Reprinted from the AMERICAN MATHEMATICAL MONTHLY
Vol. LVII, No. 6, June-July, 1950

ON ALMOST PRIMES*

P. ERDÖS

1. Introduction. D. H. Lehmer [1] and others have studied odd composite numbers n which behave like primes in that they satisfy the congruence

$$2^n \equiv 2 \pmod{n}.$$

For brevity, we call such numbers almost primes. In a previous note [2] we proved that for every k there exist infinitely many square free almost primes having k distinct prime factors; this generalizes a result of Lehmer for $k \leqq 3$. In the present note we estimate from above the number of almost primes less than a given limit.

2. Theorem. Our result is the following.

THEOREM. *Let $f(x)$ denote the number of almost primes $\leqq x$. Then, for x sufficiently large, we have*

$$f(x) < x \exp\left\{-\tfrac{1}{3}(\log x)^{1/4}\right\}.$$

Remark. Since the number of primes $\leqq x$ is asymptotic to $x/\log x$, our theorem implies that the number of almost primes $\leqq x$ is very much less than the number of actual primes.

3. Proof. Let $g(n)$ be the least positive exponent e such that

$$2^e \equiv 1 \pmod{n}.$$

We separate the almost primes $n \leqq x$ into two classes C_1 and C_2. The class C_1 consists of those n's for which

$$g(n) \leqq \left[\exp\left((\log x)^{1/2}\right)\right] = H,$$

while C_2 consists of all the other almost primes $\leqq x$.

The members of C_1 are divisors of

* Revised by D. H. Lehmer.

$$P = \prod_{r=1}^{H} (2^r - 1).$$

Let $q_1, q_2, \cdots, q_k$ be all the prime factors of P. Then the members of C_1 are included in the class Γ_1 of integers $\leq x$ having prime factors taken from the set $q_1, \cdots, q_k$ only. Since $2^r - 1$ has less than r prime factors, we have

$$k < \sum_{r=1}^{H} r \leq H^2. \tag{1}$$

We now separate the members of Γ_1 into two subclasses $\Gamma_{1,1}$ and $\Gamma_{1,2}$, where $\Gamma_{1,1}$ consists of those members of Γ_1 which have less than

$$W = \frac{1}{10} (\log x)^{1/2}$$

distinct prime factors. From the fact that if $m \leq x$ and if g^α divides m, then $\alpha \leq (\log x)/\log 2$, it follows from (1) that the number of members of $\Gamma_{1,1}$ is less than

$$(\log x/\log 2)^W \sum_{t=1}^{W} \binom{k}{t} < Wk^W (\log x/\log 2)^W,$$

a quantity less than $x^{1/4}$ for all sufficiently large x.

We consider next the class $\Gamma_{1,2}$. Let $d(m)$ denote the number of divisors of m, and let $v(m)$ be the number of distinct prime factors of m. If m belongs to $\Gamma_{1,2}$, then

$$d(m) \geq 2^{v(m)} = \exp \{v(m) \log 2\} > \exp (W/2).$$

Hence, if N is the number of members of $\Gamma_{1,2}$, we have

$$2x \log x > x \sum_{m \leq x} m^{-1} \geq \sum_{m \leq x} \left[\frac{x}{m}\right] = \sum_{m \leq x} d(m) \geq \sum_{m \subset \Gamma_{1,2}} d(m) \geq N \exp (W/2).$$

That is, we have

$$N \leq 2x(\log x) \exp (-W/2).$$

Therefore, if x is sufficiently large, the total number of members of C_1 is less than

$$x^{1/4} + N \leq x^{1/4} + 2x(\log x) \exp (-W/2) < x \exp \left\{-\frac{1}{30} (\log x)^{1/2}\right\}. \tag{2}$$

We take up now the class C_2 which we separate into two classes $C_{2,1}$ and $C_{2,2}$. The class $C_{2,1}$ consists of those members n of C_2 which have a prime factor p such that the greatest common divisor δ of $n-1$ and $p-1$ satisfies

$$\delta = (n - 1, p - 1) \geq \exp ((\log x)^{1/4}) = T.$$

In other words, for each member n of $C_{2,1}$ there is a prime p and an integer m such that

$$n = pm, \qquad p = \delta t + 1, \qquad m = \delta u + 1, \qquad x/p \geqq m > 1.$$

The last inequality follows from the fact that n is composite. If p and δ are fixed, the number of choices for m is at most $x/(\delta p)$. Hence the number of members of $C_{2,1}$ does not exceed

$$\begin{aligned}(3) \qquad \sum_{\delta > T} \sum_{\substack{p \leq x \\ p = \delta t + 1}} x/(\delta p) &< x \sum_{\delta > T} \sum_{t < x/\delta} (t\delta^2)^{-1} < x \sum_{\delta > T} 2(\log x/\delta)\delta^{-2} \\ &< 2x(\log x)T^{-1} < x \exp\left\{-\tfrac{1}{2}(\log x)^{1/4}\right\},\end{aligned}$$

for x sufficiently large.

Finally we consider the class $C_{2,2}$. This consists of almost primes

$$n = \prod_{i=1}^{k} p_i^{a_i}$$

for which

$$\delta_i = (n-1, p_i - 1) < T, \qquad (i = 1, 2, \cdots, k).$$

It is well known that the exponent $g(n)$ divides

$$\phi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1).$$

Also $g(n)$ divides $n-1$ since n is an almost prime. Hence

$$H \leqq g(n) \leqq (n-1, \phi(n)) \leqq \prod_{i=1}^{k} (n-1, p_i - 1) \leqq T^k.$$

That is,

$$k \geqq (\log H)/\log T = \log T.$$

Thus, if M denotes the number of members of $C_{2,2}$, we have, as before,

$$2x \log x > \sum_{m \leqq x} d(m) \geqq \sum_{m \leqq x} 2^{\nu(m)} \geqq 2^k \sum_{m \subset C_{2,2}} 1 \geqq M \cdot 2^{\log T}.$$

Hence, for x sufficiently large, we have

$$\begin{aligned} M &\leqq 2x(\log x) \exp\left\{-(\log 2)\log T\right\} \\ &\leqq x \exp\left\{-\tfrac{1}{2}(\log x)^{1/4}\right\}.\end{aligned}$$

Combining this result with (2) and (3) we have

$$\begin{aligned} f(x) &< x\left\{\exp\left(-\tfrac{1}{30}(\log x)^{1/2}\right) + 2\exp\left(-\tfrac{1}{2}(\log x)^{1/4}\right)\right\} \\ &< x \exp\left(-\tfrac{1}{3}(\log x)^{1/4}\right),\end{aligned}$$

for x sufficiently large. This is our theorem.

4. Discussion. By a slightly more complicated argument we could prove that, for some positive constant c,

$$f(x) < x \exp\left\{-c(\log x)^{1/2}\right\};$$

but the true order of $f(x)$ seems to be considerably smaller. As far as I know, the only estimate for $f(x)$ from below is

$$f(x) > C \log x,$$

which is due to Lehmer.

Added later. As far as I know the question of the existence of even numbers satisfying $2^n \equiv 2 \pmod{n}$ has not been considered. Except for the trivial case $n=2$, I have not succeeded in finding any such even numbers.* By the method of this paper it is easy to see that their number $\leqq x$ is certainly less than $x \exp\left\{-\frac{1}{4}(\log x)^{1/4}\right\}$.

References

1. D. H. Lehmer, On the Converse of Fermat's Theorem, I, II, this MONTHLY, vol. 43, 1936, pp. 347–354; vol. 56, 1949, pp. 300–309. These papers contain references to other work on almost primes.

2. P. Erdös, On the Converse of Fermat's Theorem, this MONTHLY, vol. 56, 1949, pp. 623–624.