117. *On the Number of Squares in an Arithmetic Progression*

By Saburô UCHIYAMA
Department of Mathematics, Okayama University, Okayama, Japan

(Communicated by Kenjiro SHODA, M. J. A., Oct. 12, 1976)

Let a and b be arbitrary integers with $a>0$ and $b\geqq 0$. For any real number $x>0$ we denote by $A(x; a, b)$ the number of those integers $an+b$, $0\leqq n\leqq x$, which are squares of an integer. P. Erdös [1; Problem 16] has conjectured that to every $\varepsilon>0$ there corresponds a number $x_0 = x_0(\varepsilon)$ such that we have

(1) $$A(x; a, b)<\varepsilon x \qquad \text{for } x>x_0.$$

He also notes there that W. Rudin has conjectured the existence of an absolute constant $c>0$ such that

(2) $$A(x; a, b)<c\sqrt{x} \qquad \text{for } x\geqq 1.$$

Recently, E. Szemerédi [3] has given a very short proof of (1) by noticing that there are no four squares that form an arithmetic progression, which is a well-known observation due to L. Euler, and by appealing to the result of his to the effect that every infinite sequence of non-negative integers that has positive upper density contains an arithmetic progression of four elements (cf. [2], and also [4]). However, the argument in [2] (and in [4] as well) is elementary but by no means simple, nor straightforward.

1. We shall first give another simple and elementary proof of (1). There is no loss in generality in assuming that $a>b$. Every non-negative integer belongs to one and only one arithmetic progression of the form $an+b$ $(n\geqq 0)$, where a is fixed and $0\leqq b<a$. Hence we have

$$\sum_{b=0}^{a-1} A(x; a, b)=[\sqrt{ax+a-1}]+1 \qquad (x>0)$$

where $[t]$ denotes the greatest integer not exceeding the real number t; this implies that

$$A(x; a, b)\leqq \sqrt{ax+a-1}+1 \qquad (x>0)$$

for any a and b with $a>b\geqq 0$, since we always have $A(x; a, b)\geqq 0$. This clearly proves (1).

We plainly have $A(x; a, b)=0$ $(x>0)$, if b is a quadratic non-residue (mod a).

2. Now, given a and b, we write $(a, b)=d=e^2f$, $a=da_0$ and $b=db_0$. Here, (a, b) denotes the greatest common divisor of a and b, and e^2 is the largest square factor of d, so that f is a squarefree integer. Our