ADVANCES IN MATHEMATICS **46**, 1–2 (1982)

On the Gaps between Numbers which Are Sums of Two Squares

IAN RICHARDS

Department of Mathematics, University of Minnesota, Minneapolis, Minnesota 55455

Besides considering sums of two squares $s = x^2 + y^2$, we can generalize to the case of numbers representable by arbitrary binary quadratic forms of a fixed discriminant D $(D \neq m^2)$.

THEOREM. *Let D be a fixed discriminant. Let $s_1, s_2, \ldots$ be the sequence, arranged in increasing order, of positive integers representable by any binary quadratic form of discriminant D. Then:*

$$\limsup_{n \to \infty} \frac{s_{n+1} - s_n}{\log s_n} \geqslant \frac{1}{|D|}.$$

Apparently this result exceeds all known estimates. (Compare Erdös [1], where the term $\log s_n$ is divided by "log log" factors.) However, the construction is strikingly simple.

Here is the construction. The details will follow. For clarity, we restrict our attention to the case $s = x^2 + y^2$. Fix an integer k (the size of the gap). For each prime $p \leqslant 4k$, $p \equiv 3 \pmod 4$, let $\beta = \beta(p)$ be the highest power such that $p^\beta \leqslant 4k$. Let P be the product of $p^{\beta+1}$ over all such primes p. Define y, $1 \leqslant y \leqslant P$, by

$$4y \equiv -1 \pmod P.$$

Then none of the numbers in the interval

$$\{y + 1, y + 2, \ldots, y + k\}$$

is the sum of two squares.

On the other hand, easy estimates show that $P < e^{(1+\varepsilon)4k}$, whence the size k of the gap is related to the size P of the numbers inside it by $k > (1 + \varepsilon)^{-1} (1/4) \log P$.

Here are the details of the proof. For the size of P, we note that

0001-8708/82/100001–02$05.00/0

$p^{\beta+1} \leqslant (4k)^2$, and that the number of primes $p \equiv 3 \pmod 4$, $p \leqslant 4k$, is asymptotic to $2k/\log 4k$. Thus:

$$P < (4k)^{2[(1+\varepsilon)(2k/\log 4k)]} = e^{(1+\varepsilon)4k}.$$

To show that $y+1, \ldots, y+k$ are not sums of two squares, we argue as follows. Since $4y \equiv -1 \pmod P$,

$$4(y+j) \equiv 4j-1 \pmod P \qquad \text{for} \quad 1 \leqslant j \leqslant k.$$

Now $4j-1$ must be divisible by some prime $p \equiv 3 \pmod 4$ to an *odd* power α. Clearly $\alpha \leqslant \beta(p)$ (the highest power of p which is $\leqslant 4k$). Since P is divisible by $p^{\beta+1}$, this means that p also divides $(y+j)$ exactly to the power α. Hence $(y+j)$ is not the sum of two squares. Q.E.D.

For the case of a general discriminant D, the primes $p \equiv 3 \pmod 4$ are replaced by the primes p for which the Kronecker symbol $(D/p) = -1$. The factor $|D|$ replaces 4 throughout, and the congruence $4y \equiv -1$ is replaced by $|D|\, y \equiv r$, where r is any number such that $(D/r) = -1$. Otherwise the proof goes as before.

We conclude with two remarks and a note of thanks. Firstly, the proof was not found this way. The original idea was to use the Chinese Remainder Theorem to juggle the arithmetic progression $\{3, 7, 11, \ldots, 4j-1\}$. The fact that all of the resulting congruences turned out to be the same came as a surprise. Secondly, if we considered *primitive* representations by forms of discriminant D, then the constant $1/|D|$ could be replaced by $2/|D|$. For in our proof, the modulii $p^{\beta+1}$ could be replaced by p.

The fact that this proof works for general rather than primitive representations was pointed out to me by Paul Erdös. It is a pleasure to extend to him my regards and thanks.

Reference

1. P. Erdös, Some problems in elementary number theory, *Publ. Math. Debrecen* **2** (1951), 103–109.