Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Rigorous analysis of a randomised number field sieve

Jonathan D. Lee [a,b,*], Ramarathnam Venkatesan [c,b]

[a] *Mathematical Institute, University of Oxford, UK*
[b] *Microsoft Research Redmond, United States*
[c] *Microsoft Research India, India*

ARTICLE INFO

Article history:
Received 18 March 2016
Accepted 1 October 2017
Available online xxxx
Communicated by S.D. Miller

MSC:
primary 11Y05
secondary 11-04, 05D40, 60C05

Keywords:
Factoring
Probabilistic combinatorics
Additive number theory

ABSTRACT

Factorisation of integers n is of number theoretic and cryptographic significance. The Number Field Sieve (NFS) introduced circa 1990, is still the state of the art algorithm, but no rigorous proof that it halts or generates relationships is known. We propose and analyse an explicitly randomised variant. For each n, we show that these randomised variants of the NFS and Coppersmith's multiple polynomial sieve find congruences of squares in expected times matching the best-known heuristic estimates.

Contents

* Corresponding author.
E-mail addresses: jonathan.lee@merton.ox.ac.uk, jonatlee@microsoft.com (J.D. Lee), venkie@microsoft.com (R. Venkatesan).

https://doi.org/10.1016/j.jnt.2017.10.019
0022-314X/

1. Introduction

For real numbers a, b, x, we write

$$L_x(a,b) = \exp\left(b(\log x)^a (\log\log x)^{1-a}\right).$$

To factor n, modern factoring algorithms first find a congruence of squares $x^2 = y^2 \bmod (n)$, which is hopefully not trivial in the sense $x \neq \pm y \bmod (n)$, and next compute $\gcd(x \pm y, n)$ to obtain factors of n. Hence the runtime analysis is devoted to the first part and studied actively [6,48,10,4,47,11,58,33,49], while the second part has been elusive and heuristic with the exception of variants of Dixon's algorithm and the class group algorithm. In the subsequent, we introduce a randomised variant of the Number Field Sieve and provide an unconditional analysis on the first part, and provide evidence that the factors so obtained are non-trivial. In particular:

Theorems 2.1 (p. 7) and 2.3 (p. 7) *There is a randomised variant of the Number Field Sieve which for each n finds congruences of squares $x^2 = y^2 \bmod (n)$ in expected time:*

$$L_n\left(\frac{1}{3}, \sqrt[3]{\frac{64}{9}} + \mathbf{o}(1)\right) \simeq L_n\left(\frac{1}{3}, 1.92299\ldots + \mathbf{o}(1)\right).$$

These congruences of squares are not trivially of the form $x = \pm y$: conditional on a mild character assumption (Conjecture 7.1 (p. 52)), for n the product of two primes congruent to 3 mod 4, the factors of n may be recovered in the same asymptotic run time.

We use a probabilistic technique, which we term *stochastic deepening*, to avoid the need to show second moment bounds on the distribution of smooth numbers. These results can be shown to extend to Coppersmith's multiple polynomial sieve of [9], a randomised variant of which finds congruences of squares modulo n in expected time:

$$L_n\left(\frac{1}{3}, \sqrt[3]{\frac{92+26\sqrt{13}}{27}} + \mathbf{o}(1)\right) \simeq L_n\left(\frac{1}{3}, 1.90188\ldots + \mathbf{o}(1)\right).$$

Part of the randomisation is similar to the polynomial selection algorithm of Kleinjung [26], which is popular in empirical studies, in that we add an $(X - m)R(X)$ to the field polynomial where m is the root of that polynomial in $\mathbb{Z}/n\mathbb{Z}$. Kleinjung chooses m and R to minimise certain norms and improve smoothness, whilst our R is random.

Please cite this article in press as: J.D. Lee, R. Venkatesan, Rigorous analysis of a randomised number field sieve, J. Number Theory (2018), https://doi.org/10.1016/j.jnt.2017.10.019