This is the author's version of the paper.
The final publication has appeared in Int. J. Number Theory 6 (2010), 1113–1116.

A note on smooth numbers in short intervals

Kaisa Matomäki *

Department of Mathematics, 20014 University of Turku, Finland

Abstract

We prove that, for any $\epsilon > 0$, there exist a constant $C > 0$ such that the interval $[x, x + C\sqrt{x}]$ contains numbers whose all prime factors are smaller than $x^{1/(5\sqrt{e})+\epsilon}$.

1 Introduction

Let $\psi(\mathcal{A}, y)$ denote the number of y-smooth integers in the set $\mathcal{A} \subset [x, 2x]$. With y-smooth integer we mean an integer whose all prime factors are at most y. For a typical set $\mathcal{A}$, one would expect that

$$\psi(\mathcal{A}, y) \approx \frac{|\mathcal{A}|}{x}\psi([x, 2x], y). \tag{1}$$

Besides being of theoretical interest, smooth numbers play a prominent role in computational number theory. For such applications, see for instance the recent survey [5]. The interval $\mathcal{A} = [x, x + \sqrt{x}]$ arises in many cases. Harman [6] has shown that

$$\psi([x, x + \sqrt{x}], y) \gg x^{1/2}$$

for $y = x^{1/(4\sqrt{e})}$. He also gave a result for slightly shorter intervals.

When the length of the interval is greater than $\sqrt{x}$, powerful Dirichlet polynomial methods can be applied. Friedlander and Granville [4] used them to show that (1) holds for $\mathcal{A} = [x, x + z]$ with

$$\exp((\log x)^{5/6+o(1)}) \leq y \leq x \quad \text{and} \quad \sqrt{x}y^2 \exp((\log x)^{1/6}) \leq z \leq x.$$

For intervals of length $\ll \sqrt{x}$ such small values of y seem to be a distant target. However some progress has been made: Recently Croot [2] proved that there exists a constant $C = C(\epsilon)$ such that

$$\psi([x, x + C\sqrt{x}], x^{47/(190\sqrt{e})+\epsilon}) > \sqrt{x}(\log x)^{-\log 4 - o(1)}$$

*Email address: ksmato@utu.fi
Keywords: Smooth numbers, short intervals
MSC (2000): 11N25

for all sufficiently large x. Notice that $47/190 \approx 0.247$, so this slightly improves the smoothness parameter y in Harman's result at the cost of a bit longer interval and a lower bound which is not of the expected order. In this paper we show how Croot's new approach can be refined to get the following result.

Theorem 1.1. *Let $\epsilon > 0$. There exists a constant $C = C(\epsilon)$ such that*

$$\psi([x, x + C\sqrt{x}], x^{1/(5\sqrt{e})+\epsilon}) > \sqrt{x}(\log x)^{-\log 4 - o(1)}$$

for all sufficiently large x.

The improvement comes from taking advantage of a result on sums over arithmetic progressions in [1].

2 Proof of Theorem 1.1

First we introduce some notation. Let δ be a small positive constant,

$$Z = [(1+\delta)^{-1}\sqrt{x}, (1+\delta)\sqrt{x}] \cap \mathbb{Z},$$
$$D = \{p_1 p_2 p_3 \mid p_i \in [x^{1/10-\epsilon/5}, x^{1/10-\epsilon/10}]\},$$

and

$$h(n) = |\{q \in D \mid q \mid n\}|.$$

The expected value of $h(n)$ over $n \in Z$ is

$$\mathbb{E}(h) = \frac{1}{|Z|}\sum_{n \in Z} h(n) = \frac{1}{|Z|}\sum_{q \in D}\left(\frac{|Z|}{q} + O(1)\right) = \sum_{q \in D}\frac{1}{q} + O\left(\frac{|D|}{|Z|}\right) \gg \epsilon^3.$$

We will show that h behaves in expected manner in almost all very short intervals.

Lemma 2.1. *For $\delta \in (0, \delta_0(\epsilon))$ and $k > k_0(\epsilon, \delta)$, we have*

$$V = \sum_{z \in Z}\left(\sum_{n \in [z, z+k]} h(n) - (k+1)\mathbb{E}(h)\right)^2 \leq \delta^2 \mathbb{E}(h)^2 (k+1)^2 |Z|$$

for all sufficiently large x.

This means that for most $z \in Z$, the interval $[z, z+k]$ contains about expected number of integers that are divisible by a member of D. These are automatically $x^{1/2-3/10+3\epsilon/5} = x^{1/5+3\epsilon/5}$-smooth. However, in considerations of smooth numbers it is often possible to reduce the smoothness parameter by the factor $1/\sqrt{e}$, which is the case also here. Indeed, by the method of [2, Section 2.4], Lemma 2.1 implies that at least $(\delta + \delta^2)\sqrt{x}$ of the integers $z \in Z$ satisfy

$$\psi([z, z+k], x^{1/(5\sqrt{e})+\epsilon}) > 0. \tag{2}$$

Now we know that a bit more than a half of the integers $z \in Z$ satisfy (2). As shown in [2, Section 2.2], this immediately implies that there are $\gg x^{1/2}$ pairs z_1, z_2 satisfying (2) such that $z_2 = \lceil x/z_1 \rceil$. Then $(z_1 + j_1)(z_2 + j_2) \in \mathcal{A}$ and is y-smooth for some $j_1, j_2 \in \{1, 2, \ldots, k\}$. As in [2, Section 2.1], this implies Theorem 1.1. Hence we only need to prove Lemma 2.1.

Proof of Lemma 2.1. Squaring out, we see that

$$
\begin{aligned}
V &= \sum_{z \in Z} \left(\sum_{n \in [z, z+k]} h(n) \right)^2 - 2(k+1)\mathbb{E}(h) \sum_{z \in Z} \sum_{n \in [z, z+k]} h(n) + (k+1)^2 \mathbb{E}(h)^2 |Z| \\
&= \sum_{z \in Z} \left(\sum_{n \in [z, z+k]} \sum_{\substack{q \in D \\ q | n}} 1 \right)^2 - (k+1)^2 \mathbb{E}(h)^2 |Z| + O(k) \\
&= 2 \sum_{j=1}^{k} (k+1-j) \sum_{q, q' \in D} \sum_{\substack{n \in Z \\ q | n, q' | n+j}} 1 - (k+1)^2 \mathbb{E}(h)^2 |Z| + O(k|Z|).
\end{aligned}
$$

Hence we need to consider the sum

$$
\sum_{q \in D} \sum_{q' \in D} \sum_{\substack{dq \in Z \\ dq \equiv -j \pmod{q'}}} 1. \tag{3}
$$

The dependence $dq \in Z$ between d and q can be removed by splitting summations to short ranges as in [2, Section 2.5].

At this stage Croot handles the congruence condition using a finite Fourier transform and then applying the bound [3, Theorem 2] on bilinear forms with Kloosterman fractions.

However, sums of the type (3) have been studied in a greater depth in a series of papers by Bombieri, Friedlander and Iwaniec. In our situation [1, Theorem 5] is applicable. Letting $q' = p_1' p_2' p_3'$, we can take $n = q$, $r = p_1'$ and $q = p_2' p_3'$ in that theorem. Then

$$
\begin{aligned}
\sum_{q \in D} \sum_{q' \in D} \sum_{\substack{dq \in Z \\ dq \equiv -j \pmod{q'}}} 1 &= \sum_{q \in D} \sum_{q' \in D} \frac{1}{\phi(q)} \sum_{\substack{dq \in Z \\ (dq, q') = 1}} 1 + O(|Z|(\log x)^{-A}) \\
&= (1 + o_{\epsilon, \delta}(1)) \mathbb{E}(h)^2 |Z|.
\end{aligned}
$$

Hence

$$
V = o_{\epsilon, \delta}((k+1)^2 \mathbb{E}(h)^2 |Z|) + O(k|Z|).
$$

This finishes the proof of Lemma 2.1 and therefore that of Theorem 1.1. $\square$

Acknowledgments

The author was supported by the Finnish Cultural Foundation.

References

[1] E. Bombieri, J. B. Friedlander, and H. Iwaniec, Primes in arithmetic progressions to large moduli, *Acta Math.*, **156** (1986) 203–251.

[2] E. Croot, Smooth numbers in short intervals, *Int. J. Number Theory*, **3** (2007) 159–169.

[3] W. Duke, J. Friedlander, and H. Iwaniec, Bilinear forms with Kloosterman fractions, *Invent. Math.*, **128** (1997) 23–43,

[4] J. B. Friedlander and A. Granville, Smoothing "smooth" numbers, *Philos. Trans. Roy. Soc. London Ser. A*, **345**(1676) (1993) 339–347.

[5] A. Granville, Smooth numbers: computational number theory and beyond, in *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, ed. J. P. Buhler and P. Stevenhagen, MSRI Publications, Vol. 44 (Cambridge University Press, Cambridge, 2008), pp. 267–323.

[6] G. Harman, Integers without large prime factors in short intervals and arithmetic progressions, *Acta Arith.*, 91 (1999) 279–289.