ACTA ARITHMETICA
111.1 (2004)

A note on two conjectures

by

JIAHAI KAN (Nanjing)

1. Introduction. Let $d(n)$ denote the divisor function, $\nu(n)$ the number of distinct prime factors, and $\Omega(n)$ the total number of prime factors of n, respectively. About 50 years ago P. Erdős formulated the following conjectures.

(C) There exist infinitely many positive integers n for which

$$d(n) = d(n+1).$$

(D) There exist infinitely many positive integers n for which

$$\Omega(n) = \Omega(n+1).$$

(E) There exist infinitely many positive integers n for which

$$\nu(n) = \nu(n+1).$$

These conjectures have been studied by many mathematicians, e.g. [1], [2], [4], [6] and [8]. Although (C) and (D) were proved by Heath-Brown (cf. [4]) in 1984, conjecture (E) remains open (cf. [8]).

In 1927 during a conversation with H. Hasse, E. Artin enunciated the following famous hypothesis, now known as Artin's conjecture.

(A) For any given non-zero integer a other than 1, -1, or a perfect square, there exist infinitely many primes p for which a is a primitive root (mod p).

This conjecture is the focal point of diverse areas of mathematics such as group theory, algebraic and analytic number theory, and algebraic geometry (cf. [10]). There is a vast amount of literature for conjecture (A), e.g. [7], [3] and [5].

The purpose of this paper is to show the following.

THEOREM. *At least one of the two conjectures* (A) *and* (E) *is true.*

2000 *Mathematics Subject Classification*: 11B, 11N, 11P.

2. The Lemma. Throughout the paper p and q denote primes.

LEMMA. *For sufficiently large x and any fixed positive integers K, M with $(K,M)=1$, $(2K+1,M)=1$, we have*

$$\#\{q : q < x,\, 2q+1 = p \textit{ or } p_1p_2,\, p_1 < p_2,\, q \equiv K \pmod M\} > \frac{C}{\varphi(M)}\, x \ln^{-2} x$$

where φ denotes the Euler totient function.

Proof. This is an easy generalization of [9, Lemma 1], with $a = 2$, $b = 1$.

3. Proof of the Theorem. From the Lemma it is easy to see that at least one of the following two cases must hold.

(i) For sufficiently large x and some positive integers K, M with $(K,M) = 1$, $(2K+1,M)=1$,

$$\#\{q : q < x,\, 2q+1 = p_1p_2,\, p_1 < p_2,\, q \equiv K \pmod M\} \gg x \ln^{-2} x.$$

(ii) For sufficiently large x and any fixed positive integers K, M with $(K,M)=1$, $(2K+1,M)=1$,

$$\#\{q : q < x,\, 2q+1 = p,\, q \equiv K \pmod M\} > \frac{C}{\varphi(M)}\, x \ln^{-2} x.$$

Let $n = 2q$, $n+1 = p_1p_2$ in (i). It is easy to see that (i) implies conjecture (E) with $\nu(n) = \nu(n+1) = 2$, and moreover, all these n belong to a given arithmetic progression. We proceed to show that (ii) implies conjecture (A).

Let a denote a given non-zero integer other than 1, -1, or a perfect square. From (ii) there are infinitely many pairs of primes p, q with $p-1 = 2q$ and $(p,a) = 1$.

By Fermat's little theorem $a^{p-1} \equiv 1 \pmod p$ and $p-1 = 2q$, we have

$$a^{2q} \equiv 1 \pmod p.$$

Consider the following two possibilities.

Case 1: $a^2 \equiv 1 \pmod p$. For sufficiently large p this is impossible.

Case 2: $a^q \equiv 1 \pmod p$. We show this is also impossible for suitably chosen p and q.

Since a is not a perfect square there is a residue class $b \pmod{4|a|}$, with b coprime to $4|a|$, such that a is a quadratic non-residue of p whenever p is congruent to b modulo $4|a|$. If we choose $M = 2|a|$ and $K = (b-1)/2$ we then see that Case 2 will not arise.

Therefore a must be a primitive root (mod p), and (ii) implies conjecture (A).

The proof of the Theorem is complete.

References

[1] P. Erdős and L. Mirsky, *The distribution of the values of the divisor function* $d(n)$, Proc. London Math. Soc. (3) 2 (1952), 257–271.
[2] P. Erdős, C. Pomerance and A. Sárközy, *On locally repeated values of certain arithmetic functions II*, Acta Math. Hungar. 49 (1987), 251–259.
[3] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math. 78 (1984), 127–130.
[4] D. R. Heath-Brown, *The divisor function at consecutive integers*, Mathematika 31 (1984), 141–149.
[5] —, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford (2) 37 (1986), 27–38.
[6] A. Hildebrand, *The divisor function at consecutive integers*, Pacific J. Math. 129 (1987), 307–319.
[7] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 226 (1967), 209–220.
[8] J. H. Kan, *On the number-theoretic functions* $\nu(n)$ *and* $\Omega(n)$, Acta Arith. 78 (1996), 91–97.
[9] J. H. Kan and Z. Shan, *On the divisor function* $d(n)$, Mathematika 43 (1996), 320–322.
[10] M. R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer 10 (1988), no. 4, 59–67.

Nanjing Institute of Post & Telecommunication
210003 Nanjing, Nanjing, China

Received on 30.4.2001
and in revised form on 14.9.2001 (4022)