Anatomy of a Number
March 13–17, 2006

Square products

Andrew Granville
andrew@dms.umontreal.ca
Département de mathématiques et de statistique
Université de Montréal
C.P. 6128, succ. Centre-ville
Montréal, Québec H3C 3J7
Canada

Abstract

In many factoring algorithms one determines a sequence of integers (created in a pseudo-random way) and one wishes to find a subsequence whose product is a square. This leads to two squares x^2 and y^2 for which $x^2 - y^2$ is a multiple of n, the integer to be factored, and then one has a fair chance that $\gcd(x - y, n)$ is a factor of n.

Rick Shroeppel showed that one practical way to search for such a product is to consider only y-smooth integers in the sequence so that once one has more than $\pi(y)$ such elements, some subproduct is guaranteed to be a square. This idea has proved to be widely applicable and the analysis of the running time of this algorithm has inspired much research into the distribution of smooth numbers.

In 1994 Carl Pomerance proposed an abstraction of this question, asking how many random integers one must typically choose from $[1, x]$ until one has a good chance that there is a subset of the chosen integers whose product is indeed a square. Pomerance showed that with probability $1 + o(1)$ one must select $J(x)^{1+o(1)}$ random integers, where $J(x)$ is the bound obtained by optimizing the value of y in Schroeppel's algorithm.

Our goal is to develop Pomerance's result in two directions:

– to show that the transition from probability $o(1)$ to probability $1 + o(1)$ is "sharp"

– to show that smooth numbers arise in the nature of the problem and are not an artifice of the method of proof.

In this talk we describe *joint work with Ernie Croot and Prasad Tetali* in the direction of these objectives.