ON PSEUDOPRIMES WHICH ARE PRODUCTS OF DISTINCT PRIMES

K. SZYMICZEK, Katowice, Poland

A composite number n is said to be pseudoprime if $n \mid 2^n-2$. Let $P(x)$ denote the number of pseudoprimes $\leqq x$ and let $P_k(x)$ denote the number of square-free pseudoprimes $\leqq x$ having k distinct prime factors. P. Erdös [1] proved that for x sufficiently large,

$$P(x) < 2x \exp\{-\tfrac{1}{3}(\log x)^{1/4}\}, \tag{1}$$

and stated that there is an estimation of $P(x)$ from below $P(x) > c \log x$, which is due to D. H. Lehmer.

In the present paper I prove the inequality $P_2(x) > \frac{1}{4}\log x$, and also estimations of $P_k(x)$ and $P(x)$ from below. As a consequence of (1) I shall prove that the series $\sum 1/P_n$, where P_n is the nth pseudoprime, is convergent.

Now we prove the following lemma.

LEMMA. *If k is a natural number $\geqq 2$ and x is sufficiently large, then*

$$P_{k+1}(x) \geqq P_k(\log x). \tag{2}$$

Proof. Let n be a pseudoprime which is product of $k \geqq 2$ distinct odd primes. In view of a theorem of Zsigmondy [3], there exists a prime $p > n$ such that $p \mid 2^{n-1}-1$ and $n-1 \mid p-1$. Thus,

$$np \mid 2^{n-1} - 1. \tag{3}$$

On the other hand, $np-1$ is divisible by $n-1$, since $n-1 \mid p-1$ and $np-1 = n(p-1)+n-1$. Then by (3) we get

$$np \mid 2^{np-1} - 1,$$

i.e. np is a pseudoprime which is product of $k+1$ distinct odd primes. We observe that if n and m are natural numbers, $n \neq m$, and p, q are primes such that $p > n$, $q > m$, then $np \neq mq$. If $np = mq$ and $p > n$ then m is divisible by p, hence $m \geqq p$, and we get $m > n$. In view of symmetry $m < n$, which is contradictory. Consequently $np \neq mq$. Thus, if n, m are distinct pseudoprimes having $k \geqq 2$ distinct prime factors, the adequate pseudoprimes np and mq are distinct, too.

From (3) it follows that

$$p \mid (2^{(n-1)/2} - 1)(2^{(n-1)/2} + 1),$$

and therefore

$$p \leqq 2^{(n-1)/2} + 1 < e^{n/2}.$$

Thus, if $n \leqq \log x$ then $pn < e^{1/2 \log x} \log x = x^{1/2} \log x < x$. Hence, for every pseudoprime $n = p_1 \cdots p_k \leqq \log x$ there exists at least one pseudoprime $p_1 \cdots p_k p < x$. Thus, by the above remark, we obtain (2).

THEOREM 1. *If* $x \geqq 2^{22}-1$, *then*

$$P_2(x) > \tfrac{1}{4} \log x. \tag{4}$$

Proof. Let m be an odd number >3. In view of Zsigmondy's [3] theorem there exist prime numbers p and q such that

$$p \mid 2^m - 1, \; q \mid 2^m + 1, \; m \mid p - 1, \; 2m \mid q - 1. \tag{5}$$

Since p and m are odd, $2m \mid p-1$. Further,

$$p \mid 2^m - 1 \mid 2^{q-1} - 1, \; q \mid 2^{2m} - 1 \mid 2^{p-1} - 1:$$

hence, by a theorem of J. H. Jeans [2], pq is pseudoprime. From (5) we get

$$pq < 2^{2m} - 1.$$

Thus, for every odd number $m>3$ there exists a pseudoprime of the form pq which is less than $2^{2m}-1$.

Let x be sufficiently large and m be the greatest odd number for which

$$2^{2m} - 1 \leqq x. \tag{6}$$

By the above argument, there are at least $(m-3)/2$ of pseudoprimes of the form pq less than x, i.e.

$$P_2(x) \geqq \frac{m-3}{2} \cdot$$

We see that there are at least $(m-3)/2$ pseudoprimes pq, where p, q are primes satisfying (5), whereas there exist pseudoprimes pq not satisfying (5), for example:

$$17 \cdot 257, \; (17 \mid 2^8 - 1, \; 257 \mid 2^8 + 1),$$

$$23 \cdot 89, \; (23 \cdot 89 = 2^{11} - 1).$$

We also remark that for $m=11$ there are two pseudoprimes satisfying (5), namely $23 \cdot 683$ and $89 \cdot 683$. Thus, if $x \geqq 2^{22}-1$, we may write

$$P_2(x) \geqq \frac{m-3}{2} + 3 > \frac{m+2}{2} \cdot \tag{7}$$

From the definition of m in (6) it follows that

$$x < 2^{2(m+2)} - 1 < e^{2(m+2)},$$

whence $m+2 > \frac{1}{2} \log x$, which, together with (7) gives (4), and the theorem is proved.

REMARK. It may be easily shown that the inequality (4) holds for $x \geqq 1387$, but not for any other x: $1 < x < 1387$.

THEOREM 2. *If k is a natural number $\geqq 2$ and x is sufficiently large, then $P_k(x) > \frac{1}{4} \log_{k-1} x$, where $\log_k x$ denote the k times iterated logarithm.*

Proof. The statement can be easily proved by induction on k if one applies Theorem 1 and our lemma.

THEOREM 3. *If k is a natural number and x is sufficiently large, then*

$$P(x) > \tfrac{1}{4} \log \left\{ x \prod_{n=1}^{k} \log_n x \right\} .$$

Proof. For sufficiently large x, $P(x) > P_2(x) + P_3(x) + \cdots + P_{k+2}(x)$, whence, by Theorem 2,

$$\begin{aligned} P(x) &> \tfrac{1}{4}\{\log x + \log_2 x + \cdots + \log_{k+1} x\} \\ &= \tfrac{1}{4} \log \left\{ x \prod_{n=1}^{k} \log_n x \right\} . \end{aligned}$$

Now we prove another result.

THEOREM 4. *The series $\sum 1/P_n$, where P_n is the n-th pseudoprime, is convergent.*

Proof. If we put $x = P_n$ then the right hand side of (1) becomes

$$n < 2P_n \exp\{-\tfrac{1}{3}(\log P_n)^{1/4}\}.$$

Since $n < P_n$, we have

$$\frac{1}{P_n} < \frac{2}{n \exp\{\frac{1}{3}(\log n)^{1/4}\}} . \tag{8}$$

On the other hand, for large m, $m^{1/4} > 4 \log m$, and thus for sufficiently large n,

$$(\log n)^{1/4} > 4 \log \log n.$$

Hence $\frac{1}{3}(\log n)^{1/4} > \log(\log n)^{4/3}$, and

$$\exp\{\tfrac{1}{3}(\log n)^{1/4}\} > (\log n)^{4/3}. \tag{9}$$

From (8) and (9) we get

$$\frac{1}{P_n} < \frac{2}{n(\log n)^{4/3}},$$

and Theorem 4 follows from the well-known convergence of $\sum 2/\{n(\log n)^{4/3}\}$.

References

1. P. Erdös, On almost primes, this MONTHLY, 57 (1950) 404–407.
2. J. H. Jeans, The converse of Fermat's theorem, Messenger of Math., 27 (1897–8) 174.
3. K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. und Physik, 3 (1892) 268–284.