Making Squares – Sieves, Smooth Numbers, Cores and Random Xorsat

Béla Bollobás
University of Cambridge, Department of Pure Mathematics and Mathematical Statistics, Wilberforce Road, Cambridge CB3 0WB, UK and University of Memphis, Department of Mathematical Sciences, Memphis, TN 38152, USA
bb12@dpmms.cam.ac.uk

Abstract

Since the advent of fast computers, much attention has been paid to practical factoring algorithms. Several of these algorithms set out to find two squares x^2, y^2 that are congruent modulo the number n we wish to factor, and are non-trivial in the sense that $x \not\equiv \pm y \pmod{n}$. In 1994, this prompted Pomerance to ask the following question.

Let $a_1, a_2, \ldots$ be random integers, chosen independently and uniformly from a set $\{1, \ldots x\}$. Let N be the smallest index such that $\{a_1, \ldots, a_N\}$ contains a subsequence, the product of whose elements is a perfect square. What can you say about this random number N? In particular, give bounds N_0 and N_1 such that $\mathbb{P}(N_0 \leq N \leq N_1) \to 1$ as $x \to \infty$. Pomerance also gave bounds N_0 and N_1 with $\log N_0 \sim \log N_1$.

In 2012, Croot, Granville, Pemantle and Tetali significantly improved these bounds of Pomerance, bringing them within a constant of each other, and conjectured that their upper bound is sharp. In a recent paper, Paul Balister, Rob Morris and I have proved this conjecture. In the talk I shall review some related results and sketch some of the ideas used in our proof.

2012 ACM Subject Classification Theory of computation → Design and analysis of algorithms

Keywords and phrases integer factorization, perfect square, random graph process

Digital Object Identifier 10.4230/LIPIcs.AofA.2018.3

Category Keynote Speakers

29th International Conference on Probabilistic, Combinatorial and Asymptotic Methods for the Analysis of Algorithms (AofA 2018).
Editors: James Allen Fill and Mark Daniel Ward; Article No. 3; pp. 3:1–3:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany