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

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

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

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

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 main result in this note is the following

Theorem. *We have for* $x>0$

$$\left|A(x\,;a,b)-\frac{N(a,b)}{a}(\sqrt{ax+b}-\sqrt{b})\right|\leqq\frac{N(a,b)}{e},$$

where $N(k,l)$ *denotes for integers* $k>0$ *and* l *the number of incongruent solutions* u (mod k) *of the congruence* $u^2\equiv l$ (mod k).

Note. If $(k,l)=1$ then we have

$$N(k,l)=2^\lambda\prod_{\substack{p\mid k\\ p>2,\text{prime}}}\left(1+\left(\frac{l}{p}\right)\right),$$

where $\lambda=0,1$ or 2 according as $2^2\nmid k$, $2^2\| k$ or $2^3\mid k$, and (l/p) is the Legendre symbol for quadratic residuarity. In particular, $N(k,l)=0$ unless l is a quadratic residue (mod k). Also, we have

$$N(a,b)=eN(a_0,fb_0)\,;$$

this follows from the fact that b is a quadratic residue (mod a) if and only if $(f,a_0)=1$ and fb_0 is a quadratic residue (mod a_0).

Proof of the theorem. We have

$$\begin{aligned}A(x\,;a,b)&=\sum_{\substack{0\leqq n\leqq x\\ an+b=m^2}}1\sum_{\substack{u^2\equiv b\,(\mathrm{mod}\,a)\\ 0\leqq u<a}}\sum_{\substack{m\equiv u\,(\mathrm{mod}\,a)\\ \sqrt{b}\leqq m\leqq\sqrt{ax+b}}}1\\ &=\sum_{\substack{v^2\equiv fb_0(\mathrm{mod}\,a_0)\\ 0\leqq v<a_0}}\left(\left[\frac{\sqrt{ax+b}}{efa_0}-\frac{v}{a_0}\right]+\left[\frac{v}{a_0}-\frac{\sqrt{b}}{efa_0}\right]+1\right)\\ &=\frac{\sqrt{ax+b}-\sqrt{b}}{efa_0}N(a_0,fb_0)+R(a,b),\end{aligned}$$

where

$$R(a,b)=-\sum_{\substack{v^2\equiv fb_0(\mathrm{mod}\,a_0)\\ 0\leqq v<a_0}}\left(\psi\left(\frac{\sqrt{ax+b}}{efa_0}-\frac{v}{a_0}\right)+\psi\left(\frac{v}{a_0}-\frac{\sqrt{b}}{efa_0}\right)\right).$$

Here, we have set $\psi(t)=t-[t]-(1/2)$ for real t. Since $|\psi(t)|\leqq1/2$ for all t, we have

$$|R(a,b)|\leqq N(a_0,fb_0),\tag{3}$$

which concludes the proof of our theorem. It seems difficult to give a finer estimate for $R(a,b)$ than (3).

A crude estimate for $N(a_0,fb_0)$ is given by

$$N(a_0,fb_0)=O(a_0^\varepsilon)\qquad\text{for any fixed }\varepsilon>0,$$

the O-constant being dependent of ε. It follows from this that

$$A(x\,;a,b)=O\left(a_0^\varepsilon\left(\sqrt{\frac{x}{a_0}}+1\right)\right)\qquad(x>0)\,;$$

this inequality is in general stronger than (2) for large values of x but it is weaker than (2) for small values of x.

References

[1] P. Erdös: Quelques problèmes de la théorie des nombres. Monographies de L'Enseignement Mathématique, No. 6 (undated).

[2] E. Szemerédi: On sets of integers containing no four elements in arithmetic progression. Acta Math. Acad. Sci. Hungar., **20**, 89–109 (1969).

[3] ——: The number of squares in an arithmetic progression. Studia Sci. Math. Hungar., **9**, 417 (1974).

[4] ——: On sets of integers no k elements in arithmetic progression. Acta Arith., **27**, 199–245 (1975).