Vol. 66, No. 3 DUKE MATHEMATICAL JOURNAL © June 1992

SQUARES IN ARITHMETIC PROGRESSIONS

ENRICO BOMBIERI, ANDREW GRANVILLE, AND JÁNOS PINTZ

I. Let $Q(N; q, a)$ denote the number of squares in the arithmetic progression $qn + a, n = 1, 2, \dots, N$, and let $Q(N)$ be the maximum of $Q(N; q, a)$ over all nontrivial arithmetic progressions $qn + a$.

It seems to be remarkably difficult to obtain nontrivial upper bounds for $Q(N)$. There are currently two proofs known of the weak bound $Q(N) = o(N)$ (which is an old conjecture of Erdös), and both are far from trivial. The first proof, found by Szemerédi [S] in 1974, has for its main tool Szemerédi's celebrated theorem that, for fixed δ and positive k, a subset of $1, \dots, N$ with cardinality at least δN must contain a k-term arithmetic progression, as soon as N is sufficiently large. (The value of k used here is $k = 4$.) The second proof, which appears to be new, uses instead Faltings's celebrated theorem that the number of rational points on a curve of genus $g \geqq 2$ is finite. (The value of g is now $g = 5$.) We shall describe both these proofs later in this section.

In this paper we improve the above upper bound, though we are still far from proving Rudin's conjecture that $Q(N) \asymp \sqrt{N}$. (See Erdös and Graham [EG], p. 17, for a history of this and related problems.) In fact, the most optimistic conjecture is $Q(N) = \sqrt{\frac{8}{3}N} + O(1)$, and even $Q(N) = Q(N; 24, -23)$ for all large N, possibly $N \geqq 8$.

THEOREM. *There are at most $c_1 N^{2/3} (\log N)^{c_2}$ squares in any arithmetic progression $a + q, a + 2q, \dots, a + Nq$ with $q \neq 0$. The constants c_1, c_2 are absolute and effectively computable.*

A possible value for c_2 is $(7^{30} - 1)/6$, although this is clearly unimportant.

Let $Q_k(N)$ be the maximum number of kth powers which can appear in an arithmetic progression of length N. Much the same arguments which go into proving our theorem can be adapted to deal with $Q_k(N)$, and we expect that they should lead to $Q_3(N) \ll N^{3/5+\varepsilon}$ and $Q_k(N) \ll N^{1/2+\varepsilon}$ for $k \geqq 4$. However, there are further complications in the study of the Mordell-Weil group of the Jacobians of the associated curves, and we shall limit ourselves to some comments at the end of this paper about this point.

We now present an outline of our proof and describe its origins: In a letter written to Frenicle in 1640, Fermat proposed the problem of proving that there are no four squares in arithmetic progression. Fermat may well have been able to prove this, but the first published proof appeared in 1780, due to Euler.

Received 2 September 1991. Revision received 18 November 1991.