Vol. 76, No. 3 DUKE MATHEMATICAL JOURNAL © December 1994

LATTICE POINTS ON ELLIPSES

J. CILLERUELO AND A. CÓRDOBA

I. Introduction. Given a positive integer d one may consider the arithmetical function $r_d(n) = \#\{n = x^2 + dy^2/x, y \in Z\}$ which can also be described as the number of lattice points on the ellipse $x^2 + dy^2 = n$, where $d = e^2D$, D square free. The main purpose of this paper is to analyse closely this function in connection with the distribution of lattice points on "small arcs" of those ellipses.

Let us denote by h_2 the number of elements of order two in the class field group of $Q(\sqrt{-D})$; then we may state our main result.

THEOREM 1. *On the ellipse $x^2 + dy^2 = n$, an arc of length $n^{(1/4)-1/(8[(m+h_2)/(2h_2+2)]+4)}$ contains, at most, m lattice points.*

In other words, for every $\varepsilon > 0$, there exists a finite constant C_ε such that given an arc of length $n^{(1/4)-\varepsilon}$ on the ellipse $x^2 + dy^2 = n$, it contains no more than C_ε lattice points. The particular case $m = h_2 + 2$, which corresponds to arcs of length $n^{1/6}$, is not difficult to prove by geometric arguments based on curvature considerations. However, the general case is of a much more intricate arithmetical nature.

Similar to the case of Gaussian integers one has estimates of the form $r_d(n) = O(n^\varepsilon)$ and $\limsup_{n\to\infty}(r_d(n)/(\log n)^\varepsilon) = \infty$ for every $\varepsilon > 0$. Therefore, in view of the theorem, one may ask what happens for arcs whose lengths are n^α, $1/2 > \alpha \geqslant 1/4$; this remains an open question which we have not been able to answer with the methods introduced to prove Theorem 1. There is a relationship between upper bounds estimates for lattice points on arcs, restriction lemmas of Fourier series and integrals, and L^p-properties of certain Gaussian sums (see [1], [2], [7], [10], [11], and [12]). The existence of this connection has stimulated this research whose first published result [1] contains the case $d = 1$.

To analyse further the properties of the function $h_2(n)$ seems to us a very interesting question, about which little is known. Nevertheless, it follows from a general result due to Gauss that h_2 is not bounded. In fact, Gauss showed that for each k, there are infinitely many imaginary quadratic fields, whose class group contains isomorphic copies of the direct product of k copies of Z_2.

Another interesting question is to analyse how "well distributed" are the lattice points on these ellipses when $r_d(n)$ is large enough. In the next theorem we answer that question in the following sense: we consider the quantity $\mathscr{D}_d(n) = \mathscr{S}_d(n)/(\pi n/\sqrt{d})$, for $r_d(n) \geqslant 4$, where $\mathscr{S}_d(n)$ denotes the area of the polygon whose vertices are the lattice points on the ellipse $x^2 + dy^2 = n$. Clearly these lattice points will be

Received 17 July 1992. Revision received 17 May 1994.