NNTDM 2 (1996) 3, 45-46

NOTE ON THE EQUATION $\varphi(x) = 2^l.q$

Mladen V. Vassilev - Missana

5, Victor Hugo Str., Sofia-1124
or
MRL - IPACT, P.O.Box 12, Sofia-1113, Bulgaria

In memory of
Prof. Paul Erdös

Let $\varphi(x)$ be the Euler's totient function.

The $n-$th Fermat number is introduced (as usually) by $F_n = 2^{2^n} + 1$, $(n = 0, 1, ...,)$. The primes of the form $2^\mu + 1$ are called Fermat primes. All known Fermat primes up to now are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.

Are there infinitely many primes q such that for every one of them and for every natural number l the equation

$$\varphi(x) = 2^l.q \qquad (1)$$

has no solutions?

The above question is meaningful. The whole answer is given by the following theorem, which is the main result in the present note.

THEOREM 1: 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 for every $l \geq 1$ the equality $\varphi(x) = 2^l.f(T)$ does not have a solution.

The key for the proof of Theorem 1 is the following author's result [1], which is a special case of the general theorem of [1], describing all natural numbers which cannot be in the range of Euler's function φ.

THEOREM 2 [1]: The equation (1) does not have a solution iff numbers $2.q + 1$, $2^2.q + 1$,..., $2^l.q + 1$ are composite and simultaneously with this, q is not a Fermat prime of the form $2^\mu + 1$, for $1 \leq \mu \leq l$.

Proof of Theorem 1: Euler has shown that $F_5 \equiv 0(mod 641)$ (see, e.g., [2]). Therefore, the sequence $\{f(T)|T \in N\}$, which is an arithmetic progression, contains only natural numbers. From Dirichlet's theorem (see e.g., [3]) there are an infinite number of prime numbers in this sequence. Let $f(T)$ be a fixed prime number. The equality $f(T) = F_n$ for some $n \geq 0$ generates the congruence $2^{2^n} \equiv 0(mod F_0)$ which is impossible. Therefore $f(T)$ is not Fermat's prime.

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

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

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

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

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

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

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

i.e. B_μ is a composite. Let $k = 2.m$, where m is an odd number. Then it can be confirmed that

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

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

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

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

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

and when m is an even number, then

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

i.e., B_μ is also composite. For k there are no other possibilities, and hence numbers $B_\mu (1 \leq \mu \leq l)$ are always composite. Therefore, for $q = f(T)$ all conditions from Theorem 2 are valid, i.e. the Theorem 1 is proved.

The author is thankful to Mr. S. Mihov who made the table below containing computer print-out of the first ten primes from the set $\{f(T)|T \in N\}$.

T	f(T)	T	f(T)
30	56703577431438935801	194	3592769605519805400661
38	71507753002111538721	232	4293745880320768362031
112	2080136591475622168231	250	4625787273647540291101
128	2375284496654974994071	264	4884041690679474013711
186	3445195652930128987741	334	6175313775839142626761

REFERENCES:

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

[2] Edwards H., Fermat's last theorem. A genetic introduction to algebraic number theory, Springer-Verlag, New York, 1977.

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