LARGE GAPS BETWEEN CONSECUTIVE PRIME NUMBERS CONTAINING SQUARE-FREE NUMBERS AND PERFECT POWERS OF PRIME NUMBERS

HELMUT MAIER AND MICHAEL TH. RASSIAS

Abstract. We prove a modification as well as an improvement of a result of K. Ford, D. R. Heath-Brown and S. Konyagin [2] concerning prime avoidance of square-free numbers and perfect powers of prime numbers.

2010 Mathematics Subject Classification: 11P32.

1. Introduction

In their paper [2], K. Ford, D. R. Heath-Brown and S. Konyagin prove the existence of infinitely many "prime-avoiding" perfect k-th powers for any positive integer k.
They give the following definition of prime avoidance: an integer m is called prime avoiding with constant c, if $m+u$ is composite for all integers u satisfying[1]

$$|u| \leq c\,\frac{\log m \log_2 m \log_4 m}{(\log_3 m)^2}.$$

In this paper, we prove the following two theorems:

Theorem 1.1. *There is a constant $c > 0$ such that there are infinitely many prime-avoiding square-free numbers with constant c.*

Theorem 1.2. *For any positive integer k, there are a constant $c = c(k) > 0$ and infinitely many perfect k-th powers of prime numbers which are prime-avoiding with constant c.*

2. Proof of the Theorem 1.1

We largely follow the proof of [2].

Lemma 2.1. *For large x and $z \leq x^{\log_3 x/(10\log_2 x)}$, we have*

$$|\{n \leq x \,:\, P^+(n) \leq z\}| \ll \frac{x}{(\log x)^5},$$

where $P^+(n)$ denotes the largest prime factor of a positive integer n.

Proof. This is Lemma 2.1 of [2] (see also [8]). □

Date: October 23, 2015.

[1] We denote by $\log_2 x = \log\log x$, $\log_3 x = \log\log\log x$, and so on.

Lemma 2.2. *Let $\mathcal{R}$ denote any set of primes and let $a \in \mathbb{Z} \setminus \{0\}$. Then, for large x, we have*

$$|\{p \leq x \ : \ p \not\equiv a (\mathrm{mod} r) \ (\forall r \in \mathcal{R})\}| \ll \frac{x}{\log x} \prod_{\substack{p \in \mathcal{R} \\ p \leq x}} \left(1 - \frac{1}{p}\right).$$

Note. Here and in the sequel p will always denote a prime number.

Proof. This is Lemma 2.2 of [2] (see also [4]). □

Lemma 2.3. *Let $N = \prod_{p \leq x} p$. Then there is $m_0 \in \mathbb{Z}$, such that for all $m \equiv m_0 (\mathrm{mod}\ N)$ we have:*

$$m + u \text{ is composite for } u \in [-y, y]\,.$$

Proof. The argument for the proof appears in [8] □

Proof of Theorem 1.1. We now consider the arithmetic progression

$$(*) \qquad m = kN + m_0, \ \ k \in \mathbb{N}\,.$$

By elementary methods (see Heath-Brown [6] for references) the arithmetic progression (*) contains a square-free number

$$(1) \qquad m \leq N^{3/2+\varepsilon},$$

where $\varepsilon > 0$ is arbitrarily small.
By the prime number theorem, we have

$$(2) \qquad N \leq e^{x+o(x)}.$$

We know that $m + u$ is a composite number for $u \in [-y, y]$ (see [8]). By the estimates (1) and (2), we obtain

$$y \geq c\, \frac{\log m \log_2 m \log_4 m}{(\log_3 m)^2}$$

for a constant $c > 0$, which proves Theorem 1.1. □

3. Primes in arithmetic progressions

The following definition is borrowed from [7].

Definition 3.1. *Let us call an integer $q > 1$ a "good" modulus, if $L(s, \chi) \neq 0$ for all characters $\chi \bmod q$ and all $s = \sigma + it$ with*

$$\sigma > 1 - \frac{C_1}{\log\left[q(|t| + 1)\right]}.$$

This definition depends on the size of $C_1 > 0$.

Lemma 3.2. *There is a constant $C_1 > 0$ such that, in terms of C_1, there exist arbitrarily large values of x for which the modulus*

$$P(x) = \prod_{p < x} p$$

is good.

Proof. This is Lemma 1 of [7] □

Lemma 3.3. *Let q be a good modulus. Then*

$$\pi(x;q,a) \gg \frac{x}{\phi(q)\log x}\,,$$

uniformly for $(a,q)=1$ and $x \geq q^D$.
Here the constant D depends only on the value of C_1 in Lemma 3.2.

Proof. This result, which is due to Gallagher [3], is Lemma 2 from [7]. □

4. Congruence conditions for the prime-avoiding number

Let x be a large positive number and y, z be defined as in Definition **??**.
Set

$$P(x)=\prod_{p\leq x} p\,.$$

We will give a system of congruences that has a single solution m_0, with

$$0 \leq m_0 \leq P(x)-1$$

having the property that the interval $[m_0^k-y, m_0^k+y]$ contains only few prime numbers.

Definition 4.1. *We set*

$$\begin{aligned}
\mathcal{P}_1 &= \{p\,:\, p\leq \log x \quad or \quad z<p\leq x/40k\}\,,\\
\mathcal{P}_2 &= \{p\,:\, \log x<p\leq z\}\,,\\
\mathcal{U}_1 &= \{u\in[-y,y],\ u\in\mathbb{Z},\ p\mid u \text{ for at least one } p\in\mathcal{P}_1\}\,,\\
\mathcal{U}_2 &= \{u\in[-y,y]\,:\, u\notin\mathcal{U}_1\}\,,\\
\mathcal{U}_3 &= \{u\in[-y,y]\,:\, |u| \text{ is prime}\}\,,\\
\mathcal{U}_4 &= \{u\in[-y,y]\,:\, P^+(|u|)\leq z\}\,,\\
\mathcal{U}_5 &= \{u\in\mathcal{U}_3\ : p\nmid u+2^k-1 \text{ for } p\in\mathcal{P}_2\}
\end{aligned}$$

Lemma 4.2. *We have*

$$\mathcal{U}_2=\mathcal{U}_3\cup\mathcal{U}_4\,.$$

Proof. Assume that $u\in\mathcal{U}_2\setminus\mathcal{U}_4$. Then by Definition 4.1 there is a prime number $p_0\in\mathcal{P}_2$ with $p_0\mid |u|$. Since $u\notin\mathcal{U}_1$, we have $p_0>x/4$. Thus, there is no prime $p_1\mid \frac{|u|}{p_0}$, since otherwise

$$|u|\geq p_0p_1>\frac{x}{4}\log x>y\,,$$

a contradiction. Thus $|u|=p_0$ and therefore $u\in\mathcal{U}_3$. □

Lemma 4.3. *We have*

$$|\mathcal{U}_4|\ll\frac{x}{(\log x)^4}\,.$$

Proof. This follows from Lemma 2.1. □

A trivial consequence of Lemma 2.2. is the following Lemma:

Lemma 4.4. *We can choose the constants c_1, c_2 such that*

$$|\mathcal{U}_5|\leq\frac{x}{30k\log x}\,.$$

For the next definitions and results we follow the paper [2]. For the convenience of the reader we repeat the explanations of [2].
Let k be odd. For each $u \in U$ associate with u a different prime $p_u \in \left(\frac{x}{40k}, x\right]$ such that $(p_u - 1, k) = 1$ (e.g. one can take $p_u \equiv 2(\text{mod } k)$, if $k \geq 3$). Then every residue modulo p_u is a k-th power residue.
Let k be even. There do not exist primes for which every residue modulo p is a k-th power residue.
We maximize the density of k-th power residues by choosing primes p such that $(p-1, k) = 2$, e.g. taking $p \equiv 3(\text{mod } 4k)$. For such primes p every quadratic residue is a k-th power residue.

Definition 4.5. *Let*

$$\tilde{\mathcal{P}}_3 = \begin{cases} \left\{p \, : \, \frac{x}{40k} < p \leq x, \ p \equiv 2 \, (\text{mod } k)\right\} \, , & \textit{if } k \textit{ is odd} \\ \left\{p \, : \, \frac{x}{40k} < p \leq \frac{x}{2}, \ p \equiv 3 \, (\text{mod } 4k)\right\} \, , & \textit{if } k \textit{ is even} \, , \end{cases}$$

We now define the exceptional set $\mathcal{U}_6$ as follows:
For k odd we set

$$\mathcal{U}_6 = \emptyset \, .$$

For k even and $\delta > 0$, we set

$$\mathcal{U}_6 = \left\{ u \in [-y, y] \, : \, \left(\frac{-u}{p}\right) = 1 \ \textit{ for at most } \frac{\delta x}{\log x} \textit{ primes } p \in \tilde{\mathcal{P}}_3 \right\} \, .$$

Lemma 4.6.

$$|\mathcal{U}_6| \ll_\varepsilon x^{1/2 + 2\varepsilon} \, ,$$

if δ is sufficiently small.

Proof. Each u may be written uniquely in the form

$$u = s 2^a u_1^2 u_2 \, ,$$

where $s = \pm 1$, $a \in \{0, 1\}$ and u_2 is odd and squarefree.
From $p \equiv 3(\text{mod} 4k)$ it follows by the law of quadratic reciprocity, that

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{-1}{p}\right) = -1 \, .$$

Therefore

$$(*) \qquad \left(\frac{-u}{p}\right) = -s(-1)^{\frac{u_2 - 1}{2}} \left(\frac{2^a}{p}\right) \left(\frac{p}{u_2}\right) \, .$$

We consider the sum

$$S = \sum_{u \in U} \left| \sum_{p \in \tilde{\mathcal{P}}_3} \left(\frac{-u}{p}\right) \right|^2$$

Given u_2, there are at most $\sqrt{y/u_2} \leq \sqrt{y}$ choices for u_1.
Each of the eight possibilities for the choices $s \in \{-1, 1\}$, $a \in \{0, 1\}$, $u_2 \equiv 1$ or $3 \ (\text{mod } 4)$ leads to a coefficient of $\left(\frac{p}{u_2}\right)$ on the right hand side of (*) that is independent of p.
Thus, we have

$$S \ll y^{1/2} \sum_{u_2 \leq y} \left| \sum_{p \in \tilde{\mathcal{P}}_3} \left(\frac{p}{u_2}\right) \right|^2 \ll_\varepsilon x^{5/2 + \varepsilon}$$

by Lemma 2.3 of [2].

If $u \in \mathcal{U}_6$, then clearly

$$\left| \sum_{p \in \tilde{\mathcal{P}}_3} \left(\frac{-u}{p} \right) \right| \geq \eta \, \frac{x}{\log x}$$

with $\eta = \eta(k) > 0$.

It follows that $|S| \gg |\mathcal{U}_6|(x/\log x)^2$, and consequently that

$$|\mathcal{U}_6| \ll_\varepsilon x^{1/2+2\varepsilon}.$$

□

Definition 4.7. *We set*

$$\mathcal{U}_7 = \mathcal{U}_4 \cup \mathcal{U}_5 \, .$$

Lemma 4.8. *We have*

$$|\mathcal{U}_7| \leq \frac{x}{20k \log x} \, .$$

Proof. This follows from Definition 4.7 and Lemmas 4.3, 4.4 □

We now introduce the congruence conditions, which determine the integer m_0 uniquely (mod $P(x)$).

Definition 4.9.

(C_1) $$m_0 \equiv 1 \pmod p, \ \textit{for } p \in \mathcal{P}_1 \, ,$$

(C_2) $$m_0 \equiv 2 \pmod p, \ \textit{for } p \in \mathcal{P}_2 \, .$$

For the introduction of the congruence conditions (C_3) we make use of Lemma 4.8. Since

$$|\tilde{\mathcal{P}}_3| \geq |\mathcal{U}_7|,$$

there is an injective mapping

$$\Phi \, : \, \mathcal{U}_7/\mathcal{U}_6 \to \tilde{\mathcal{P}}_3, \quad u \to \mathcal{P}_u.$$

We set

$$\mathcal{P}_3 = \Phi(\mathcal{U}_7/\mathcal{U}_6) \, .$$

Every residue modulo p_u is a k-th power residue and we take m_u such that

$$m_u^k \equiv -(u-1) \pmod{p_u}$$

The set (C_3) of congruences is then defined by

(C_3) $$m_0 \equiv m_u \pmod{p_u}, \quad p_u \in \mathcal{P}_3 \, .$$

Let

$$\mathcal{P}_4 = \{ p \in [0, x) \, : \, p \notin \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3 \} \, .$$

The set of congruences is then defined by

(C_4) $$m_0 \equiv 1 \pmod p, \quad p \in \mathcal{P}_4 \, .$$

Lemma 4.10. *The congruence systems* $(C_1) - (C_4)$ *and the condition* $1 \leq m_0 \leq P(x) - 1$ *determine* m_0 *uniquely. We have* $(m_0, P(x)) = 1$.

Proof. The uniqueness follows from the Chinese Remainder Theorem. The coprimality follows, since by the definition of $(C_1) - (C_4)$ m_0 is coprime to all p, with $0 < p \leq x$. □

Lemma 4.11. *Let $m \equiv m_0 \pmod{P(x)}$. Then $(m, P(x)) = 1$ and the number*

$$m^k + (u-1)$$

is composite for all $u \in [-y, y] \setminus \mathcal{U}_6$.

Proof. For $u \in \mathcal{U}_1$, there is $p \in \mathcal{P}_1$ with $p \mid u$. Therefore, since by Definition 4.9, the system (C_1) implies that $m_0 \equiv 1 \pmod{p}$, we have

$$m^k + (u-1) \equiv m_0^k + (u-1) \equiv 1 + u - 1 \equiv u \equiv 0 \pmod{p} ,$$

i.e.

$$p \mid m^k + (u-1) .$$

For $u \in \mathcal{U}_3$, $u \notin \mathcal{U}_5$, there is $p \in \mathcal{P}_2$ with $p \mid u + 2^k - 1$.
Since by (C_2) $m_0 \equiv 2 \pmod{p}$, we have

$$m_0^k + (u-1) \equiv 2^k - 2^k \equiv 0 \pmod{p} ,$$

i.e.

$$p \mid m^k + (u-1) .$$

There is only one remaining case, namely $u \in \mathcal{U}_7/\mathcal{U}_6$, and one uses (C_3). □

5. Conclusion of the proof of Theorem 1.2

Let now x be such that $P(x)$ is a good modulus in the sense of Definition 3.1. By Lemma 3.2, there are arbitrarily large such elements x. Let D be a sufficiently large positive integer. Let $\mathcal{M}$ be the matrix with $P(x)^{D-1}$ rows and $U = 2\lfloor y \rfloor + 1$ columns, with the r, u element being

$$a_{r,u} = (m_0 + rP(x))^k + u - 1,$$

where $1 \leq r \leq P(x)^{D-1}$ and $-y \leq u \leq y$.
Let $N_0(x, k)$ be the number of perfect k-th powers of primes in the column

$$\mathcal{C}_1 = \{a_{r,1} \ : \ 1 \leq r \leq P(x)^{D-1}\} .$$

Since $P(x)$ is a good modulus, we have by Lemma 3.2 that

$$N_0(x, k) \geq C_0(k) \, \frac{P(x)^{D-1}}{\log(P(x)^{D-1})} . \tag{5.1}$$

Let $\mathcal{R}_1$ be the set of rows R_1, in which these powers of primes appear. We now give an upper bound for the number N_1 of rows $R_r \in \mathcal{R}_1$, which contain primes. We observe that for all other rows $R_r \in \mathcal{R}_1$, the element

$$a_{r,1} = (m_0 + rP(x))^k$$

is a prime avoiding k-th power of the prime $m_0 + rP(x)$.

Lemma 5.1. *For sufficiently small c_2, we have*

$$N_1 \leq \frac{1}{2} N_0(x, k) .$$

Proof. For all v with $v - 1 \in \mathcal{U}_6$, let

$T(v) = \{r \ : \ 1 \leq r \leq P(x)^{D-1},\ m_0 + rP(x) \text{ and } (m_0 + rP(x))^k + v - 1 \text{ are primes}\}.$

We have

$$N_1 \leq \sum_{v \in \mathcal{U}_6} T(v) . \tag{5.2}$$

A standard application of sieves gives

$$T(v) \ll P(x)^{D-1} \prod_{x<p\le P(x)} \left(1-\frac{1}{p}\right) \prod_{x<p\le P(x)} \left(1-\frac{\rho(p)}{p}\right) . \tag{5.3}$$

By Lemma 3.1 of [2], we have

$$\prod_{x<p\le P(x)} \left(1-\frac{\rho(p)}{p}\right) \ll_{k,\varepsilon} |v|^{\varepsilon} \frac{\log x}{\log P(x)} .$$

Lemma 5.1 now follows from (5.2), (5.3) and the bound for $|\mathcal{U}_6|$.
This completes the proof of Theorem 1.2. □

Acknowledgements. We would like to thank the referee for his very valuable comments which improved the presentation of the paper.

References

[1] A. C. Cojocaru, M. Ram Murty, *An Introduction to Sieve Methods and their Applications*, Cambridge Univ. Press, 2006.
[2] K. Ford, D. R. Heath-Brown and S. Konyagin, *Large gaps between consecutive prime numbers containing perfect powers*, In: Analytic Number Theory. In honor of Helmut Maier's 60th birthday, Springer, New York, 2015 (to appear).
[3] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math., 11(1970), 329-339.
[4] H. Halberstam and H. -E. Richert, *Sieve Methods*, Academic Press, London, 1974.
[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford Univ. Press, 1979.
[6] D. R. Heath-Brown, *The least square-free number in an arithmetic progression*, J. Reine Angew. Math., 332(1982), 204-220.
[7] H. Maier, *Chains of large gaps between consecutive primes,* Adv. in Math., 39(1981), 257-269.
[8] R. A. Rankin, *The difference between consecutive prime numbers*, J. London Math. Soc., 13(1938), 242-247.

Department of Mathematics, University of Ulm, Helmholtzstrasse 18, 8901 Ulm, Germany.
E-mail address: helmut.maier@uni-ulm.de

Department of Mathematics, ETH-Zürich, Rämistrasse 101, 8092 Zürich, Switzerland & Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA
E-mail address: michail.rassias@math.ethz.ch, michailrassias@math.princeton.edu