Journal of Number Theory 154 (2015) 63–73

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

On the greatest common divisor of shifted sets

Randell Heyman *, Igor E. Shparlinski

School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

A R T I C L E I N F O

Article history:
Received 4 February 2014
Received in revised form 22 February 2015
Accepted 22 February 2015
Available online 2 April 2015
Communicated by David Goss

MSC:
11A05

Keywords:
GCD
Approximate GCD

A B S T R A C T

Given a set of n positive integers $\{a_1, \ldots, a_n\}$ and an integer parameter H we study the greatest common divisor of small additive shifts of its elements by integers h_i with $|h_i| \le H$, $i = 1, \ldots, n$. In particular, we show that for any choice of $a_1, \ldots, a_n$ there are shifts of this type for which the greatest common divisor of $a_1 + h_1, \ldots, a_n + h_n$ is much larger than H.

1. Introduction

Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ be a nonzero vector. The *approximate common divisor problem*, introduced by Howgrave-Graham [12] for $n = 2$, can generally be described as follows. Suppose we are given two bounds $D > H \ge 1$. Assuming that for some h_i with $|h_i| \le H$, $i = 1, \ldots, n$, we have

$$\gcd(a_1 + h_1, \ldots, a_n + h_n) > D, \tag{1}$$

* Corresponding author.
E-mail addresses: randell@unsw.edu.au (R. Heyman), igor.shparlinski@unsw.edu.au (I.E. Shparlinski).

http://dx.doi.org/10.1016/j.jnt.2015.02.012

the task is to determine the shifts $h_1, \dots, h_n$. If it is also requested that $h_1 = 0$ then we refer to the problem as the *partial approximate common divisor problem* (certainly in this case the task is to find the shifts faster than via complete factorisation of $a_1 \neq 0$).

This problem has a strong cryptographic motivation as it is related to some attacks on the RSA and some other cryptosystems, see [3,4,12,17] and references therein for various algorithms and applications. In particular, much of the current motivation for studying approximate common divisor problems stems from the search for efficient and reliable *fully homomorphic encryption*, that is, encryption that allows arithmetic operations on encrypted data, see [5,10,15].

Here we consider a dual question and show that for any $\mathbf{a} = (a_1, \dots, a_n) \in \mathbb{Z}^n$, there are shifts $|h_i| \le H$, $i = 1, \dots, n$, for which (1) holds with a relatively large value of D. Throughout we use $\gcd(\mathbf{x})$ to mean $\gcd(x_1, \dots, x_n)$ for any $\mathbf{x} \in \mathbb{Z}^n$.

We also denote the height of $\mathbf{x}$ with $\mathfrak{H}(\mathbf{x}) = \max\{|x_1|, \dots, |x_n|\}$.

The implied constants in the symbols 'O', '$\ll$' and '$\gg$' may occasionally, where obvious, depend on the integer parameter n and the real positive parameter ε, and are absolute otherwise. We recall that the notations $U = O(V)$, $U \ll V$ and $V \gg U$ are all equivalent to the assertion that the inequality $|U| \le c|V|$ holds for some constant $c > 0$.

Our treatment of this question is based on some results of Baker and Harman [2] (see also [1]). For an integer $n > 1$ and real positive $\varepsilon < 1$, we define $\kappa(n, \varepsilon)$ as the solution $\kappa > 0$ to the equation

$$\frac{n(\varepsilon\kappa - 1)}{n - 1} = \frac{1}{2^{2+\max\{1,\kappa\}} - 4}. \tag{2}$$

The solution is unique, as the left hand side of (2) is monotonically increasing (as a function of κ) from $-n/(n-1)$ to $+\infty$ on $[0, \infty)$ whilst the right hand side of (2) is positive and monotonically non-increasing.

We also set

$$\vartheta(n, \varepsilon) = \frac{1}{(n-1)}\left(1 - \frac{1}{\varepsilon\kappa(n, \varepsilon)}\right).$$

It easy to see from (2) that $\varepsilon\kappa(n, \varepsilon) > 1$, so $\vartheta(n, \varepsilon) > 0$.

Theorem 1. *For any vector $\mathbf{a} \in \mathbb{Z}^n$, any real positive $\varepsilon < 1$ and*

$$H \ge \mathfrak{H}(\mathbf{a})^{\varepsilon}$$

there exists a vector $\mathbf{h} = (h_1, \dots, h_n) \in \mathbb{Z}^n$ of height

$$\mathfrak{H}(\mathbf{h}) \le H$$

such that

$$\gcd(\mathbf{a} + \mathbf{h}) \gg \mathfrak{H}(\mathbf{h}) H^{\vartheta(n,\varepsilon)}.$$