A Lower Bound for Double Base Expansions

Supervisor: Francesco Sica

office: 7.204 email: `francesco.sica@nu.edu.kz` tel: 5775

1 Capstone Project Description

All mathematics students know that a positive integer n can be expanded (uniquely) in base 2 as

$$n = \sum_{i=0}^{b} d_i 2^i \ , \quad d_i = 0, 1 \quad (\forall i = 0, \ldots, b) \ ,$$

where $b = \lceil \log_2 n \rceil$. In recent years, the implementation of elliptic curve cryptography has requested more varied representations of n. The following double base number system (DBNS) was then proposed[1]. It consists in choosing two small primes, say $2, 3$, so that one can write

$$n = \sum_{i=0}^{k} c_i 2^{a_i} 3^{b_i} \ , \quad a_i, b_i \in \mathbb{N} \cup \{0\} \text{ and } c_i = \pm 1 \quad (\forall i = 0, \ldots, k) \ .$$

It was proved by several authors[2] (using different methods) that such DBNS expansions always exist (although not unique), with $k = O(\log n / \log\log n)$. On the other hand, little is known about a lower bound for k, i.e. the shortest DBNS expansion of n. The only generic result is[3]

$$k > \frac{C \log n}{\log\log n \log\log\log n}$$

for some constant $C > 0$. In fact, a lower bound of[4] $\Omega(\log n / \log\log n)$ seems quite plausible.

The goad of this project is to give evidence towards this lower bound and attempt to prove it using two approaches.

2 Outcomes

The student will learn to study independently, typeset using LaTeX. This work could lead to a publication.

3 Preparation (Reading Material)

The ideal student will come with the following preparation: Math 301 Introductory Number Theory and some programming skills.

---

[1] V. S. Dimitrov, G. A. Jullien, and W. C. Miller. *An algorithm for modular exponentiation.* Information Processing Letters, 66(3):155-159, 1998.

[2] For instance: R. Avanzi, V. S. Dimitrov, C. Doche, and F. Sica. Extending Scalar Multiplication using Double Bases. Proceedings of Asiacrypt 2006, LNCS 4284, pp. 130-144 (2006).

[3] V. Dimitrov and E. Howe. Lower bounds on the lengths of double-base representations. Proc. Amer. Math. Soc. 139(10):3423-3430.

[4] We write $f(n) = \Omega(g(n))$ for some eventually positive function g to denote that $|f(n)| > \tilde{c} g(n)$ for some $\tilde{c} > 0$.