SOME PROBABILISTIC REMARKS ON FERMAT'S LAST THEOREM

P. ERDÖS AND S. ULAM

Let \( a_1 < a_2 < \cdots \) be an infinite sequence of integers satisfying \( a_n = (c + o(1))n^{\alpha} \) for some \( \alpha > 1 \). One can ask: Is it likely that \( a_i + a_j = a_r \) or, more generally, \( a_i + \cdots + a_n = a_r \), has infinitely many solutions. We will formulate this problem precisely and show that if \( \alpha > 3 \) then with probability 1, \( a_i + a_j = a_r \) has only finitely many solutions, but for \( \alpha \leq 3 \), \( a_i + a_j = a_r \) has with probability 1 infinitely many solutions. Several related questions will also be discussed.

Following [1] we define a measure in the space of sequences of integers. Let \( \alpha > 1 \) be any real number. The measure of the set of sequences containing \( n \) has measure \( C_1 n^{1/\alpha - 1} \) and the measure of the set of sequences not containing \( n \) has measure \( 1 - C_1 n^{1/\alpha - 1} \). It easily follows from the law of large numbers (see [1]) that for almost all sequences \( A = \{a_1 < a_2 < \cdots \} \) ("almost all" of course, means that we neglect a set of sequences which has measure 0 in our measure) we have

\[
A(x) = (1 + o(1))C_1 \sum_{n=1}^{x} \frac{1}{n^{1/\alpha - 1}} = (1 + o(1))C_1 \alpha x^{1/\alpha}
\]

where \( A(x) = \sum_{a_i < x} 1 \). (1) implies that for almost all sequences \( A \)

\[
a_n = (1 + o(1))(n/c_1\alpha)^{\alpha}.
\]

Now we prove the following

**Theorem.** Let \( \alpha > 3 \). Then for almost all \( A \)

\[
a_i + a_j = a_r
\]

has only a finite number of solutions. If \( \alpha \leq 3 \), then for almost all \( A \), (3) has infinitely many solutions.

It is well known that \( x^3 + y^3 = z^3 \) has no solutions, thus the sequence \( \{n^3\} \) belongs to the exceptional set of measure 0.

Assume \( \alpha > 3 \). Denote by \( E_\alpha \) the expected number of solutions of \( a_i + a_j = a_r \). We show that \( E_\alpha \) is finite and this will immediately...