Anatomy of Integers
March 13–17, 2006

Analysis of the lattice sieve

Gagan Garg
gagan@csa.iisc.ernet.in
Dept. of Computer Science & Automation
Indian Inst. of Sci. (IISc)
Bangalore, Karnataka 560012
India

R. Balasubramanian
balu@imsc.res.in
The Institute of Mathematical Sciences
Chennai 600113
India

H. V. Kumar Swamy
kumar@csa.iisc.ernet.in
Dept. of Computer Sci. & Automation
Indian Inst. of Sci.
Bangalore, Karnataka 560012
India

Shailesh Patil
shailesh@csa.iisc.ernet.in
Dept. of Computer Sci.& Automation
Indian Inst. of Sci.
Bangalore, Karnataka 560012
India

C. E. Veni Madhavan
cevm@csa.iisc.erne.in
Dept. of Computer Sci. & Automation
Indian Inst. of Sci.
Bangalore, Karnataka 560012
India

Abstract

Anatomy of Integers

March 13–17, 2006

We want to study the following problem: Why is the lattice sieve better than the traditional line sieve? A preliminary analysis of this problem was done by Pollard in his introductory paper on the lattice sieve. However, he had not considered the large prime variations of the number field sieve. We will discuss that in this talk. We will also discuss how we can numerically estimate $\psi_4(x, x^t, x^s)$ i.e. the number of integers upto x with exactly 4 prime divisors between x^s and x^t and the rest of the prime divisors less than x^s.