PUBLIKACIJE ELEKTROTEHNIČKOG FAKULTETA UNIVERZITETA U BEOGRADU
PUBLICATIONS DE LA FACULTÉ D'ÉLECTROTECHNIQUE DE L'UNIVERSITÉ À BELGRADE

SERIJA: MATEMATIKA I FIZIKA — SÉRIE: MATHÉMATIQUES ET PHYSIQUE

№ 381 — № 409 (1972)

389. ON THE NUMBER OF PSEUDOPRIMES $\leqq x$*

Andrzej Rotkiewicz

A composite number n is said to be pseudoprime if $n \mid 2^n - 2$. Let $P(x)$ denote the number of pseudoprimes $\leqq x$. K. SZYMICZEK [3] proved the following theorem:

If k is a natural number and x is sufficiently large, then

$$P(x) > \frac{1}{4}\{\log x + \log\log x + \cdots + \underbrace{\log\log \cdots \log x}_{k \text{ times iterated logarithm}}\}.$$

Here we shall prove the following much stronger theorem.

Theorem 2. $P(x) > \frac{5}{8}\log_2 x$ (*Here* $\log_2 x$ *denotes logarithm at the base* 2.)

Definition. *A factor* m *of* $2^n - 1$ *is said to be primitive if it does not divide any of the numbers* $2^k - 1$, $k = 1, \ldots, n-1$.

Lemma. *For every* $n > 2$, $n \neq 6$ *the number* $2^n - 1$ *has at least one primitive prime factor of the form* $nk + 1$. *For* $2^2 \| n$[1], $n > 20$ *the number* $2^n - 1$ *has two primitive factors of the form* $nk + 1$.

This Lemma follows from theorem of K. ZSIGMONDY [4] and theorem of A. SCHINZEL [2].

Theorem 1. *If n is a positive even integer* $\neq 2, 4, 6, 8, 12$ *then* $2^n - 1$ *has at least one primitive composite factor of the form* $nk + 1$. *For* $2^2 \| n$, $n > 20$ *the number* $2^n - 1$ *has at least two primitive composite factors of the form* $nk + 1$.

***Proof of the Theorem* 1.** We shall distinguish the following three cases:

a) $2 \| n$, $n \neq 2$, 6 or $16 \mid n$.

Let $2 \| n$, $n \neq 2$, 6. By our lemma the number $2^{\frac{n}{2}} - 1$ has a primitive prime factor of the form $\frac{n}{2}k + 1$. Since $2 \nmid \frac{n}{2}$ this prime factor is of the form $nk + 1$.

---

* Presented December 25, 1971 by D. S. MITRINOVIĆ.

[1]) $r^\alpha \| m$ means that $r^\alpha \mid m$ but $r^{\alpha+1} \nmid m$.

If $16 \mid n$ then by lemma the number $2^{\frac{n}{2}}-1$ has a primitive prime factor p of the form $\frac{n}{2}k+1$.

Since $8 \left| \frac{n}{2} \right.$ the number 2 is a quadratic residue mod p. Thus $p \mid 2^{\frac{p-1}{2}}-1$. Since p is a primitive prime factor of $2^{\frac{n}{2}}-1$, thus $\frac{n}{2} \left| \frac{p-1}{2} \right.$, hence p is of the form $nk+1$.

Thus in both cases $(2 \| n,\ n \neq 2, 6$ or $16 \mid n)$ the number $2^{\frac{n}{2}}-1$ has a prime factor of the form $nk+1$.

If we multiply this prime factor by a primitive prime factor of the number 2^n-1 we get a composite primitive factor of the form 2^n-1, which is of the form $nk+1$.

b) Let $2^2 \| n$. If $n=20$, then $341 \cdot 41$ is the primitive composite factor of the number 2^n-1, which is of the form $nk+1$.

Let $2^2 \| n$, $n>20$. By lemma the number 2^n-1 has two different primitive prime factors p and q of the form $nk+1$.

On the other hand, since $2^2 \| n$, $n \neq 4$, 12 we have $n=4(2k+1)$, where $k>1$. The numbers

$$2^{\frac{n}{4}}-1=2^{2k+1}-1, \qquad 2^{\frac{n}{2}}-1=2^{2(2k+1)}-1$$

have prime factors $r=\frac{n}{2}k_1+1$ and $s=\frac{n}{2}k_2+1$.

If $2 \mid k_1 k_2$ then one of the numbers r, s is of the form $nk+1$.

If $2 \nmid k_1 k_2$, then $2 \mid k_1+k_2$ and the product rs has the form $nk+1$. In the both cases the number $2^{\frac{n}{2}}-1$ has a factor of the form $nk+1$. Denote this factor by t. The numbers pt and qt are composite primitive factors of the number 2^n-1. Both are of the form $nk+1$.

c) $8 \mid n$. Since $n \neq 8$ we have $\frac{n}{2}=(2k+1)4$, where $k \geqq 1$. For $k=1$ the number $5 \cdot 13 \cdot 17 \cdot 241 \equiv 1 \pmod{24}$ is a composite primitive factor of the number $2^n-1=2^{24}-1$.

Let $k=2$, then $41 \mid 2^{20}-1=2^{\frac{n}{2}}-1$ and $41p$, where p denotes primitive prime factor of the number $2^{40}-1$, is a composite primitive factor of 2^n-1, which is of the form $nk+1$.

If $k>2$, then by our lemma the number $2^{4(2k+1)}-1$ has two different primitive prime factors $r=\frac{n}{2}k_1+1$ and $s=\frac{n}{2}k_2+1$.

If $2 \mid k_1 k_2$, then one of the numbers r, s is of the form $nk+1$. If $2 \nmid k_1 k_2$, then $2 \mid k_1+k_2$ and rs is of the form $nk+1$. In both cases the number $2^{\frac{n}{2}}-1$ has a factor of the form $nk+1$. If we multiply this factor by a primitive prime factor of 2^n-1 we get a primitive composite factor of 2^n-1, which is of the form $nk+1$.

This completes the proof of Theorem 1.

***Proof of the Theorem* 2.** Let $x \geqq 1905$. Let a denote the greatest positive integer a such that $2a \leqq \log_2 x$ and b donote the greatest positive integer b such that $4(2b-1) \leqq \log_2 x$.

Let us consider the following two sequences:

$$2^{2\cdot 1}-1,\ 2^{2\cdot 2}-1, \dots, 2^{2a}-1 \leqq 2^{\log_2 x}-1 = x-1, \tag{1}$$

$$2^4-1,\ 2^{4\cdot 3}-1, \dots, 2^{4(2b-1)}-1 \leqq 2^{\log_2 x}-1 = x-1. \tag{2}$$

As it is easy to see every composite divisor of the number 2^n-1 which is of the form $nk+1$ is a pseudoprime number. Indeed, if $nk+1$ is a composite divisor of 2^n-1, then $nk+1 \mid 2^n-1 \mid 2^{nk}-1 \mid 2^{nk+1}-2$ and $nk+1$ is a pseudoprime number. We also see that every number of the sequence (2) occurs in the sequence (1).

By Theorem 1 every number $2^{2c}-1$, where c is any positive integer $\leqq \frac{1}{2}\log_2 x$, $c \neq 1, 2, 3, 4, 6$ has a primitive composite factor of the form $2ct+1$ and every number $2^{4(2d-1)}-1$, where d is any positive integer such that $4(2d-1) \leqq \log_2 x$, $d \neq 1, 2, 3$ has two primitive composite factors of the form $4(2d-1)t+1$.

Thus $P(x) \geqq a+b-8$. But $2a > \log_2 x - 2$, hence $a > \frac{\log_2 x}{2} - 1$. Similarly $4(2b-1) > \log_2 x - 8$, hence $b > \frac{\log_2 x}{8} - \frac{1}{2}$.

Thus $P(x) > \frac{5}{8}\log_2 x - 1.5 - 8 > \frac{5}{8}\log_2 x - 10$.

From the proof of Theorem 1 it follows that any primitive composite divisor of 2^n-1 which we obtain by applying the method given in this theorem is not divisible by any of the numbers: 3, 5, 7 with the exception of the number $3\cdot 13\cdot 17\cdot 241$. But ([1]) 10 numbers: $561 = 3\cdot 11\cdot 17$, $645 = 3\cdot 5\cdot 43$, $1105 = 5\cdot 13\cdot 17$, $1729 = 7\cdot 13\cdot 19$, $1905 = 3\cdot 5\cdot 127$, $2465 = 5\cdot 17\cdot 29$, $2821 = 7\cdot 13\cdot 31$, $4371 = 3\cdot 31\cdot 47$, $6601 = 7\cdot 23\cdot 41$, $8911 = 7\cdot 19\cdot 67$ are pseudoprimes.

Thus $P(x) > \frac{5}{8}\log_2 x$ for $x \geqq 8911$. For $1905 \leqq x \leqq 8911$ we verify Theorem 2 directly.

This completes the proof of Theorem 2.

REFERENCES

1. P. Poulet: *Tables de nombres composés vérifiant la théorème de Fermat pour le module* 2 *jusque'à* 100000000. Sphinx **8** (1938), 42—52.

2. A. Schinzel: *On primitive prime factors of $a^n - b^n$.* Proc. Cambridge Phil. Soc. **58** (1962), 555—562.

3. K. Szymiczek: *On pseudoprimes which are products of distinct primes.* Amer. Math. Monthly **74** (1967), 35—37.

4. K. Zsigmondy: *Zur Theorie der Potenzreste.* Monatsh. Math. **3** (1892), 268—284.

Math. Institute PAN
ul. Sniadeckich 8,
Warszawa 1, Poland