a multiplicity different to B_{j_0}.

Below we shall show some applications of Theorem 1.

In (1) we replace g = 1. Then γ = 1 and from the inequality $1 \leq h \leq \gamma$ it follows that h = 1. The SR-components can be only of the form $Q = q_j$ $(1 \leq j \leq r)$. If $Q = q_{j_0}$ is a SR-component, we obtain from (3):

$$q_{j_0} - 1 = 2 . q_{j_0}^{\Gamma_{j_0}} . \prod_{j=1}^{j_0 - 1} q_j^{B_j} . \prod_{j=j_0+1}^{r} q_j^{B_j} . \tag{15}$$

Let $r \geq 2$. When $j_0 < r$, the equality (15) is obviously impossible. When $j_0 = r$, we put the restrictions $q_r \neq \frac{A}{q_r^{B_r}} + 1$ and the number A + 1 is a composite one. Then A does not have SR- and SI- components. As a corollary of Theorem 1 it follows

THEOREM 2: When the number A is given by (1), g = 1 and $r \geq 2$, then the equation (8) does not have solutions iff the following two conditions are valid simultaneously:

(a_2) $q_r \neq \frac{A}{q_r^{B_r}} + 1$;

(b_2) The number A + 1 is a composite one.

Let r = 1. Then $A = 2.q_1^{\beta_1}$ and A does not have a SR-component iff $q_1 > 3$. Obviously, A does not have a SI-component iff A + 1 is a composite number (see Lemma 2). As corollary of Theorem 1 it follows also

THEOREM 3: If number $A = 2.q^{\beta}$, where $q \geq 3$ is a prime number and $\beta \geq 1$ is a natural number, then the equation (8) does not have solutions iff the following two conditions are valid simultaneously:

(a_3) $q > 3$

(b_3) The number A + 1 is a composite one.

COROLLARY 1: If $q > 2$ is a prime number such that number $2.q + 1$ is a composite one then the equation (8) does not have solutions for A = 2q.

COROLLARY 2: Let a and b be natural numbers for which (a, b) = 1, (a, 2.b + 1) > 1. If q is a prime number which belongs to the sequence $\{b+k.a \,/\, k \in N\}$, then the equation (8) does not have solutions when A = 2.q. Particularly, if q is a prime number from the sequence $\{6.k + 1 \,/\, k \in N\}$, then the equation (8) does not have solutions for A = 2.q.

COROLLARY 3: If A = 2.m, where m = 6.k + 1 $(k \in N)$ and $m = q^{\beta}$ $(\beta \geq 1)$ and q is odd prime number, then (8) does not have solutions.

COROLLARY 4: If A = 2.m, where m = 6.k + 1 $(k \in N)$ and both conditions $r \geq 2$ and β_r is an even number are simultaneously valid (see (1)) then the equation (8) does not have solution.

Proof: From $m \equiv 1 \pmod 3$ and $q_r^{\beta_r} \equiv 1 \pmod 3$ we obtain that $\frac{A}{q_r^{\beta_r}} + 1 \equiv 0 \pmod 3$, hence the equality $q_r = \frac{A}{q_r^{\beta_r}} + 1$ is impossible. Then the validity of the assertion follows from Theorem 2.

Up to here we researched the case g = 1. For the case g > 1 we must give some definitions.

It is known (see e.g. [2]) that the prime numbers of the form $F_t = 2^{2^t} + 1$ $(t \in N)$ are called Fermat's prime numbers.

Let $\beta \geq 0$, $g \geq 1$, $q > 2$ and q be a prime number.

Definition 4: We shall call that the couple $\langle g_i, \partial_i \rangle$, where $1 \leq i \leq t$ and $t \geq 1$ generates a Fermat's chain about the couple $\langle g, \beta \rangle$ iif the following two conditions are valid simultaneously:

a') $g_i \geq 1$, $\partial_i \geq 0$ for i = 1, 2, ..., t;

b') $\sum_{i=1}^{t} g_i = g$, $\sum_{i=1}^{t} \partial_i = \beta$ and numbers $2^{g_i}.q^{\partial_i} + 1$ $(1 \leq i \leq t)$ are prime ones.

We must note that the idea for this definition was generated from the case when $\beta = 0$, because in this case numbers $2^{g_i} + 1$ $(1 \le i \le t)$ are Fermat's prime numbers. The numbers g_i $(1 \le i \le t)$ can be called Fermat's chain about g.

THEOREM 4: Let $g \ge 1$, $\beta \ge 1$ and $q > 2$ be a prime number. The equation (8) does not have solutions for $A = 2^g.q^\beta$ iff the following two conditions are valid simultaneously:

(a_4) $q \ne 2^\partial + 1$ for $1 \le \partial \le g$,

(b_4) The numbers $2^\mu.q^\beta + 1$ $(1 \le \mu \le g)$ are composite ones,

(c_4) For every μ $(1 \le \mu \le g)$ there is not Fermat's chain $\langle g_i, \partial_i \rangle$ for which $\partial_i < \beta$ $(1 \le i \le t)$ about the couple $\langle \mu, \beta \rangle$.

The proof follows from Theorem 1.

COROLLARY 5: Let q be a prime number and $q \ne 2^\partial + 1$ $(1 \le \partial \le g)$. If numbers $2^\mu.q^\gamma + 1$ $(1 \le \gamma \le \beta$, $1 \le \mu \le g)$ are all composite, then (8) does not have solutions when $A = 2^g.q^\beta$.

COROLLARY 6: Let $g \ge 1$ and q be a prime number. The equation (8) does not have a solution for $A = 2^g.q$ iff numbers $2.q + 1$, $2^2.q + 1$, ..., $2^g.q + 1$ are composite and simultaneously with this, q is not a Fermat's prime number of the form $2^\mu + 1$ for $1 \le \mu \le g$.

Proof: The validity of the assertion follows directly from Theorem 4 after the substitution $\beta = 1$, because the condition (c_4) is satisfied.

The Dirichlet's theorem for the prime numbers' distribution in an arithmetic progression (see e.g. [3]) in combination with Corollary 2 gives the conclusion that there are infinitely many even numbers A for which the equation (8) does not have a solution, when $g = 1$.

The analogical assertion for the case with an arbitrary number $g \ge 1$ follows from the next

THEOREM 6: If $f(T) = (\prod_{i=0}^{5} F_i).T + \frac{490}{641}.(\prod_{i=0}^{5} F_i) + 1$ is a prime number, then the equality $\varphi(x) = 2^g.f(T)$ does not have a solution.

Proof: Euler has shown that $F_5 \equiv 0 (\mathrm{mod}\ 641)$ (see e.g. [2]). Therefore, the sequence $\{f(T) \mid T \in N\}$, which is an arithmetic progression, contains only natural numbers. From Dirichlet's theorem (see e.g. [3]) in this sequence there are an infinite number of prime numbers. Let $f(T)$ be a fixed prime number. The equality $f(T) = F_n$ for a some $n \ge 0$ generates the congruence $2^{2^n} \equiv 0 (\mathrm{mod}\ F_0)$ which is impossible. Therefore $f(T)$ is not Fermat's prime number.

Below we shall show that numbers $B_\mu = 2^\mu.f(T) + 1$ are composite for $1 \le \mu \le g$.

When μ has the forms $\mu = 4.k + 1$ or $\mu = 4.k + 3$ for some number k, the validity of the assertion follows from congruences

$$B_\mu = 2^{4.k+1}.f(T) + 1 \equiv 0 (\mathrm{mod}\ F_0),$$

$$B_\mu = 2^{4.k+3}.f(T) + 1 \equiv 0 (\mathrm{mod}\ F_0),$$

which are valid. When $\mu = 4.k + 2$ we obtain:

$$B_\mu = 2^{4.k+2}.f(T) + 1 \equiv 0 (\mathrm{mod}\ F_1),$$

i.e., B_μ is a composite number, too. The fourth (the last) case is $\mu = 4.k$. Let $k = m$ is an odd number. It is easily checked that

$$B_\mu = 2^{4.m}.f(T) + 1 \equiv 0 (\mathrm{mod}\ F_2),$$

i.e. B_μ is a composite. Let $k = 2.m$, where m is an odd number. Now, it is checked that

$$B_\mu = 2^{8.m}.f(T) + 1 \equiv 0 (\mathrm{mod}\ F_3).$$

Let $k = 4.m$, where m is an odd number. Then

$$B_\mu = 2^{16.m}.f(T) + 1 \equiv 0 (\mathrm{mod}\ F_4).$$

Finally, let $k = 8.m$. When m is an odd number, it is checked that

$$B_\mu = 2^{32.m}.f(T) + 1 \equiv 0 (\mathrm{mod}\ F_5/641),$$

and when m is an even number, then

$$B_\mu = 2^{32.m}.f(T) + 1 \equiv 0 (\mathrm{mod}\ 641),$$

i.e., B_μ is also composite. For k there are no other possibilities and hence numbers B_μ $(1 \le \mu \le 1)$ are always composite. Therefore, for the numbers $A = 2^g.f(T)$ are valid all conditions from Corollary 6, i.e., the theorem is proved.

In the following Table we give the first ten primes from set $\{f(T) / T \in N\}$, which Stojan Mihov calculated by computer:

T	f(T)	T	f(T)
30	5670357743143893580 1	194	35927696055198054006 61
38	715077530021115387 21	232	429374588032076836 2031
112	208013659147562216823 1	250	462578727364754029 1101
128	237528449665497499407 1	264	488404169067947401 3711
186	344519565293012898774 1	334	617531377583914262676 1

The paper is based on [4].

REFERENCES:

[1] Nagell T., Introduction to number theory, John Wiley & Sons, New York, 1950.

[2] Vasilev M., The numbers which cannot be values of Euler's function φ, Preprint MRL-2-92, Sofia, 1992.

[3] Dirichlet P G. L., Dedekind R., Vorlesungen uber Zahlentheorie, Chelsea, New York, 1968.

[4] Vassilev M., The numbers which cannot be values of Euler's function φ, Preprint MRL-2-92, Sofia, 1992.

Received in BNT in June 1993